EXAM CRAM

CISSP®

Fifth Edition

Cram Sheet

Flash Cards

Practice Tests

MICHAEL GREGG

EXAM CRAM

CISSP® Exam Cram

Fifth Edition

Michael Gregg

CISSP® Exam Cram, Fifth Edition

Copyright © 2021 by Pearson Education, Inc.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-13-741955-5

ISBN-10: 0-13-741955-4

Library of Congress Control Number: 2021907884

ScoutAutomatedPrintCode

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact

governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact

intlcs@pearson.com.

Editor-in-Chief
Mark Taub

Director, ITP Product Management
Brett Bartow

Executive Editor
James Manly

Development Editor
Christopher A. Cleveland

Managing Editor
Sandra Schroeder

Project Editor
Mandie Frank

Copy Editor
Kitty Wilson

Indexer
Ken Johnson

Proofreader
Donna Mulder

Technical Editor
Dr. Dwayne Hodges

Publishing Coordinator
Cindy Teeters

Designer
Chuti Prasertsith

Page Layout
codeMantra

Credits

Figure	Attribution/Credit Line
Figure 3-2	Screenshot of World's Biggest Data Breaches © 2021 Information is Beautiful
Figure 4-13	Screenshot of The Burp Proxy Attack Tool © 2021 PortSwigger Ltd
Figure 4-21	Screenshot of X.509 Certificate © Google LLC
Figure 5-5	Courtesy of Cisco Systems, Inc.
Figure 5-6	Courtesy of Cisco Systems, Inc.
Figure 5-8	Courtesy of Cisco Systems, Inc.
Figure 5-9	Courtesy of Cisco Systems, Inc.
Figure 5-10	Courtesy of Cisco Systems, Inc.
Figure 5-13	Courtesy of Unified IT Services Pvt Ltd
Figure 6-5	Courtesy of Cisco Systems, Inc.
Figure 6-6	Courtesy of Cisco Systems, Inc.
Figure 7-1	Courtesy of Cisco Systems, Inc.
Figure 7-8	Screenshot of Tejon Crypter © Rdgsoft.net
Figure 7-9	Screenshot of Ransomware © 2016 Malware Removal Guides
Figure 8-2	Courtesy of Cisco Systems, Inc.

Contents at a Glance

Table of Contents

About the Author

Michael Gregg has more than 20 years of experience in information security and risk management. He holds two associate's degrees, a bachelor's degree, and a master's degree. Some of the certifications he holds include CISSP, SSCP, MCSE, CTT+, A+, N+, Security+, CASP, CCNA, GSEC, CEH, CHFI, CEI, CISA, CISM, and CGEIT.

In addition to his experience performing security management, audits, and assessments, Gregg has authored or coauthored more than 25 books, including *Certified Ethical Hacker Exam Prep* (Que), *CISSP Exam Cram 2* (Que), and *Security Administrator Street Smarts* (Sybex). He has testified before the U.S. Congress, his articles have been published on IT websites, and he has been sourced as an industry expert for CBS, ABC, CNN, Fox News, and the *New York Times*. He has created more than 15 security-related courses and training classes for various companies and universities. Although leading, building, and managing security programs is where he spends the bulk of his time, contributing to the written body of IT security knowledge is how Michael believes he can give something back to the community that has given him so much.

About the Technical Reviewer

Dr. Dwayne Hodges is a retired U.S. Army officer and combat Iraq War veteran with over 25 years' experience. He is the founder and owner of Wellspring Services, a service disabled veteran–owned small business, and he is a senior cybersecurity executive with extensive education, training, and experience working in commercial, government, and military agencies. Dr. Hodges is a university professor, consultant, and board member in higher education with over 17 years' experience with teaching, course development, and curriculum design. He holds a doctorate in education and organizational leadership, a master's degree in information systems technologies and management information systems security, a master's degree in public administration, and a bachelor's degree in sociology and criminal justice. He is a graduate of the U.S. Army Signal Communications School: School of Information Technology, U.S. Army Signal Center, and U.S. Army Command and General College. Dr. Hodges holds several industry certifications and certificates, including (ISC)^2 CISSP, CCISO, and CEH; CompTIA Information Security+; Certified Network Defense Architect; Information Technology Infrastructure Library (ITIL); and Certified Encryption Specialist. Dr. Hodges has been a featured TEDx speaker, he is a published author, and he has been a featured speaker for the State of Cyber Security discussions. He has testified in front of the National Academy of Sciences on cybersecurity threats. He is also an author, instructor, and course developer for advanced cryptography concepts on Udemy.

Dedication

I dedicate this book to my godson, Alexander Bucio.
May his life be filled with success and happiness. Mucho gusto!

Acknowledgments

I would like to thank the entire Pearson crew, as they have allowed me to maintain this book over 15 years and 5 editions. It's been a great pleasure to help thousands of individuals prepare for and pass the CISSP exam.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@informit.com

Reader Services

Register your copy of *CISSP Exam Cram* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account.* Enter the product ISBN 9780137419555 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box to indicate that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

Welcome to *CISSP® Exam Cram*. The goal of this book is to get you ready to take the Certified Information Systems Security Professional (CISSP) certification exam. Whether this is your first or your fifteenth *Exam Cram*, you'll find information here and in Chapter 1 that will ensure your success as you pursue knowledge, experience, and certification. This introduction explains the (ISC)^2 certification programs in general and talks about how the *Exam Cram* series can help you prepare for the CISSP exam. It includes sections covering preparation, how to take an exam, this book's contents, how this book is organized, and how to contact the author.

Each chapter in this book contains practice questions. This book also provides two practice exams that can help you accurately assess your level of expertise and whether you are ready to take the exam. This book includes answers and explanations for all practice exam and exam preparation questions. I suggest that you study until you can consistently get correct answers on at least 95% on the practice questions and exams in this book before you attempt the real exam.

How to Prepare for the Exam

Preparing for the CISSP exam requires that you obtain and study materials designed to provide comprehensive information about security. In addition to this book, the following sources will help you study and prepare:

- The (ISC)^2 website: www.isc2.org
- The exam outline available at the (ISC)^2 website

One of the best methods to prepare is by setting a target date for taking the exam and then building out a study plan to meet your deadline. One approach is the 80/20 rule: Use 80% of your time reading and 20% of your time taking practice tests or meeting with a study group to review the material. This approach will help you prepare for the CISSP and pass on your first attempt.

Many people have found that forming a study group, attending seminars, and attending a formal training class helped them study for and master the material needed to pass the CISSP exam.

Practice Tests

This book is filled with practice questions to get you ready. Enjoy the following:

- Review Questions ending each chapter: These questions give you a final pass through the material covered in the chapter.
- Two full Practice Exams: The Answer Keys for the Practice Exams include explanations and tips for approaching each Practice Exam question.

In addition, the book includes two additional full practice tests in the Pearson Test Prep software available to you either online or as an offline Windows application. To access these practice tests, please see the instructions in the card inserted in the sleeve in the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep software.

If you are interested in more practice exams than are provided with this book, check out the Pearson IT Certification Premium Edition eBook and Practice Test product. In addition to providing you with three eBook files (EPUB, PDF, and Kindle), this product provides you with two additional exams' worth of questions. The Premium Edition version also offers you a link to the specific section in the book that presents an overview of the Topic covered in the question, allowing you to easily refresh your knowledge. The insert card in the back of the book includes a special offer for a 80% discount on this Premium Edition eBook and Practice Test product, which is an incredible deal.

Taking a Certification Exam

To take the CISSP exam, you must register with (ISC)^2. The CISSP exam is given at Pearson VUE testing centers. (ISC)^2 has implemented regional pricing: For example, as of this writing, registration is $749 https://www.isc2.org/Register-for-Exam/ISC2-Exam-Pricing in the United States. Check the Pearson VUE website at www.pearsonvue.com to get specific details.

After you register for the CISSP exam, you will receive a confirmation notice. Some locations may have limited test centers available, so you should schedule your exam in advance to make sure you can get the specific date and time you would like.

Arriving at the Exam Location

For any exam, you should arrive at the testing center early. Be prepared! You will need to bring your confirmation notice and identification. Two forms of ID are usually required, and any photo ID will suffice (for example, driver's license, green card, passport). The testing center staff requires proof that you are who you say you are and that someone else is not taking the test for you. Arrive early because if you are late, you will be barred from entry and will not receive a refund for the cost of the exam.

ExamAlert

You'll be spending a considerable amount of time in the exam room. All English versions of the exam use the CISSP Computer Adaptive Test (CISSP-CAT) format. You are given three hours to answer 100 to 150 questions. For non-English versions, a 250-question, non-adaptive six-hour version is used.

In the Testing Center

You will not be allowed to take into the examination room study materials or anything else that could raise suspicion of cheating—including practice test material, books, exam prep guides, or other test aids.

After the Exam

You will get your exam results immediately after you finish taking the exam. If you pass the exam, the screen will simply show that you have passed the exam; you will not receive an exact score. If you do not pass, you will receive a complete breakdown on your score, by domain, so you can see the areas where you need further study.

Retaking a Test

If you fail the exam, you must wait at least 30 days to take it again. During this time, you should especially study the exam domains where you were weak. For example, if you received a 95% score in the Communication and Network Security domain and only 12% in Asset Security, you should focus your studies on the Asset Security domain. In addition, you should invest in some practice tests if you have not already done so. There is much to be said for getting used to a testing format.

Tracking Your CISSP Status

After you pass the CISSP certification exam, you need to attest to the CISSP Code of Ethics and have a security professional who already holds the CISSP certification complete an endorsement form for you. This person must be able to attest to your professional experience and be in good standing with (ISC)^2. If you don't know anyone who is CISSP certified, you can get endorsements from another professional who is certified, licensed, or commissioned as well as an officer of the organization where you are employed. (For more information on endorsement, see the (ISC)^2 website.)

To maintain the validity of your CISSP certification, you must get recertified every three years and earn continuing professional education (CPE) credits by attending webinars, writing white papers, and doing other activities that improve your knowledge of information security and help you remain up to date with the security world.

When you earn the CISSP certification, you are recognized as someone who understands IT security and the role of a security leader. It will definitely boost your confidence and help provide greater opportunities to discuss security in a way that leadership will understand.

About This Book

The ideal reader for an *Exam Cram* book is someone seeking certification. However, an *Exam Cram* book is an easily readable book that presents many important facts. Therefore, an *Exam Cram* book is also extremely useful as a quick reference manual.

Most people seeking certification use multiple sources of information. Check out the links at the end of each chapter to get more information about subjects you need to get to know better. You might also seek out security books that describe particular topics in much greater detail. Many have described the CISSP exam as being "a mile wide," so it is important to understand a wide range of topics.

This book includes a number of helpful elements, such as ExamAlerts, tips, notes, and practice questions to make information easier to read and absorb.

Note

Reading this book from start to finish is not necessary; this book is set up so that you can quickly jump back and forth to find sections you need to study.

Inside the front cover of this book is a tear-out *Cram Sheet* that provides a lot of exam-critical information in a short space; use it to study and also to remember last-minute facts immediately before the exam. Use the practice questions to test your knowledge. Brush up on specific topics, when needed, referring to the table of contents and the index. Even after you achieve certification, you can use this book as a rapid-access reference manual.

The Chapter Elements

Each *Exam Cram* book has chapters that follow a predefined structure that makes these books easy to read and provides a familiar format for all *Exam Cram* books. This book, like other *Exam Cram* books, includes the following elements in each chapter:

- Key terms
- Chapter topics
- ExamAlerts
- Notes
- Tips
- Sidebars
- Cautions
- Exam prep questions and answers
- A “Need to Know More?” section that provides links to relevant information

> **Note**
>
> Bulleted lists, numbered lists, tables, and graphics are also used where appropriate. A picture can paint a thousand words sometimes, and tables can help associate different elements with each other visually.

Now let’s look at each of the chapter elements in detail:

- **Key terms**: Each chapter starts with a list of terms you should understand.
- **Chapter topics**: Each chapter follows up the key terms list with a list of topics covered in the chapter. The objective of an *Exam Cram* book is to cover all the important facts without giving too much detail. When examples are required, they are included.

- **ExamAlerts**: ExamAlerts address exam-related information, highlighting content that is particularly important, tricky, or likely to appear on the exam. An ExamAlert looks like this:

ExamAlert

Make sure you look closely at each exam question as reading one word in a question incorrectly may lead you to make an incorrect choice.

- **Notes**: Notes typically contain useful information that is not directly related to the topic currently being discussed. To avoid breaking up the flow of the text, notes are set off from the regular text.

Note

The length of the exam will depend on what version you request. The non-English version is 250 questions.

- **Tips**: Tips often provide shortcuts or better ways to do things.

Tip

A clipping level is the point at which you set a control to distinguish between activity that should be investigated and activity that should not be investigated.

- **Sidebars**: Sidebars, which run beside the main text of a chapter, often describe real-world examples or situations.

How Caller ID Can Be Hacked

Some voice over IP (VoIP) providers allow a user to inject a call party number (CPN) into a call. Because VoIP is not a traditional telephony service, users can take advantage of this injection option to hack caller ID.

- **Cautions**: Cautions apply directly to the use of the technology being discussed in the chapter. For example, a caution might point out that the CER is one of the most important items to examine for biometric devices.

Caution

The crossover error rate (CER) is the point at which Type I errors and Type II errors intersect. The lower the CER is, the more accurate the device.

- **Exam prep questions**: At the end of each chapter is a list of at least 10 exam practice questions similar to those you will see on the actual exam. The exam prep questions in each chapter are relevant to that chapter, and answers and explanations are provided to help you test your skills and learn more as you read.
- **"Need to Know More?" section**: This section at the end of most chapters provides links to relevant sources of information.

Other Book Elements

A number of important elements are provided in this book in addition to the standard chapters:

- **Practice exams**: In addition to exam-preparation questions at the end of each chapter, two full practice exams are included with this book.
- **Answers and explanations for practice exams**: For each question on each of the practice exams, I provide answers and explanations to help you understand why the correct answer is correct and why the incorrect answers are incorrect.
- **Glossary**: The glossary contains a list of important terms used in this book and their definitions.
- **Cram Sheet**: The Cram Sheet is a quick-reference, tear-out sheet of important facts that is especially useful for last-minute preparation. The facts on the Cram Sheet are important for the exam, and many of them can be difficult to remember.
- **Companion website**: The companion website contains the Pearson IT Certification Practice Test engine, which provides multiple test modes that you can use for exam preparation. The practice exams are designed to appropriately balance the questions over the domains covered by the exam. The practice exams cover the same concepts as the actual exam to ensure that you're prepared for the exam.

Chapter Contents

The following list provides an overview of the chapters in the book:

- **Chapter 1, "The CISSP Certification Exam"**: This chapter introduces exam strategies and considerations.
- **Chapter 2, "Asset Security"**: This chapter discusses both physical and logical security and the countermeasures available for protecting an organization's resources. Key topics include CIA, data classification, scoping and tailoring, and control of an organization's assets from creation to destruction.
- **Chapter 3, "Security and Risk Management"**: This chapter discusses asset management and the protection of critical resources. Quantitative and qualitative risk assessment are two major topics covered in this chapter. You need to understand these concepts in order to assess and measure risk while reducing threats to your organization. Key concepts include the development of compliance requirements, professional ethics, policies, procedures, guidelines, and assorted controls.
- **Chapter 4, "Security Architecture and Engineering"**: This chapter discusses key concepts such as computer hardware, operating system design, security models (such as Biba, Bell-LaPadula, and Clark-Wilson), cryptography, and web, mobile, and embedded device vulnerabilities. This chapter also reviews basic physical controls and documentation used to verify, certify, and accredit systems and networks.
- **Chapter 5, "Communication and Network Security"**: This chapter discusses telecommunications technology. The OSI model; TCP/IP; network equipment; SD-WAN; LAN, MAN, and WAN protocols; and wireless technologies are just a few of the technologies discussed. This is an expansive domain and covers a lot of information that you need to master.
- **Chapter 6, "Identity and Access Management"**: This chapter covers the basics of access control and addresses the three A's: authentication, authorization, and accountability. It discussed topics such as identification, single sign-on, centralized authentication, and federation.
- **Chapter 7, "Security Assessment and Testing"**: This chapter discusses security assessments, ethical hacking, and vulnerability scanning. It also reviews common types of malware and various attack methodologies.

- **Chapter 8, "Security Operations"**: This chapter covers operational controls an organization can implement to provide security. This chapter introduces topics such as background checks, dual controls, mandatory vacations, rotation of duties, and auditing.
- **Chapter 9, "Software Development Security"**: This chapter discusses databases, the software development lifecycle, and the importance of building security into applications and systems as early as possible during the development process. This chapter also covers project management, malicious code, knowledge-based systems, and application issues.
- **Practice Exam I**: This is a full-length practice exam.
- **Answers to Practice Exam I**: This element contains the answers and explanations for the first practice exam.
- **Practice Exam II**: This is a second full-length practice exam.
- **Answers to Practice Exam II**: This element contains the answers and explanations for the second practice exam.

Companion Website

Register this book to get access to the Pearson IT Certification test engine and other study materials, plus additional bonus content. Check this site regularly for new and updated postings written by the author that provide further insight into the more troublesome topics on the exam. Be sure to check the box indicating that you would like to hear from us to receive updates and exclusive discounts on future editions of this product or related products.

To access the companion website, follow these steps:

1. Go to www.pearsonITcertification.com/register and log in or create a new account.
2. Enter the ISBN 9780137419555.
3. Answer the challenge question as proof of purchase.
4. Click on the "Access Bonus Content" link in the Registered Products section of your account page to be taken to the page where your downloadable content is available.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following these steps, please visit www.pearsonITcertification.com/contact and select the Site Problems/Comments option to get help from our customer service representatives.

Accessing the Pearson Test Prep Practice Test Software and Questions

The companion site includes access to the Pearson Test Prep practice test software, which displays and grades a set of exam-realistic multiple-choice questions. Using Pearson Test Prep practice test software, you can either study by going through the questions in Study Mode or take a simulated exam that mimics real exam conditions.

These practice tests are available to you either online or as an offline Windows application. To access the practice exams that were developed with this book, please see the instructions in the card inserted in the sleeve in the back of the book. This card includes a unique activation code that enables you to activate your exams in the Pearson Test Prep software.

Note

The cardboard case in the back of this book includes a piece of paper, which provides the activation code for the practice exam associated with this book. Do not lose the activation code. Also included on the paper is a unique, one-time-use coupon code for the purchase of the Premium Edition eBook and Practice Test.

Accessing the Pearson Test Prep Software Online

The online version of the Pearson Test Prep software can be used on any device with a browser and connectivity to the Internet, including desktop machines, tablets, and smartphones. To start using your practice exams online, simply follow these steps:

1. Go to https://www.PearsonTestPrep.com.
2. Select Pearson IT Certification as your product group.
3. Enter your email address and the password for your account. If you don't have an account on PearsonITCertification.com, you need to establish one by going to PearsonITCertification.com/join.
4. In the My Products tab, click the Activate New Product button.

5. Enter the activation code printed on the insert card in the back of your book to activate your product. The product is then listed in your My Products page.
6. Click the Exams button to launch the exam settings screen and start the exam.

Accessing the Pearson Test Prep Software Offline

If you wish to study offline, you can download and install the Windows version of the Pearson Test Prep software. You can use the download link for this software on the book's companion website, or you can just enter this link in your browser: http://www.pearsonitcertification.com/content/downloads/pcpt/engine.zip.

To access the book's companion website and the software, simply follow these steps:

1. Register your book by going to PearsonITCertification.com/register and entering the ISBN 9780137419555.
2. Respond to the challenge questions.
3. Go to your account page and select the Registered Products tab.
4. Click on the Access Bonus Content link under the product listing.
5. Click the Install Pearson Test Prep Desktop Version link in the Practice Exams section of the page to download the software.
6. When the software finishes downloading, unzip all the files onto your computer.
7. Double-click the application file to start the installation and follow the onscreen instructions to complete the registration.
8. When the installation is complete, launch the application and click the Activate Exam button on the My Products tab.
9. Click the Activate a Product button in the Activate Product Wizard.
10. Enter the unique activation code from the card in the sleeve in the back of your book and click the Activate button.
11. Click Next and then click Finish to download the exam data to your application.
12. To start using the practice exams, select the product and click the Open Exam button to open the exam settings screen.

Note that the offline and online versions will sync together, so saved exams and grade results recorded on one version will be available to you in the other version as well.

Customizing Your Exams

When you are in the exam settings screen, you can choose to take exams in one of three modes:

- Study mode
- Practice Exam mode
- Flash Card mode

Study mode allows you to fully customize an exam and review answers as you are taking the exam. This is typically the mode you use first to assess your knowledge and identify information gaps. Practice Exam mode locks certain customization options in order to present a realistic exam experience. Use this mode when you are preparing to test your exam readiness. Flash Card mode strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation, when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes provide, so it is not the best mode for helping you identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters, or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. The two exams printed in the book are available to you, as are two additional exams of unique questions. You can have the test engine serve up exams from all four banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time allowed for taking the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, and whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software, it will check to see if there are any updates to your exam data and automatically download any changes made since the last time you used the software. This requires that you be connected to the Internet at the time you launch the software.

Sometimes, due to a number of factors, the exam data might not fully download when you activate your exam. If you find that figures or exhibits are missing, you might need to manually update your exams.

To update a particular exam you have already activated and downloaded, simply select the Tools tab and click the Update Products button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Windows desktop version of the Pearson Test Prep exam engine software, simply select the Tools tab and click the Update Application button. Doing so allows you to ensure that you are running the latest version of the software engine.

Contacting the Author

Thank you for selecting my book; I have worked to apply the same concepts in this book that I have used in the hundreds of training classes I have taught. I hope this book provides you with the tools you need to pass the CISSP exam. Feedback is appreciated.

Spend your study time wisely and you can earn CISSP certification. Good luck on the exam!

Assessing Your Readiness for the CISSP Exam

This section helps you understand what's required to obtain the CISSP certification and evaluate your readiness to take the CISSP certification exam. Are you ready?

Security Professionals in the Real World

Security is growing more important all the time, and the CISSP certification continues to be one of the most sought-after security certifications. Increasing numbers of people are studying for and obtaining CISSP certification. Congratulations on making the decision to follow in their footsteps. If you are willing to tackle the process seriously and do what it takes to obtain the necessary experience and knowledge, you can pass the exam on the first try.

The Ideal CISSP Candidate

The CISSP certification is designed for any individual who is leading, planning, organizing, or controlling the security initiative of an organization. The ideal CISSP candidate is likely to have a four-year college education and have at least five to seven years' experience in one or more of the eight CISSP domains. The most applicable degree is in computer science or a related field. Exam candidates who do not have a four-year college degree must have a minimum of five years of direct full-time security work experience in two or more of the eight domains. (The complete list of approved certifications can be found at www.isc2.org/credential_waiver/default.aspx.)

Don't be lulled into thinking that the CISSP exam is an easy test. Some words of caution are in order:

- The CISSP exam requires the candidate to absorb a substantial amount of material. Both the adaptive exam and the fixed-form exam are considered quite challenging.
- The pass mark is set high, at 700 points out of 1,000. The individual questions are weighted so that harder questions are worth more than easier ones.
- Most of the individuals attempting the exam are familiar with one to three of the eight domains covered on the CISSP exam. Studying for the exam can be overwhelming because there is a lot of material to cover. This book can help you identify and remediate the areas in which you are weak.
- To be eligible for the CISSP exam, students are required to have five years of experience or four years of experience and a college degree.

Put Yourself to the Test

This section prompts you to answer some simple questions to better understand how much work and effort you need to invest to pass the CISSP certification exam. The experience and education you have will dictate how difficult it will be for you to pass the exam.

From the beginning, two things should be clear:

- Any educational background in computer science will be helpful, as will other IT certifications you have achieved.
- Hands-on actual experience is not only essential but required to obtain CISSP certification.

Your Educational Background

Be honest in your answers to the following questions, or you will end up wasting around $700 on an exam you were not ready to take:

- **Do you have a computer science degree?**

  If you have a computer science degree and some fairly sophisticated computer skills, you should have some good basic knowledge needed for three or more of the eight domains. Subject areas such as application development, networking, and database design are a great help.

- **Did you attend some type of technical school or week-long CISSP course?**

  This question applies to low-level or short-term computer courses, many of which are extremely basic or focused in one particular area. Although the CISSP exam is not platform specific, training classes focused on networking, security, hacking, or database design will help you pass the exam.

- **Have you developed any security policies, performed security audits, performed penetration tests, or developed response plans?**

  If yes, you will probably be able to handle about half of the CISSP exam domains.

- **Do you have a photographic memory?**

  If yes, you might have a slim chance of passing simply by reading this book, taking some practice exams, and using the Internet to brush up on the subjects you are weak in. However, the goal here is to gain a real understanding of the material. As a security professional, you might be asked to lead, plan, organize, or control your organization's security operations, and to do so, you'll need a real understanding of how the various technologies and techniques work. Don't cheat yourself or gamble with your career.

The education and requirements given here are by no means absolute. Still, an education can give you a very good grounding in any endeavor; the higher the level of education, the better.

Testing Your Exam Readiness

Whether you attend a training class, form a study group, or study on your own, preparing for the CISSP exam is essential. The exam will cost you more than MG $700, depending on where you are located, and you'll want to do everything you can to make sure you pass on the first try. Reading, studying, and taking practice exams are the best ways to increase your readiness. Remember that two full-length practice exams are provided with this book. Practice exams help in two main ways:

- They highlight weak spots for further study.
- They help you get familiar with the question format. Practicing the questions the way they are asked can help enormously on exam day.

After the Exam

As mentioned earlier in this introduction, after you have passed the exam, you need to earn CPE credits each year to maintain your certification. Your certification will come up for renewal every three years, at which point you'll need to obtain 120 CPE credits or retake the exam. Retaking the exam is not a popular choice. These are some ways to gain CPE credits to keep your certification current:

- Write a book.
- Read a book. (Only one per year can be used for credit.) This will give you a couple of credits—but not enough to keep your certification current.
- Do volunteer work that is approved by (ISC)^2. When you are certified, you can log on to the (ISC)^2 website for more information on volunteer work.

- Attend a training class. Just about any type of technology training class is accepted, as long as it is tied to one of the CISSP domains.
- Teach a training class.
- Attend a college-level security class.

As you can see, the goal here is to help you stay current with changing technology.

Chapter 1, "The CISSP Certification Exam," provides more information about how the exam is structured and describes some effective test-taking strategies.

This page intentionally left blank

CHAPTER 1

The CISSP Certification Exam

Terms you'll need to understand:

- Common body of knowledge (CBK)
- Exam strategy

Techniques you'll need to master:

- Assessing exam requirements
- Determining whether you're ready for the exam
- Using practice questions
- Using your time wisely

Introduction

Welcome to *CISSP Exam Cram*! The aim of this chapter is to help you become prepared for the CISSP exam and understand what to expect when you enter the testing area. Most people do not eagerly anticipate exam taking. The best way to reduce your test-related anxiety is to be fully prepared before you attempt to pass the exam. Taking a few extra steps will help you feel more relaxed and confident when you enter the testing area.

The exam format is different depending on where you take the exam. However, before beginning your studies, you should take a few minutes to make sure you fully understand the CISSP exam process. You don't want to wait until the day of the exam to figure out what you will face. Reviewing these details now will help you concentrate on the exam so that you aren't worried about how much time you have to answer each question. Finally, mastering a few basic exam-taking skills should help you recognize—and perhaps even overcome—some of the tricks or unusual verbiage you're bound to find on the exam.

In addition to reviewing the exam environment, this chapter describes some proven exam-taking strategies that you can use to your advantage.

Assessing Exam Readiness

Before you rush out and sign up for the CISSP exam, check out the $(ISC)^2$ website (www.ISC2.org) and review the CISSP certification requirements. To be eligible for CISSP certification, you must qualify for and meet two separate requirements:

- **Examination**: You must submit the examination fee and assert that you possess a minimum of five years of professional experience in the information security field or four years plus a college degree. (The information you provide is subject to audit and verification.) You must also review and sign the Candidate Agreement, stating that you will legally commit to adhere to the CISSP Code of Ethics, and answer several questions regarding your criminal history and background.
- **Certification**: You must pass the exam with a score of 70% (or 700 points out of 1000), submit a completed and executed Endorsement Form, and, in some cases, pass a verification audit regarding your professional experience.

When you are confident that you meet these requirements, you can continue with your studies. To be fully prepared for the exam, I recommend that you read this entire book, review the practice questions, and review the additional resources identified in each chapter. After you read the book and test yourself with the questions and practice exams, you will have a good idea of whether you are ready to take the real exam.

Be aware that the CISSP exam is difficult and challenging; therefore, this book shouldn't be your only vehicle for CISSP study. The CISSP exam is based on the Common Body of Knowledge (CBK). The CBK is a collection of the subjects and items that all the topics on the exam are pulled from. You can read more at https://www.isc2.org/Certifications/CBK.

Many companies offer training classes to help you review the material and prepare for the exam. Because of the breadth and depth of knowledge needed to pass the CISSP exam, be sure to use plenty of study materials and use this book to help gauge your strengths and weaknesses. The (ISC)^2 website is a good place to find additional study material, and so are the "Need to Know More?" sections in the chapters of this book.

Exam Topics

Every three years, (ISC)^2 updates the CISSP exam topics. The 2021 version of the exam includes the following domains:

Domain 1: Security and Risk Management

Domain 2: Asset Security

Domain 3: Security Architecture and Engineering

Domain 4: Communication and Network Security

Domain 5: Identity and Access Management (IAM)

Domain 6: Security Assessment and Testing

Domain 7: Security Operations

Domain 8: Software Development Security

With each update to the exam, (ISC)^2 rewords topics, reorganizes topics, and adds new topics. The reorganization of topics between or within domains does not have a significant impact on prep or study. However, you do need to be familiar with the new and reworded topics. The "Domain Refresh" guide is the best place to learn about the changes in the exam from one version to another; see https://www.isc2.org/-/media/ISC2/Certifications/Domain-Refresh/CISSP-Domain-Refresh.ashx?la=en&hash=73FF18379098B1480D22A174BF7BB544E83237E9.

Taking the Exam

When you arrive at the testing center, you need to sign in. You will be asked to show your exam confirmation and photo identification. You cannot take the exam without a photo ID and your exam confirmation number. After you've signed in, you can find a seat, get comfortable, and wait for the exam to begin.

The exam is completely closed book. In fact, you will not be permitted to take any study materials into the testing area; you may be given a scratch pad to use that must be returned at the completion of the exam.

The biggest change from previous versions of the test is that the original CISSP exam was a paper-based, bubble-sheet test consisting of 250 questions to be completed in a six-hour time window. Today the exam is electronic and is very similar to CompTIA exams and those given by ISACA. (ISC)^2 now offers an adaptive test, called CISSP Computer Adaptive Test (CISSP-CAT). The CISSP-CAT is used only for the English version of the exam. For non-English versions, a 250-question, non-adaptive six-hour version is used.

If you are taking the English (CISSP-CAT) version of the exam, your exam strategy will be different than with the fixed length exam. As an example, the CISSP-CAT will not allow you to revisit a question. Once you answer a question you cannot go back.

You will view a minimum of 100 questions and a maximum of 150. Of the first 100 questions, 75 are graded and count toward your score, and the other 25—which are scattered randomly throughout the first 100 questions—are ungraded questions that are used for evaluation.

When you reach the 100th question, the system evaluates the probability that you will achieve a passing score. If the system estimates that your pass potential is 95% or higher, the test ends with a passing grade. If the system estimates that your failure potential is 95% or higher, the test ends with a failing grade. If the system cannot make this pass/fail determination at question 100, it reevaluates the potential again after each question until you reach the 150th question. You are then assessed only on the last 75 graded questions. This means that as you answer question 101, the first graded question is discarded and replaced with question 101. Then as you answer question 102, the second originally graded question is discarded and replaced with question 102, and so forth.

One big change is that with the CISSP-CAT you cannot revisit previous questions. You get only one chance to view a question and select an answer. If you skip a question, it is marked as incorrect. Therefore, guessing is a better strategy than skipping. You should always attempt to eliminate question options from consideration and then select your answer from the remaining options.

Non-English versions of the test contain 250 questions. Of these, 25 questions are for research purposes, and only the other 225 questions are actually scored for certification.

The exam questions are developed by an $(ISC)^2$ committee and are frequently updated and changed. Make sure to look for keywords such as *not*, *least*, and *most.* Or as an example a question may ask about configuration management but show some incorrect answers that discuss change management. Missing one word or confusing one word for another on the exam can make a big difference.

Examples of CISSP Test Questions

This section describes what CISSP test questions look like and how they must be answered. The following are some examples of the various CISSP test question formats. Following each example is a brief summary of each potential answer and why it is either right or wrong.

Multiple-Choice Question Format

Each multiple-choice exam question requires you to select a single answer from the given choices. To answer this type of question, click the letter or text of one answer. In some cases, more than one answer might appear correct; you must determine which one is most correct.

1. What is the most widely used device to control physical access?

   ○ **A.** Chain

   ○ **B.** Lock

   ○ **C.** Alarm

   ○ **D.** Firewall

Drag and Drop Question Format

For a drag and drop question, you must move one or more correct answers from a pool of possible answers into the correct answers area. To answer this type of question, simply click, drag, and drop the correct answers from the "Possible Answers" section to the "Correct Answers" box.

1. Which of the following are examples of asymmetric encryption?

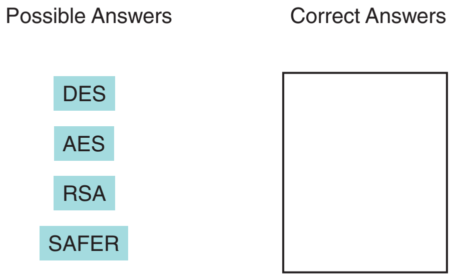


FIGURE 1.1 **Drag and Drop Question**

Hotspot Question Format

For a hotspot exam question, you must click on the correct area of a diagram—a hotspot—to answer a question.

1. When designing network controls, which would be the proper location for a firewall to protect the DMZ?

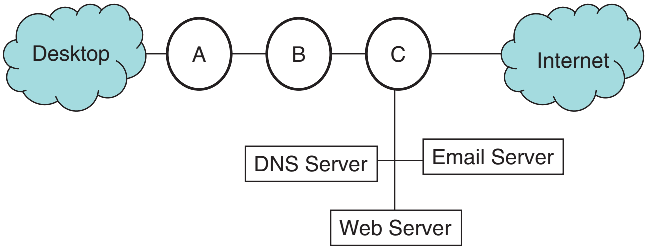


FIGURE 1.2 **Hotspot Question**

Answer to Multiple-Choice Question

1. **B.** Locks are the devices most commonly used to control physical access. Locks have been used since the time of the Egyptians. Answer A is incorrect because chains are not the devices most commonly used for physical access control. Answer C is incorrect because alarms don't prevent access; they only inform you that possible unauthorized access has occurred. Answer D is incorrect because a firewall is used to control logical access.

Answer to Drag and Drop Question

1. **RSA.** RSA is the only example of asymmetric encryption. DES, AES, and SAFER are all examples of symmetric encryption. In this case, you should drag and drop only "RSA" into the "Correct Answers" box.

Answer to Hotspot Question

1. **C.** To answer the question, hold the mouse cursor over the area on the diagram that you want to choose as your answer. All available areas will light up (A, B, or C in this example), and you must click on the one you believe is correct. In this case, you'd want to deploy a firewall where item C is located between the internal network and the Internet.

Question-Handling Strategies

Because of the way that multiple-choice CISSP exam questions are structured, many times one or two of the answers will be obviously incorrect and two of the answers will be plausible. Take the time to reread the question. Words such as *sometimes*, *not*, *always*, and *best* can make a big difference when choosing the correct answer. Unless the answer leaps out at you, begin the process of answering by eliminating the answers that are most obviously wrong.

Almost always, at least one answer out of the possible choices for a question can be eliminated immediately because it matches one of these conditions:

- The answer does not apply to the situation.
- The answer describes a nonexistent issue, an invalid option, or an imaginary state.

After you eliminate all answers that are obviously wrong, you can apply your retained knowledge to eliminate further answers. Look for items that sound correct but refer to actions, commands, or features that are not present or not available in the situation that the question describes.

If you're still faced with a blind guess among two or more potentially correct answers, reread the question. Try to picture how each of the possible remaining answers would alter the situation.

Only when you've exhausted your ability to eliminate answers but remain unclear about which of the remaining possibilities is correct should you guess at an answer. An unanswered question offers you no points, but guessing gives you at least some chance of getting a question right. Just don't be too hasty when making a blind guess!

Mastering the Inner Game

Knowledge breeds confidence, and confidence breeds success. If you study the materials in this book carefully and review all the practice questions at the end of each chapter, you should become aware of those areas where additional learning and study are required.

ExamAlert

You will be expected to understand CISSP terminology on the exam. You need to understand the terms that might be used, and you also need to be able to apply them in the context provided in the test questions. As an example, the exam might talk about intrusion detection, but a specific question might address physical intrusion detection or logical intrusion detection.

After you've worked your way through this book, take the practice exams at the end of the book. Taking these practice exams will provide a reality check and help you identify areas to study further. Make sure you follow up and review materials related to the questions you missed on the practice exams before taking the real exam. Only when you've covered that ground and feel comfortable with the whole scope of the practice exams should you set an exam appointment. It's advisable to score 90% or better before you attempt the real exam. Until you hit that magic number, you should obtain additional practice tests and keep trying.

ExamAlert

Armed with the information in this book and with the determination to augment your knowledge, you should be able to pass the certification exam. However, you need to work at it, or you'll spend the exam fee more than once before you finally pass. If you prepare seriously, you should do well. I am confident that you can do it!

Need to Know More?

Passing the CISSP exam: cybersecurityventures.com/how-to-pass-the-cissp-exam-top-10-tips-from-a-chief-risk-officer/

(ISC)^2 CISSP certification: www.isc2.org/cissp/default.aspx

CHAPTER 2
Understanding Asset Security

Terms you'll need to understand:

- Confidentiality
- Integrity
- Availability
- Personally identifiable information
- Information lifecycle management (ILM)
- Data retention
- Data classification
- Data destruction
- Data remanence

Techniques you'll need to master:

- Proper methods for destruction of data
- Development of documents that can aid in compliance with local, state, and federal laws
- The implementation of encryption and its use for the protection of data
- How to use data security controls

Introduction

Understanding asset security is a key requirement of a CISSP candidate. Asset security addresses the controls needed to protect data throughout its lifecycle, from the point of creation to the end of its life. Data protection controls must be implemented to ensure that information is adequately protected during each lifecycle phase. This chapter starts by reviewing the basic security principles of confidentiality, integrity, and availability and moves on to data management and governance.

The CISSP exam requires you to understand data security and how information is protected while it is in transit, in storage, and at rest. You must understand that protection of data is much more important today than it was years ago because data is no longer isolated in standalone servers. Today data often resides in the cloud; data can also be found on laptops, in RAID arrays, or even in paper form. Regardless of its storage location, data must have adequate protection and must be properly disposed of at the end of its useful life.

Basic Security Principles

Confidentiality, integrity, and availability (CIA) are the basic building blocks of any good security program. When defining the goals for network, asset, information, and/or information system security, the term *CIA triad* is commonly used to refer to these concepts. Although the abbreviation CIA might not be as intriguing as the U.S. government's spy organization, it is a concept that security professionals must know and understand.

Confidentiality addresses the secrecy and privacy of information and preventing unauthorized persons from viewing sensitive information. A number of controls are used in the real world to protect the confidentiality of information, such as locked doors, armed guards, and fences. Administrative controls that can enhance confidentiality include the use of information classification systems, such as requiring sensitive data be encrypted. For example, news reports have detailed several large-scale breaches in confidentiality as a result of corporations misplacing or losing laptops, data, and even backup media containing customer account, name, and credit information. The simple act of encrypting this data could have prevented or mitigated the damage. Sending information in an encrypted format denies attackers the opportunity to intercept and sniff plaintext information. The Organization for Economic Co-operation and Development (OECD) specifies that personal data should be limited and provides guidelines for ensuring privacy and confidentiality.

Integrity has to do with accuracy of information and offering users a high degree of confidence that the information they are viewing has not been tampered with. The integrity of data must be protected while the data is in storage, at rest, and in transit. It is important to ensure that unauthorized users have not made any changes and authorized users have not made inappropriate changes. Data in storage can be protected through the use of access controls and audit controls. Cryptography and hashing algorithms can enhance this protection. Cryptography tools include programs such as HashTools, HashCheck, and PowerShell. Likewise, integrity in transit can be ensured primarily through the use of these tools in combination with protocols and frameworks such as public key infrastructure (PKI), digital signatures, and asymmetric algorithms.

Availability refers to the need for information and systems to be available when needed. Although many people think of availability only in electronic terms, availability also applies to physical access. If, at 2 a.m., you need access to backup media stored in a facility that allows access only from 8 a.m. to 5 p.m., you have an availability problem. Availability in the world of electronics can manifest in many ways. 24x7 access to a backup facility does little good if there are no updated backups to restore from and the original copies have been encrypted with ransomware.

Keeping backups is a good way to ensure availability. A backup provides a copy of critical information that can be reinstated if data is destroyed or equipment fails. Using failover equipment is another way to ensure availability. Systems such as redundant arrays of independent disks (RAID) and redundant sites (which can be hot, cold, or warm sites) are two other examples. Disaster recovery is tied closely to availability because it's all about getting critical systems up and running quickly.

Which part of the security triad is considered most important? It depends. In different organizations with different priorities, one part might be more important than the other two. For example, your local bank might consider integrity the most important, an organization responsible for data processing might see availability as the primary concern, and an organization such as a healthcare records clearing agency might value confidentiality the most.

Even though this book refers to the triad as CIA, others might refer to it as AIC or as CAIN (where the *N* stands for *nonrepudiation*).

Security management does not stop at CIA. These are but three of the core techniques that apply to asset security. True security requires defense in depth. In reality, many techniques are required to protect the assets of an organization; take a moment to look over Figure 2.1.

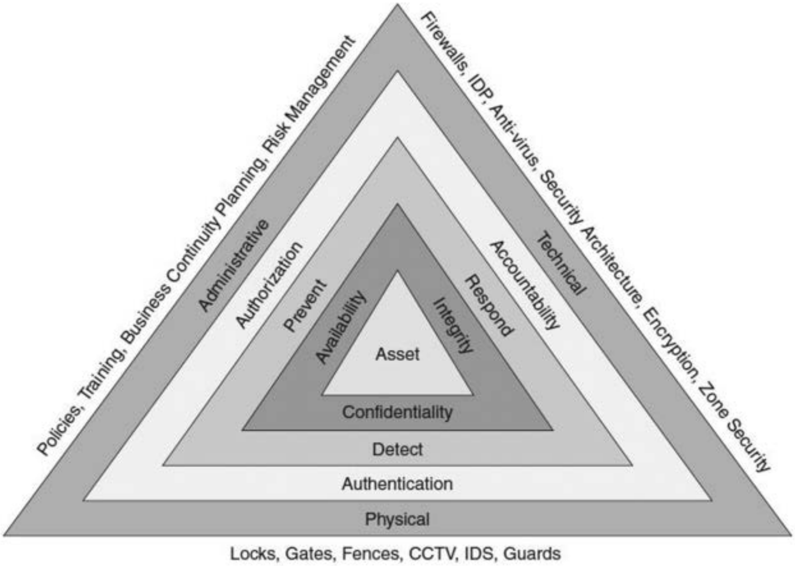

Policies, Training, Business Continuity Planning, Risk Management
Firewalls, IDP, Anti-virus, Security Architecture, Encryption, Zone Security
Administrative
Technical
Authorization
Accountability
Prevent
Respond
Availability
Integrity
Asset
Confidentiality
Detect
Authentication
Physical
Locks, Gates, Fences, CCTV, IDS, Guards

FIGURE 2.1 **Asset Protection Triad**

Data Management: Determining and Maintaining Ownership

Data management is not easy, and it has in fact become more complex recently. Years ago, people only had to be concerned with paper documents, and control might have only meant locking a file cabinet. Today, electronic data might be found on thumb drives, SAN storage arrays, laptop hard drives, mobile devices, and in a public cloud.

Data Governance Policies

Generally, you can think of policies as high-level documents developed by management to transmit the guiding strategy and philosophy of management to employees. A data governance policy is a documented set of specifications for the guarantee of approved management and control of an organization's digital assets and information.

Data governance programs generally address the following types of data:

- Sets of master data
- Metadata

- Sensitive data
- Acquired data

Such specifications can involve directives for business process management (BPM) and enterprise risk planning (ERP), as well as security, data quality, and privacy. The goals of data governance include the following:

- Establish appropriate responsibility for the management of data
- Improve ease of access to data
- Ensure that once data is located, users have enough information about the data to interpret it correctly and consistently
- Improve the security of data, including confidentiality, integrity, and availability

Issues to consider include the following:

- **Cost**: This can include the cost of providing access to the data as well as the cost of protecting it.
- **Ownership**: This includes concerns about who owns the data or who might be a custodian. For example, you might be the custodian of 50 copies of Microsoft Windows Server 2019, yet the code is owned by Microsoft. Users pay for a software license and not ownership of the software itself, and they typically have only the compiled .exe file and not the source code for a program.
- **Liability**: This refers to the financial and legal costs an organization would bear if data were lost, stolen, or hacked.
- **Sensitivity**: This includes issues related to the sensitivity of data that should be protected against unwarranted disclosure (for example, Social Security numbers, date of birth, medical history information).
- **Ensuring law/legal compliance**: This includes items related to legal compliance. For example, you must retain tax records for a minimum number of years, but you might be required to retain personally identifiable information (PII) customer information for only the time it takes to process a single transaction.
- **Process**: This includes methods and tools used to transmit or modify data.

Roles and Responsibilities

Data security requires responsibility. A clear division of roles and responsibility is a tremendous help when dealing with any security issues. Everyone should be subject to the organization's security policy, including employees, management, consultants, and vendors. Specific roles have unique requirements. Some key players and their responsibilities are as follows:

- **Data owner**: Because senior management is ultimately responsible for data and can be held liable if it is compromised, the data owner is usually a member of senior management or the head of that department. The data owner is responsible for setting the security classification of the data. The data owner can delegate some day-to-day responsibility.

- **Data custodian**: The data custodian, who is usually a member of the IT department, does not decide what controls are needed but implements controls on behalf of the data owner. Other responsibilities include handling the day-to-day management of data, controlling access, adding and removing privileges for individual users, and ensuring that the proper controls have been implemented.

- **Information security steering committee**: Individuals on this committee are from various levels of management and represent the various departments of the organization. They meet to discuss and make recommendations on security issues.

- **Senior management**: These individuals are ultimately responsible for the security practices of the organization. Senior management might delegate day-to-day responsibility to another party or someone else but cannot delegate overall responsibility for the security of the organization's data.

- **Security advisory group**: These individuals are responsible for reviewing security issues with the chief security officer and are also responsible for reviewing security plans and procedures.

- **Chief security officer**: This individual is responsible for the day-to-day security of the organization and its critical assets.

- **Users**: End users in an organization have responsibilities: They must comply with the requirements laid out in policies and procedures.

- **Developers**: These individuals develop code and applications for the organization. They are responsible for implementing the proper security controls within the programs they develop.

- **Auditor**: This individual is responsible for examining the organization's security procedures and mechanisms. The auditor must provide an independent and objective opinion about the effectiveness of the organization's security controls. How often this process is performed depends on the industry and its related regulations. For example, the healthcare industry in the United States is governed by Health Insurance Portability and Accountability Act (HIPAA) regulations and requires yearly reviews.

ExamAlert

The CISSP exam might test you on the concept that data access does not extend indefinitely. It is not uncommon for an employee to gain more and more access over time while moving to different positions within a company. However, this type of poor management can endanger an organization. When employees are terminated, data access should be withdrawn. If unfriendly termination is known in advance, access should be terminated as soon as possible to reduce the potential for damage.

Data Ownership

Every data object within an organization must have an owner. Any object without a data owner will be left unprotected. The process of assigning a data owner and set of controls to information is known as *information lifecycle management* (*ILM*). ILM is the science of creating and using policies for effective information management. ILM includes every phase of a data object, from its creation to its end. ILM applies to any and all information assets.

ILM is focused on fixed content or static data. While data may not stay in a fixed format throughout its lifecycle, there are times when it is static. For example, after this book has been published, it will stay in a fixed format until the next edition is released.

For the purposes of business records, the lifecycle process includes five phases:

1. Creation and receipt
2. Distribution
3. Use
4. Maintenance
5. Disposition

Data Custodians

Data custodians are responsible for the safe custody, transport, and storage of data and the implementation of business rules. This can include the practice of due care and the implementation of good practices to protect intellectual assets such as patents or trade secrets. Some common responsibilities for a data custodian include the following:

- **Data owner identification**: A data owner must be identified and known for each data set and must be formally appointed. Many times data owners do not know that they are data owners and do not understand the role and its responsibilities. In many organizations the data custodian or IT department by default assumes the role of data owner.
- **Data controls**: Access to data is authorized and managed. Adequate controls must be in place to protect the confidentiality, integrity, and availability of the data. This includes administrative, technical, and physical controls.
- **Change control**: A change control process must be implemented so that change and access can be audited.
- **End-of-life provisions or disposal**: Controls must be in place so that when data is no longer needed or is not accurate, it can be destroyed in an approved method.

Data Documentation and Organization

Organizing and structuring data can help ensure that that it is better understood and interpreted by users. Data documentation should detail the following:

- Data context
- Methodology of data collection
- Data structure and organization
- Validity of data and quality assurance controls
- Data manipulations through data analysis from raw data
- Data confidentiality, access, and integrity controls

Data Warehousing

A *data warehouse* is a database that contains data from many other databases. It allows for trend analysis and marketing decisions through data analytics (discussed later in this chapter). Data warehousing enables a strategic view. Because of the amount of data stored in one location, data warehouses are tempting targets for attackers who can comb through and discover sensitive information.

Data Mining

Data mining is the process of analyzing data to find and understand patterns and relationships about the data (see Figure 2.2). Many things must be in place for data mining to occur, including multiple data sources, access, and warehousing. Data becomes information, information becomes knowledge, and knowledge becomes intelligence through a process called *data analytics*, which is simply examination of data. *Metadata* is best described as being data about data. For example, the number 212 has no meaning by itself. But qualifications can be added to give it meaning; for example, if you learn that 212 is an area code, then you understand that the number represents an area code in Manhattan.

Organizations treasure data and the relationships that can be deduced between individual data elements. These relationships can help companies understand their competitors and the usage patterns of their customers and can help them target their marketing. For example, diapers may be located in the back of the store, near the beer case, because data mining shows that after 10 p.m., more men than women buy diapers, and they tend to buy beer at the same time.

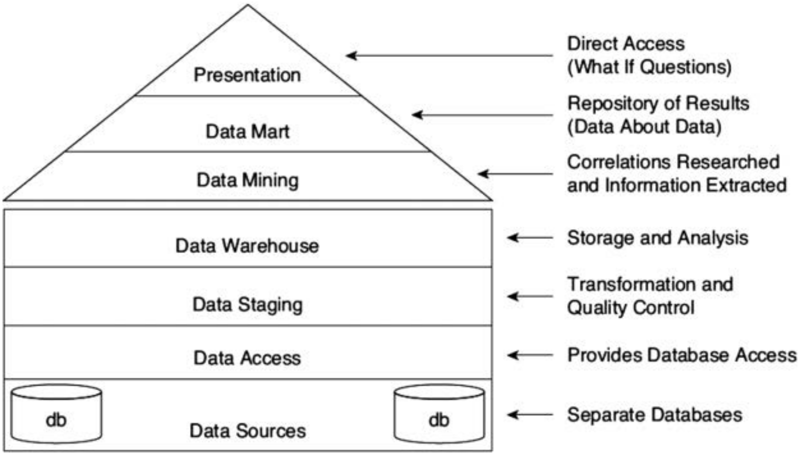


FIGURE 2.2 Data Mining

Knowledge Management

Knowledge management seeks to make intelligent use of the data in an organization by applying wisdom to it. This involves turning data into intelligence through analytics by tying together databases, document management, business processes, and information systems. The result is a huge store of data that can be mined to extract knowledge using artificial intelligence techniques.

There are three main approaches to knowledge extraction:

- **Classification**: This approach is used to discover patterns and can be used to reduce large databases to only a few individual records or data marts. (Think of data marts as small slices of data from a data warehouse.)
- **Probabilistic**: This approach is used to permit statistical analysis, often in planning and control systems or in applications that involve uncertainty.
- **Statistical**: This is a number-crunching approach in which rules are constructed to identify generalized patterns in the data.

Data Standards

Data standards provide consistent meaning to data shared among different information systems, programs, and departments throughout a product's lifecycle. Data standards are part of any good enterprise architecture. Data standards make data much easier to use. For example, say that you get a new 850-lumen flashlight that requires two AA batteries. You don't need to worry about what brand of batteries to buy as all AA batteries are manufactured to the same size and voltage standards.

Tip

To see an example of a data standard, check out FDA Resources for Data Standards, at www.fda.gov/industry/fda-resources-data-standards. The FDA provides this site to ensure that common data standards are used throughout the FDA.

Data Lifecycle Control

Data lifecycle control is a policy-based approach to managing the flow of an information system's data throughout its lifecycle from the point of creation to the point at which it is out of date and is destroyed or archived.

Data Audits

After all the tasks discussed so far in this chapter have been performed, the organization's security management practices need to be evaluated periodically. This is accomplished by means of an *audit process*. The audit process can be used to verify that each individual's responsibility is clearly defined. Employees should know their accountability and their assigned duties. Most audits follow a code or set of documentation. For example, financial audits can be performed using the Committee of Sponsoring Organizations of the Treadway Commission (COSO). IT audits typically follow the Information Systems Audit and Control Association (ISACA) Control Objectives for Information and Related Technology (COBIT) framework. COBIT is designed around four domains:

- Plan and organize
- Acquire and implement
- Deliver and support
- Monitor and evaluate

Although the CISSP exam will not expect you to understand the inner workings of COBIT, you should understand that it is a framework that helps provide governance and assurance. COBIT was designed for performance management and IT management, and it is considered a system of best practices. COBIT was created by the ISACA and the IT Governance Institute (ITGI) in 1992.

Auditors can use COBIT, and this framework is also useful for IT users and managers designing controls and optimizing processes.

Audits make it possible to verify that the controls put in place are working, that the policies that were written are being followed, and that the training provided to employees actually works. To learn more about COBIT, see www.isaca.org/cobit/. Another set of documents that can be used to benchmark the infrastructure is the ISO 27000 family of standards; for details, see www.27000.org.

Data Storage and Archiving

Organizations have a never-ending need for increased storage. Whereas thumb drives were revolutionary and initially provided in the range of 10 MB of storage, today they can provide terabytes of storage. Data storage options in organizations typically include the following:

- Network attached storage (NAS)
- Storage area network (SAN)
- Cloud

Organizations should fully define their security requirements for data storage before deploying a technology. For example, NAS devices are small, easy to use, and can be implemented quickly, but physical security is a real concern, as is implementing strong controls over the data. A SAN can be implemented with much greater security than can a NAS. Cloud-based storage offers yet another option but also presents concerns, including the following:

- Is it a private or public cloud?
- Does it use physical or virtual servers?
- How are the servers provisioned and decommissioned?
- Is the data encrypted and, if so, what kind of encryption is used?
- Where is the data actually stored?
- How is the data transferred (data flow)?
- Where are the encryption keys kept?
- Are there co-tenants?

Keep in mind that storage integration also includes securing virtual environments, services, applications, appliances, and equipment that provide storage.

The Storage Networking Industry Association (SNIA) defines a SAN as "a data storage system consisting of various storage elements, storage devices, computer systems, and/or appliances, plus all the control software, all communicating in efficient harmony over a network." A SAN appears to the client OS as a local disk or volume that is available to be formatted and used locally as needed.

For the CISSP exam, it is important to know the following terms related to SANs:

- **Virtual SAN**: A virtual SAN (VSAN) is a SAN that offers isolation for devices that are physically connected to the same SAN fabric. The use of VSANs is sometimes called *fabric virtualization*. VSANs were developed to support independent virtual fabrics on a single switch. VSANs improve consolidation and simplify management by allowing for more efficient SAN utilization. A VSAN allows a resource on any individual VSAN to be shared by other users on a different VSAN without requiring the SAN fabrics to be merged.
- **Internet Small Computer System Interface (iSCSI)**: iSCSI is a SAN standard used for connecting data storage facilities and allowing remote SCSI devices to communicate. Many see it as a replacement for Fibre

Channel because it does not require any special infrastructure and can run over existing IP LAN, MAN, or WAN networks.

- **Fibre Channel over Ethernet (FCoE)**: FCoE, a transport protocol that is similar to iSCSI, can operate at speeds of 10 Gbps and rides on top of the Ethernet protocol. While it is fast, it has a disadvantage in that it is non-routable. By contrast, iSCSI is routable because it operates higher up the stack, on top of the TCP and UDP protocols.
- **Host bus adapter (HBA) allocation**: A host bus adapter is used to connect a host system to an enterprise storage device. HBAs can be allocated either through soft zoning or persistent binding. Soft zoning is more permissive, whereas persistent binding decreases address space and increases network complexity.
- **LUN masking**: LUN masking is implemented primarily at the HBA level. It is a system that makes LUNs available to some HBAs but not to others. LUN masking implemented at this level is vulnerable to any attack that compromises the local adapter.
- **Location redundancy**: Location redundancy makes contents accessible from more than one location. An extra measure of redundancy can be provided by means of a replication service so that data is available even if the main storage backup system fails.
- **Secure storage management and replication**: Secure storage management and replication systems are designed to allow an organization to manage and handle all its data in a secure manner with a focus on the confidentiality, integrity, and availability of the data. A replication service allows the data to be duplicated in real time so that additional fault tolerance is achieved.
- **Multipath solutions**: Enterprise storage multipath solutions reduce the risk of data loss or lack of availability by setting up multiple routes between a server and its drives. The multipath software maintains a listing of all requests, passes them through the best possible path, and reroutes communication if a path fails.
- **SAN snapshots**: SAN snapshot software is typically sold with SAN solutions and offers a way to bypass typical backup operations. The snapshot software has the ability to temporarily stop writing to a physical disk and then make a point-in-time backup copy. Snapshot software is typically fast and makes a copy quickly, regardless of the drive size.

- **Data de-duplication (DDP)**: Data de-duplication is the process of removing redundant data to improve enterprise storage utilization. Redundant data is not copied. It is replaced with a pointer to the one unique copy of the data. Only one instance of redundant data is retained on the enterprise storage medium, such as disk or tape.

Data Security, Protection, Sharing, and Dissemination

Data security involves protecting data from unauthorized activity by authorized users and from access by unauthorized users. Although laws differ depending on which country an organization is operating in, organizations must make the protection of personal information in particular a priority. To understand the importance of data security, consider that according to the Privacy Rights Clearinghouse (www.privacyrights.org), the total number of records containing sensitive personal information accumulated from security breaches in the United States between January 2005 and December 2020 is 11,717,011,063.

The international standard ISO/IEC 17799 covers data security on a global level. ISO 17799 makes clear the fact that all data should have a data owner and data custodian so that it is clear who is responsible for securing and protecting access to that data.

An example of a proprietary international information security standard is the Payment Card Industry Data Security Standard (PCI-DSS). PCI-DSS sets standards for any entity that handles cardholder information for credit cards, prepaid cards, and POS cards. PCI-DSS comprises 6 control objectives and 12 requirements:

1. Build and maintain a secure network.

   Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

   Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

2. Protect cardholder data.

   Requirement 3: Protect stored cardholder data.

   Requirement 4: Encrypt transmission of cardholder data across open, public networks.

3. Maintain a vulnerability management program.

   Requirement 5: Use and regularly update antivirus software.

   Requirement 6: Develop and maintain secure systems and applications.

4. Implement strong access control measures.

   Requirement 7: Restrict access to cardholder data based on business need to know.

   Requirement 8: Assign a unique ID to each person with computer access.

   Requirement 9: Restrict physical access to cardholder data.

5. Regularly monitor and test networks.

   Requirement 10: Track and monitor all access to network resources and cardholder data.

   Requirement 11: Regularly test security systems and processes.

6. Maintain an information security policy.

   Requirement 12: Maintain a policy that addresses information security.

Privacy Impact Assessment

Another approach for organizations seeking to improve their protection of personal information is to develop an organization wide policy based on a *privacy impact analysis* (*PIA*). A PIA should determine the risks and effects of collecting, maintaining, and distributing PII in electronic-based systems. The PIA should be used to evaluate privacy risks and ensure that appropriate privacy controls exist. Existing data controls should be examined to verify that accountability is present and that compliance is built in every time new projects or processes are planned to come online. The PIA must include a review of the following items as they adversely affect the CIA of privacy records:

- **Technology**: Any time new systems are added or modifications are made, reviews are needed.

- **Processes**: Business processes change, and even though a company might have a good change policy, the change management system might overlook personal information privacy.

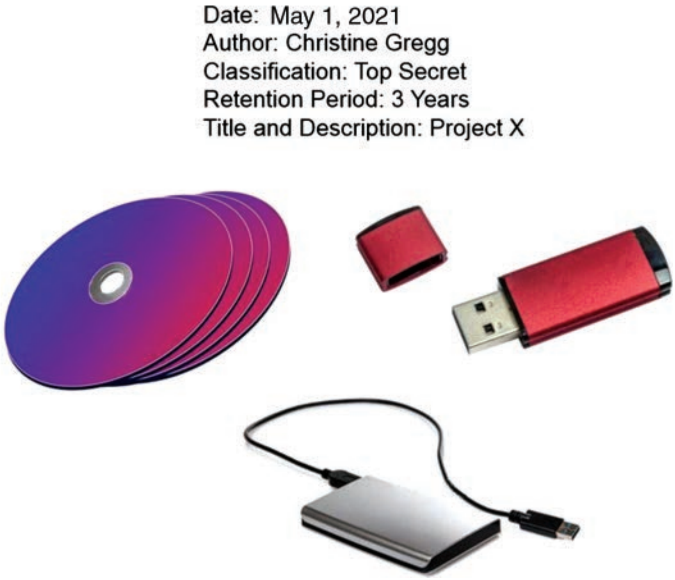
- **People**: Companies change employees and others with whom they do business. Any time business partners, vendors, or service providers change, the impact of the change on privacy needs to be reexamined.

Privacy controls tend to be overlooked for the same reason many security controls are overlooked. Management might have a preconceived idea that security controls will reduce the efficiency or speed of business processes. To overcome such barriers, senior management must make a strong commitment to protection of personal information and demonstrate its support. Risk assessment activities aid in the process by informing stakeholders of the actual costs related to the loss of personal information of clients and customers. These costs can include fines, lawsuits, lost customers, reputation, and, ultimately, the viability of the company.

Information Handling Requirements

Organizations handle large amounts of information and should have policies and procedures in place that detail how information is to be stored. You can think of policies as high-level documents and procedures as step-by-step instructions. Many organizations are in industries that are subject to regulatory standards that detail how and how long information must be retained.

One key concern with storage is to ensure that media is appropriately labeled. Media should be labeled so that the data librarian or individual in charge of media management can identify the media owner, when the content was created, the classification level, and when the content is to be destroyed. Figure 2.3 shows an example of appropriate media labeling.



Date: May 1, 2021
Author: Christine Gregg
Classification: Top Secret
Retention Period: 3 Years
Title and Description: Project X

FIGURE 2.3 **Data Labeling**

Note

Unless you're a classic car enthusiast like I am, it might have been a while since you have seen a working in-dash cassette player. Technology changes, and the requirement to be able to read and access old media is something to consider. Stored media—including older options such as cassette tapes, laser discs, Zip drives, and PATA hard drives—must be readable in order to be useful.

Record Retention and Destruction

All data has a lifetime. Eventually data should either be purged, released, or unclassified. Record retention involves maintaining important information as long as it is needed and destroying or declassifying it when it isn't needed.

Some record retention guidelines are legally mandated by governments. For example, companies typically cannot legally delete potential evidence after a lawsuit is filed and must maintain these assets and records until the court case has concluded. In addition, the JFK Records Act was a record retention act put in place to eventually declassify all records dealing with the assassination of President John F. Kennedy and make these records public by 2018.

The steps in creating a record retention policy include the following:

1. Understand the business needs and any existing regulatory requirements.
2. Classify assets or records.
3. Create retention periods and specify data destruction methods.
4. Develop the policy and determine the impact should the policy not be followed.
5. Conduct training, education, and awareness about the policy.
6. Audit the policy and procedures.
7. Review the policy and procedures regularly.
8. Record the implementation and audit results.

ExamAlert

Two key aspects of data retention are categorization and classification. *Categorization* defines the impact should the asset be exposed. *Classification* defines the value. The CISSP exam is likely to test you on your understanding of these terms.

The Problem of Data Disposal

While hard drive size and performance have continued to grow rapidly, most hard drives and thumb drives are still shipped without encryption enabled. This means, for example, that you can take a hard drive from a computer you bought at an auction that will not boot up, plug the drive into another computer, and possibly gain access to the data on the drive. While many of us have used a paper shredder, few have probably ever sanitized a hard drive. Whether your organization is planning to sell old hard drives, give them to charity, or just throw them away, you need to make sure the data on the drives cannot be recovered.

To find out whether organizations are doing a good job of ensuring that their data is unrecoverable, two researchers from MIT bought 158 used hard drives from eBay. Out of these hard drives, 129 drives still functioned, and 69 of these drives contained data that the researchers were able to copy. The data on these drives included personal information, company HR records, medical information, a pharmacy database, and another database containing several thousand credit card numbers.

Data Remanence and Decommissioning

Object reuse must be carefully considered because information may remain on a hard disk or any other type of media. Even when data has been sanitized, there may be some remaining information. *Data remanence* is the residual data that remains after data has been erased from a storage device. *Sanitization* is the process of clearing all identified content such that no data remnants can be recovered. The CISSP exam will expect you to understand the differences between various types of sanitization methods.

Asset disposal must be handled in an approved manner and must be part of the systems development lifecycle. For example, media that has been used to store sensitive or secret information should be physically destroyed. Before systems or data are decommissioned or disposed of, you must understand any existing legal requirements pertaining to records retention. When archiving information, you must consider the method for retrieving the information.

Clearing and purging are two ways to decommission hardware. Zeroization is a type of clearing. Purging is considered a stronger, permanent form of sanitization. Degaussing and drive wiping are types of purging. The details of these methods are as follows:

- **Zeroization**: This process, which is a type of clearing, is usually associated with cryptographic processes. The term was originally used with mechanical cryptographic devices, which would be reset to 0 to prevent anyone from recovering the key. In the electronic realm, *zeroization* involves overwriting the data with zeros. Zeroization is defined in ANSI X9.17. Data may be recoverable with this method.

- **Degaussing**: This process is used to permanently destroy the contents of a hard drive or magnetic media. Degaussing involves using a powerful magnet whose field strength penetrates the media and reverses the polarity of the magnetic particles on the tape or hard disk. After media has been degaussed, it cannot be reused. The only method more secure than degaussing is physical destruction.
- **Drive wiping**: This is the act of overwriting all information on a drive. Drive wiping, which is covered in National Institute of Standards and Technology (NIST) 800-88 and U.S. Department of Defense (DoD) 5200.28, allows a drive to be reused. One form of drive wiping (specified in DoD 5200.28) is overwriting a drive with a special digital pattern through seven passes.

It is common for a storage device to have some remaining amount of information left on it after it has been erased. If the media is going to be reused rather than destroyed, the best practice is to overwrite it with a minimum of seven passes of random ones and zeros.

For information deemed too sensitive, assets such as hard drives, media, and other storage devices may need to be destroyed rather than reused. Destruction, which is the strongest form of sanitization, can include acid baths and physical destruction. If records that are no longer needed are held on a newer non-magnetic drive, such as a solid-state drive (SSD), Curie temperature may be used to heat the drive to the point where it loses its magnetic properties.

ExamAlert

The CISSP exam will expect you to understand the different ways you can dispose of data. One easy way to memorize this is to think of the phrase “Cow, Pig, Sow,” or “CP SOW,” which stands for **c**learing **c**an be recovered, **p**urging is **p**ermanent, **s**anitizing is the **s**ame, **o**verwriting **o**’s, and **w**iping is **w**riting.

Classifying Information and Supporting Asset Classification

Asset classification involves assigning assets to groups, based on a number of common characteristics. Before you can classify assets, however, you must know what you have. You determine this through an asset inventory. Modern organizations rely heavily on asset inventories and the use of tools such as Asset

Panda, AssetCloud, and ManagerPlus. These applications (and others) assist organizations in identifying, locating, and classifying their assets. The components of an asset inventory include items such as the following:

- Asset name
- Asset location
- Asset cost
- Asset owner
- Asset classification
- Data protection level required

The standard or process used to classify and manage assets is typically left to the discretion of an individual organization. Two things to consider are the size and structure of the organization and what is considered common in the country or industry in which the organization operates. Regardless of the particular approach, the asset classification process consists of five steps:

1. Create an asset inventory.
2. Assign ownership.
3. Classify based on value.
4. Protect based on classification.
5. Assess and review.

Note

To memorize the asset classification process for the CISSP exam, think of CACPA, which rhymes with "Cat Paw" and refers to the steps listed above.

In addition to protecting its assets, an organization must protect the information maintained in those assets that is proprietary or confidential. Data classification is a useful way to rank an organization's informational assets. A well-planned data classification system makes it easy to store and access data. It also makes it easier for users of data to understand the importance of the data. For example, if an organization has a clean desk policy and mandates that company documents, memos, and electronic media not be left on desks, it can change people's attitudes about the value of that information. However, whatever data classification system is used, it should be simple enough that all employees can understand it and execute it properly.

Data Classification

The two most common data classification schemes are military and public. Organizations store and process so much electronic information about their customers and employees that it's critical for them to take appropriate precautions to protect this information. The responsibility for the classification of data lies with the data owner. Both military and private data classification systems accomplish this task by placing information into categories and applying labels to data and clearances to people who access the data.

The first step of the data classification process is to assess the value of the information in question. When the value is known, it becomes much easier to determine what resources should be used to protect the data. It would not make sense, for example, to spend a lot of resources protecting something with a very small value. Instead, data that requires more protection gets it, and funds are not wasted protecting data that does not need it.

Each level of classification established should have specific requirements and procedures. The military and commercial data classification models have predefined labels and levels for both users and data. Clearance is assigned to users, and labels are assigned to data. When an organization decides which model to use, it can evaluate data placement based on criteria such as the following:

- Data value
- Data age
- Laws pertaining to data
- Regulations pertaining to disclosure
- Replacement cost

Regardless of which model is used, the following questions will help determine the proper placement of the information:

- Who owns the asset or data?
- Who controls access rights and privileges?
- Who approves access rights and privileges?
- What level of access is granted to the asset or data?
- Who currently has access to the asset or data?

Classification of data requires several steps:

1. Identify the data custodian.
2. Determine the criteria used for data classification.
3. Task the owner with classifying and labeling the information.
4. Identify any exceptions to the data classification policy.
5. Determine security controls to be applied to protect each category of information.
6. Specify a sunset policy or an end-of-life policy and detail in a step-by-step manner how data will be reclassified or declassified. Reviews specifying retention and end-of-life should occur at specific periods.
7. Develop an awareness program.

Military Data Classification

The military data classification system is mandatory within the U.S. Department of Defense. This system has five levels of classification:

- **Top secret**: Exposure could lead to grave damage.
- **Secret**: Exposure could lead to serious damage.
- **Confidential**: Disclosure could cause damage.
- **Sensitive but unclassified (SBU)**: Disclosure should be avoided.
- **Unclassified or official**: If released, no damage should result.

Each classification represents a level of sensitivity. *Sensitivity* is the desired degree of secrecy that the information should maintain. The concept of need to know is similar to the principle of least privilege in that employees should have access only to information that they need to know to complete their assigned duties. If you hold a confidential clearance, it means that you can access unclassified, sensitive, or confidential information that you have need to know. You cannot, however, access secret or top secret information. Sometimes organizations use the term *for official use only* (*FOUO*) to further define the scope of information usage.

Public/Private Data Classification

Public, or commercial, data classification is built on a four-level model:

- **Confidential**: This is the highest level of sensitivity, and disclosure could cause extreme damage to the organization.
- **Private**: This information is for organization use only, and its disclosure would damage the organization.
- **Sensitive**: This information requires a greater level of protection to prevent loss of confidentiality.
- **Public**: This information might not need to be disclosed, but if it is, it shouldn't cause any damage.

Table 2.1 lists the military and public/private data classification models.

TABLE 2.1 **Commercial and Military Data Classifications**

Military Classifications	Commercial Business Classifications
Top secret	Confidential
Secret	Private
Confidential	Sensitive
Sensitive but unclassified (SBU)	Public
Unclassified	

Caution

Information has a useful life. Data classification systems need to include mechanisms to monitor whether information has become obsolete, and obsolete information should be declassified or destroyed.

Asset Management and Governance

The job of asset management and governance is to align the goals of IT to the business functions of the organization, to track assets throughout their lifecycle, and to protect the assets of the organization. An asset management system inventories, monitors, and maintains items of value. Assets, which can be both tangible and intangible, include the following:

- Hardware
- Software

- Employees
- Services
- Reputation
- Documentation

You can think of asset management as a structured approach to cost-effectively deploying, operating, maintaining, upgrading, and disposing of assets. Asset management is required for proper risk assessment. Before you can place a value on an asset, you must know what it is and determine what it is worth. Its value can be assessed either quantitatively or qualitatively. A quantitative approach requires the following steps:

1. Estimate the potential losses and determine single loss expectancy (SLE).
2. Complete a threat frequency analysis and calculate the annual rate of occurrence (ARO).
3. Determine the annual loss expectancy (ALE).

A qualitative approach does not place a dollar value on an asset but ranks it as being of high, medium, or low concern. The downside of performing qualitative evaluations is that you are not working with dollar values, so it can be difficult to communicate the results of the assessment to management.

One key asset is software. CISSP candidates should understand common issues related to software licensing. Because software vendors usually license their software rather than sell it, and because they license it for a number of users on a number of systems, software licenses must be accounted for by the purchasing organization. If users or systems exceed the licensed number, the organization can be held legally liable.

We have moved into an age where software is being delivered over the Internet and not via media such as CDs, and software asset management is still an important concern.

Software Licensing

Intellectual property rights issues have always been hard to enforce. Just consider the uproar that Napster caused years ago, as the courts tried to work out issues of intellectual property and the rights of individuals to share music and other files. The software industry has long dealt with such issues. Since the early days of computing, some individuals have been swapping, sharing, and illegally copying computer software. The unauthorized copying and sharing of software is considered software piracy, which is illegal. It is tempting to think that giving a copy of a computer game to a friend does not hurt anyone. But software piracy is big business, and the accumulated losses to property owners are staggering. According to an American Bar Association report on stolen intellectual property, the estimated loss is between $200 and $250 billion annually.

Microsoft and other companies are actively fighting to protect their property rights. A number of organizations have formed the Software Publishers Association, which is one of the primary bodies working to enforce licensing agreements. The Business Software Alliance (BSA) and the Federation Against Software Theft are international groups targeting software piracy. These associations target organizations of all sizes, from small, two-person companies to large multinationals.

Software companies are making clear in their licenses what a user can and cannot do with their software. Some vendors even place limits on virtualization. License agreements can actually be distributed in several different ways, including the following:

- **Click-wrap license agreements**: These agreements, found in many software products, require you to click through and agree to terms to install the software product. These are often called *contracts of adhesion*; they are "take it or leave it" propositions.
- **Master license agreements**: These agreements are used by large companies that develop specific software solutions that specify how the customer can use the product.
- **Shrink-wrap license agreements**: These agreements, first created when software began to be sold commercially, are named for the fact that breaking the shrink wrap on a physical media signifies your acceptance of the license.

Even with licensing and increased policing activities by organizations such as the BSA, improved technologies make it increasingly easy to pirate software, music, books, and other types of intellectual property. These factors and the need to comply with two World Trade Organization (WTO) treaties led to the passage of the 1998 Digital Millennium Copyright Act (DMCA). Here are some salient highlights:

- The DMCA makes it a crime to bypass or circumvent antipiracy measures that are built into commercial software products.
- The DMCA outlaws the manufacture, sale, or distribution of any equipment or device that can be used for code-cracking or illegally copying software.

- The DMCA provides exemptions from anti-circumvention provisions for libraries and educational institutions under certain circumstances; however, for those not covered by such exceptions, the act provides for penalties up to $1 million and 10 years in prison.
- The DMCA provides Internet service providers exceptions from copyright infringement liability enabling transmission of information across the Internet.

The Equipment Lifecycle

The equipment lifecycle begins when equipment is requested and extends to the end of its useful life or when it is discarded. The equipment lifecycle typically consist of four phases:

1. Definition of requirements
2. Acquisition and implementation
3. Operation and maintenance
4. Disposal and decommission

While some may think that much of the work is done once equipment has been acquired, that is far from the truth. An organization needs to have some support functions established. Routine maintenance is one important item. Without routine maintenance, equipment will fail, and the costs related to those failures can be calculated. Items to consider include:

- Lost productivity
- Delayed or canceled orders
- Cost of repair
- Cost of rental equipment
- Cost of emergency services
- Cost to replace equipment or reload data
- Cost to pay personnel to maintain the equipment

Technical support is another consideration. The longer a piece of equipment has been in use, the more issues it may have. For example, if you did a search for exploits for Windows Server 2008 or Windows Server 2019, which do you think would return more results? Most likely Windows Server 2008—because it has been in use for many years, during which many exploits have been created. This all points to the need for more support the longer a resource has been in use.

Determining Data Security Controls

Any discussion of logical asset security must at some point address encryption. While there is certainly more to protecting data than just encrypting it, encryption is one of the primary controls used to protect data. Just consider all the cases of lost hard drives, laptops, and thumb drives that have made news because they contained data that was not encrypted. In many cases, encryption is not just a good idea but mandated by law. CISSP candidates must understand corporate policies addressing where and how encryption will be used.

Let's examine the two areas where encryption can be used to protect data at a high level: data at rest and data in transit.

Data at Rest

Information stored on some form of media that is not traversing a network or residing in temporary memory is referred to as *data at rest*. Failure to properly protect data at rest can lead to attacks such as the following:

- Various forms of USB (Universal Serial Bus) malware, including USB Rubber Ducky
- Pod slurping, a technique for illicitly downloading or copying data from a computer, which is typically used for data exfiltration
- Other forms of malicious software, including viruses, worms, Trojans, and various types of key loggers

Data at rest can be protected via different technical and physical hardware or software controls that should be defined in your security policy. Some hardware offers the ability to build in encryption. A relatively new hardware security device for computers is called a *Trusted Platform Module* (TPM) chip. A TPM chip is a "slow" cryptographic hardware processor that can be used to provide a greater level of security than software encryption. A TPM chip installed on the motherboard of a client computer can also be used for system state authentication. A TPM chip can also be used to store encryption keys.

A TPM chip measures the system and stores the measurements as it traverses the boot sequence. When queried, the TPM chip returns these values, signed by a local private key. These values can be used to discover the status of a platform. The recognition of the state and validation of these values is referred to as *attestation*. Attestation allows you to confirm, authenticate, or prove a system to be in a specific state. Data can also be encrypted using these values. This process is referred to as *sealing a configuration*. In short, a TPM chip is a tamper-resistant cryptographic module that can provide a means to report the system configuration to a policy enforcer or health monitor.

A TPM chip also provides the ability to encrypt information to a specific platform configuration by calculating hashed values based on the system's firmware, configuration details, or core components of the operating system as it boots. These values, along with a secret key stored in the TPM chip, can be used to encrypt information and allow it to become usable only in a specific machine configuration. This process is called *sealing*.

ISO 11889-1:2009 addresses TPM chips, which can also be used with other forms of data and system protection to provide a layered approach referred to as *defense in depth*. For example, a TPM chip can help protect a system, and another set of encryption keys can be stored on a user's common access card or smart card to decrypt and access the data set.

Another potential option that builds on this technology is self-encrypting hard drives (SEDs). SEDs are hardware that offers many advantages over non-encrypted drives, including the following:

- **Compliance**: SEDs have the ability to offer built-in encryption, which can help with compliance laws that many organizations must adhere to.
- **Strong security**: SEDs make use of strong encryption. The contents of an SED are always encrypted, and the encryption keys are themselves encrypted and protected in hardware.
- **Ease of use**: Users only have to authenticate to the drive when the device boots up or when they change passwords/credentials. The encryption is not visible to the user.
- **Performance**: As SEDs are not visible to the user and are integrated into hardware, the system operates at full performance and has no impact on user productivity.

Software encryption is another protection mechanism for data at rest. There are many options available, such as BitLocker and PGP. Software encryption can be used on specific files, databases, or even entire RAID arrays that store sensitive data. With any potential software option, the encrypted data must remain secure and inaccessible when access controls, such as usernames and passwords, are incorrect; in addition, the encryption keys must be protected, and they should therefore be updated on a regular basis.

Caution

Encryption keys should be stored separately from the data.

Data in Transit

Any time data is being processed or moved from one location to another, it requires proper controls. The basic problem is that many protocols and applications send information via plaintext. Services such as email, the Web, and FTP were not designed with security in mind, and with them, information is sent with few security controls and no encryption. Examples of insecure protocols include the following:

- **File Transfer Protocol (FTP)**: Plaintext username and password
- **Telnet**: Plaintext username and password
- **Hypertext Transfer Protocol (HTTP)**: Plaintext data
- **Simple Mail Transfer Protocol (SMTP)**: Plaintext data

Data in transit that is not protected by some form of encryption faces many dangers, including the following:

- Eavesdropping
- Sniffing
- Hijacking
- Data alteration

Today, many people connect to corporate networks from many different locations. Employees may connect via free Wi-Fi from coffee shops, restaurants, airports, or even hotels.

One way to protect this type of data in transit is by means of a virtual private network (VPN). A VPN is used to connect devices through the public Internet. Three protocols are used to provide a tunneling mechanism in support of VPNs: Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and IP Security (IPsec). When an appropriate protocol is defined, the VPN traffic is encrypted. Microsoft supplies Microsoft Point-to-Point Encryption (MPPE), with PPTP, native to the Microsoft operating systems. L2TP offers no encryption, and it is therefore usually used with IPsec in ESP mode to protect data in transit and provide both confidentiality and authentication. IPsec can provide both tunneling and encryption.

Two types of tunnels can be implemented:

- **LAN-to-LAN, or gateway-to-gateway, tunnels**: Users can tunnel transparently to each other on separate LANS.
- **Host-to-LAN tunnels**: Mobile or remote users can connect to a corporate LAN.

Having an encrypted tunnel is just one part of protecting data in transit. Another important concept is authentication. Almost all VPNs use digital certificates as the primary means of authentication. X.509 v3 is the de facto standard. X.509 specifies certificate requirements and contents. Much like a state driver's license office, a certificate authority (CA) guarantees the authenticity of a certificate holder and the contents of the certificate. These digital certificates can have different use cases, including providing for authentication and holding the public keys of the certificate holder.

Just as with other services, organizations need to develop policies to define who will have access to its VPN and what encryption mechanisms will be used. It's important that VPN policies be designed to map to the organization's security policy. As senior management is ultimately responsible, they must approve and support this policy.

Standard email is also very insecure, and data can be exposed while in transit over email. Standard email protocols such as SMTP, POP3, and IMAP all send data via plaintext. To protect email in transit, you must use encryption. Email protection mechanisms include PGP, Secure Multipurpose Internet Mail Extensions (S/MIME), and Privacy-Enhanced Mail (PEM). Regardless of what is being protected, periodic auditing of sensitive data should be part of policy and should occur on a regular schedule.

With data in transit, it is important to consider how encryption will be applied. Encryption can be performed at different locations with different amounts of protection applied. Consider the following options:

- **Link encryption**: The data is encrypted through the entire communication path. Because all header information is encrypted, each node must decrypt and encrypt the routing information. The source and destination addresses cannot be seen to someone sniffing traffic. For example, think of a police TV series that pulls a pen register on a phone. The police officers see a list of numbers the phone has called, the times, and the durations of the calls. While the officers cannot hear what was said on the calls, they can derive useful information about the frequency and duration of calls. IP headers can provide similar information about endpoints.

Note

A man-in-the-middle attack may be used against link encryption to see the routing information and perform traffic analysis, which involves looking at the source and destination IP addresses to determine what systems are communicating and how often they are communicating.

- **End-to-end encryption**: This type of encryption is generally performed by the end user, who can pass through each node without further processing. However, source and destination addresses are passed in plaintext, so they can be seen by someone sniffing traffic.

Data can be encrypted using either of these two methods with or without the IP header being encrypted. With both link encryption and end-to-end encryption, the confidentiality of data is protected. If a VPN is set up to use link encryption, the IP information is encrypted, as is the data traffic.

Caution

Because link encryption requires the encryption of the IP header, it would be very difficult to use it for routing over a LAN or the Internet; each routing device would have to have a copy of the secret key used.

Endpoint Security

A review of logical asset security would not be complete without a discussion of endpoint security. Endpoint security consists of the controls placed on client or end-user systems, such as antivirus, anti-malware, anti-spyware, and so on. Much of the IT security world has moved to a *zero-trust environment*, in which networked devices, such as laptops, are not trusted by default, even if they are connected to a managed corporate network.

Other controls placed on a client system, including the following, are also very important:

- **Removable media**: Malware is commonly propagated via USB thumb drive. Malware such as Stuxnet, Conficker, and Flame were all able to spread using thumb drives. Removable drives should be restricted and turned off when possible.

- **Disk encryption**: Disk encryption software such as PGP and BitLocker can be used to encrypt the contents of desktop and laptop hard drives. Also, corporate smartphones and tablets should have encryption enabled.
- **Application whitelisting**: This approach only allows known good applications and software to be installed, updated, and used. Whitelisting techniques can include code signing, digital certificates, known good cryptographic hashes, or trusted full paths and names. Blacklisting, on the other hand, involves blocking known bad software from being downloaded and installed.
- **Host-based firewalls**: For defense in depth, a company should consider not just enterprise firewalls but also host-based firewalls.
- **Configuration lockdown**: Not just anyone should have the ability to make changes to equipment or hardware. Configuration controls can be used to prevent unauthorized changes.
- **Antivirus**: Antivirus software is the most commonly deployed endpoint security product. While it is still a needed component, traditional, signature-based antivirus has become much less effective over the past several years as AI driven solutions have increased market share.

One basic starting point is to apply the principle of least privilege to each logical asset: Each computer, system component, or process should have the least authority necessary to perform its duties.

Baselines

A *baseline* is a standard of security. Baselines are usually mapped to industry standards. For example, an organization might specify that all computer systems must be certified to Common Criteria Evaluation Assurance Level (EAL) 3. Another example of baselining can be seen in NIST 800-53, which describes a tailored baseline as a starting point for determining the needed level of security (see Figure 2.4).

Some methods used to establish baselines includes the following:

- **IT structure analysis (survey)**: Analysis of technical, operation, and physical aspects of the organization, division, or group.
- **Assessment of protection needs**: Determination of the needed level of protection. This activity can be quantitative or qualitative.

- **Selection of actions**: Determination of what specific controls need to be implemented.
- **Running comparison of nominal and actual**: Periodic review of activities and actions to measure the change between what was previously occurring and what is currently occurring.

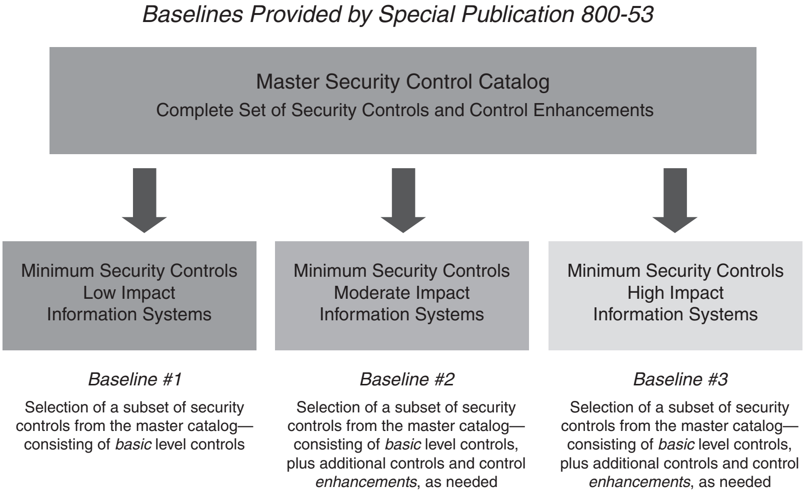

Baselines Provided by Special Publication 800-53
Master Security Control Catalog
Complete Set of Security Controls and Control Enhancements
Minimum Security Controls
Low Impact
Information Systems
Minimum Security Controls
Moderate Impact
Information Systems
Minimum Security Controls
High Impact
Information Systems
Baseline #1
Selection of a subset of security controls from the master catalog—consisting of basic level controls
Baseline #2
Selection of a subset of security controls from the master catalog—consisting of basic level controls, plus additional controls and control enhancements, as needed
Baseline #3
Selection of a subset of security controls from the master catalog—consisting of basic level controls, plus additional controls and control enhancements, as needed

FIGURE 2.4 **NIST 800-53 Scoping and Baselining Controls**

NIST 800-53 specifies scoping or tailoring activities and categorizes information based on impact (low, moderate, or high).

- Low impact
- Moderate impact
- High impact

Scoping or tailoring determines how standards are used to get the right level of protection for an organization. *Scoping* is the process of determining which portions of a standard will be implemented by an organization. For example, a high-security facility may decide not to deploy Wi-Fi and might state that Wi-Fi standards are out of scope and shall not apply. *Tailoring* is the process of customizing a standard for an organization.

NIST 800-52 (*Security and Privacy Controls for Federal Information Systems and Organizations*) describes the tailoring process:

1. Identify and designate common controls in initial security control baselines.

2. Apply scoping considerations to the remaining baseline security controls.
3. Select compensating security controls, if needed.
4. Assign specific values to organization-defined security control parameters (such as password complexity policies) via explicit assignment and selection statements.
5. Supplement baselines with additional security controls and control enhancements, if needed.
6. Provide additional specification information for control implementation, if needed.

ExamAlert

The CISSP exam will expect you to understand terms such as scoping, tailoring, and supplementation. For example, you might reduce the standard logout time from 24 hours to 8 hours. *Supplementation* is the addition of specific details to your specified controls. For example, you might replace the term *cloud hosting* with *Microsoft Azure*.

By scoping a project to remove items, you might be able to reduce costs, but in doing so, you might expose the system to unnecessary threats. Therefore, due care must be used to determine the proper level of controls. Scoping and tailoring activities should be well documented with appropriate justification. In some cases, information and information systems must be protected regardless of the cost because of laws that govern certain industries.

Exam Prep Questions

1. Which of the following levels does the military classification system include?

❍ **A.** Confidential, private, sensitive, and public

❍ **B.** Top secret, secret, private, sensitive, and public

❍ **C.** Top secret, confidential, private, sensitive, and unclassified

❍ **D.** Top secret, secret, confidential, sensitive, and unclassified

2. Your company is considering implementing NIST 800-53. Which of the following terms refers to the process of modifying security controls to align with the mission of the organization?

❍ **A.** Standards selection

❍ **B.** Tailoring

❍ **C.** Scoping

❍ **D.** Conforming

3. Which of the following endpoint security controls could have been used to potentially prevent malware such as Stuxnet, Conficker, and Flame?

❍ **A.** Implementing disk encryption

❍ **B.** Hardening edge devices

❍ **C.** Blocking removable media

❍ **D.** Enforcing application whitelisting

4. Which of the following shows the proper order?

❍ **A.** Determine SLE, ARO, and ALE and then asset value.

❍ **B.** Determine asset value and then ARO, SLE, and ALE.

❍ **C.** Determine asset value and then SLE, ALE, and SLE.

❍ **D.** Determine asset value and then SLE, ARO, and ALE.

5. With which of the following assessment types do you not work with dollar values, which can make it difficult to communicate the results of the assessment to management?

❍ **A.** Qualitative

❍ **B.** Quantitative

❍ **C.** Numeric mitigation

❍ **D.** Red team

6. Which of the following categories of control can include the logical mechanisms used to control access and authenticate users?

   ○ **A.** Administrative

   ○ **B.** Clerical

   ○ **C.** Technical

   ○ **D.** Physical

7. Which of the following does not describe an SED?

   ○ **A.** Eases compliance

   ○ **B.** Slows performance

   ○ **C.** Eases use

   ○ **D.** Provides strong security

8. Which of the following is the top level of protection for commercial business classification?

   ○ **A.** Secret

   ○ **B.** Confidential

   ○ **C.** Top secret

   ○ **D.** Private

9. Which of the following is the most specific type of security document?

   ○ **A.** Procedure

   ○ **B.** Standard

   ○ **C.** Policy

   ○ **D.** Baseline

10. It is important to avoid a situation in which everyone is accountable but no one is responsible. In which of the following groups should a data owner be?

    ○ **A.** End users

    ○ **B.** Technical managers

    ○ **C.** Senior management

    ○ **D.** Everyone is responsible; therefore, all groups are owners

11. You need to provide protection for sensitive information that will be transmitted between two business units, and you decide to use link encryption. Which of the following statements is incorrect?

    ○ **A.** The data packet is encrypted along the communication path.

    ○ **B.** The data packet is protected from eavesdropping and sniffing.

    ○ **C.** Headers are in plaintext.

    ○ **D.** Everything is encrypted from source to destination along the journey.

12. After opening a new branch in the Midwest, your company is analyzing buying patterns to determine the relationship between various items purchased. Which of the following best describes this situation?

❍ **A.** Data mining

❍ **B.** Knowledge management

❍ **C.** Data warehouse

❍ **D.** Data standards

13. Which administrative process is driven by the need to protect sensitive data?

❍ **A.** Tailoring

❍ **B.** Scoping

❍ **C.** Information classification

❍ **D.** Asset classification

14. Which of the following SAN solutions is fast, rides on top of Ethernet, and is non-routable?

❍ **A.** SCSI

❍ **B.** iSCSI

❍ **C.** HBA

❍ **D.** FCoE

15. Who is ultimately responsible for the security of an asset?

❍ **A.** Asset owner

❍ **B.** Auditor

❍ **C.** Custodian

❍ **D.** Risk assessment team

Answers to Exam Prep Questions

1. **D.** The military data classification system is widely used within the Department of Defense. This system has five levels of classification (from lowest sensitivity to highest): unclassified, sensitive, confidential, secret, and top secret.

2. **B.** Tailoring refers to customizing a standard for an organization. Answers A, C, and D are incorrect: Standards selection involves determining which standard your organization will apply and follow. Scoping involves defining which portion of the standard will be applied. Conforming simply means complying with a standard or standards.

3. **C.** Restricting removable media may have helped prevent infection from malware that is known to spread via thumb drive or removable media. Answer A is incorrect because encryption of media would not have helped. Answer B is incorrect because edge devices were not specifically targeted. Answer D is incorrect because enforcing application whitelisting would not have prevented advanced persistent threats from executing on local systems.

4. **D.** The proper order is to determine the asset value and then SLE, ARO, and ALE. Answers A, B, and C are incorrect; they are not in the proper order.

5. **A.** Qualitative assessment is scenario driven and does not attempt to assign dollar values to components of the risk analysis. Quantitative assessment is based on dollar amounts. Both numeric mitigation and red team are distractors.

6. **C.** Technical controls can be hardware or software. They are logical mechanisms used to control access and authenticate users, identify unusual activity, and restrict unauthorized access. Clerical is a nonexistent category, and all other answers are incorrect: Administrative controls are procedural, and physical controls include locks, guards, gates, and alarms.

7. **B.** Self-encrypting hard drives offer many advantages, such as easing compliance issues with items like personally identifiable information. They are easy to use and offer strong encryption. Answer B is correct because SEDs do not slow down performance; they are actually integrated into the hardware and operate at full performance with no impact on user productivity.

8. **B.** Confidential is the top level of data classification for commercial business classification. Answers A, C, and D are incorrect because secret and top secret are both part of the military classification, while private is a lower-level commercial business classification.

9. **A.** A procedure is a detailed, in-depth, step-by-step document that lays out exactly what is to be done. It's tied to specific technologies and devices. Standards are tactical documents; policies are high-level documents; and baselines are minimum levels of security that a system, network, or device must adhere to.

10. **C.** Senior management is the ultimate owner because these individuals are responsible for the asset and must answer if data is compromised. Although answer C is the best possible choice, it is important to realize that, in most cases, the data owner is a member of management but might not be the most senior executive within the organization. For example, the CFO would be the data owner

for all financial data, the director of human resources would be the data owner for all HR data, and so on. All other answers are incorrect because end users, technical managers, and other employees are not typically the data owners.

11. **D.** While link encryption does protect a data packet, the header is in plaintext. Answers A, B, and C are incorrect as they are all true statements concerning link encryption. With link encryption, the data packet is encrypted, the packet is protected from sniffing, and headers are in plaintext.
12. **A.** Data mining is the process of analyzing data to find and understand patterns and relationships in the data. Answers B, C, and D are incorrect. Knowledge management seeks to make intelligent use of all the knowledge in an organization. A data warehouse is a database that contains data from many different databases. Data standards provide consistent meaning to data shared among different information systems.
13. **C.** Organizations use information classification to assign value to information based on its impact should it be exposed or its sensitivity. Answers A, B, and D are incorrect as tailoring is modifying standards to an industry. Scoping is determining which portions of standards to apply. Asset classification is a system for assigning assets to groups, based on a number of common characteristics.
14. **D.** Fibre Channel over Ethernet (FCoE) can operate at speeds of 10 Gbps and rides on top of the Ethernet protocol. While it is fast, it has a disadvantage in that it is non-routable. Answers A, B, and C are incorrect. SCSI is used for local devices only. iSCSI is a SAN standard used for connecting data storage facilities and allowing remote SCSI devices to communicate. An HBA is used to connect a host system to an enterprise storage device.
15. **A.** Some day-to-day responsibility may be passed down to the custodian; however, ultimately the owner is responsible.

Need to Know More?

Data classification: mrcissp.com/2019/01/17/data-classification-why-what-how/

Asset retention: https://info-savvy.com/cissp-asset-retention-bk2d2t5/

ISO 27002 overview: https://www.iso27001security.com/html/27002.html

HIPAA regulations and the CISSP: cissp2021.blogspot.com/2020/12/gdpr-hipaa-compliance-key-similarities.html

IT asset management: searchcio.techtarget.com/definition/IT-asset-management-information-technology-asset-management

Security policy templates: www.sans.org/security-resources/policies/

IT security baselines: https://resources.infosecinstitute.com/certification/cissp-prep-security-policies-standards-procedures-guidelines/

Building effective policy: csrc.nist.gov/nissc/1997/panels/isptg/pescatore/html/

OECD versus GDPR: piwik.pro/blog/oecd-guidelines-8-privacy-principles-to-live-by/

Scoping and tailoring: www.hackingtheuniverse.com/infosec/nist-computer-security/security-control-implementation/tailoring-security-controls

CHAPTER 3

Security and Risk Management

Terms you'll need to understand:

- Security governance
- Compliance
- Regulation
- Information security laws and regulations
- Professional ethics
- Threat
- Vulnerability
- Security and risk management
- Single loss expectancy (SLE)
- Annual rate of occurrence (ARO)
- Residual risk
- Annual loss expectancy (ALE)
- Business continuity requirements
- Threat modeling
- Supply chain risk management

Topics you'll need to master:

- Calculations used for risk management
- Approved approaches to good security management
- How to perform qualitative risk analysis
- How to perform quantitative risk analysis
- How to perform hybrid risk analysis
- Good resource protection
- The roles of security policies, procedures, guidelines, and baselines
- Proper data classification
- Proper implementation of security roles
- How to perform risk calculations

Introduction

The CISSP exam Security and Risk Management domain encompasses data classification and evaluation as well as security governance and protection of intellectual property. Each of these is driven by documents such as policies, procedures, and guidelines. These documents are of great importance because they spell out how an organization manages its security practices and detail what is most important to the organization. These documents provide a roadmap, demonstrating the level and amount of governance in an organization. These documents are not developed in a void. Senior management must lead by driving this process. Senior management has the vision, knows the overall goals of the organization, and knows the mission of the organization. Each of these documents should be tied to laws, regulations, and mandates that govern the organization.

This chapter goes into more depth on the two ways to calculate risk: qualitative and quantitative. The key to mastering the Security and Risk Management domain is understanding these two methods. Neither of these methods is better than the other. Both quantitative and qualitative risk assessment methods have advantages and disadvantages. It is important that you, as a CISSP candidate, understand the differences and how each method can be used to address threats, assess risk potential, and evaluate an organization's vulnerabilities. You need to understand that risk can occur in the supply chain, in processes, and even in a lack of robust business continuity processes.

Finally, it's important to remember that employees play a key part in security and risk management. They are tasked with carrying out the policies implemented by management. Although the workers in an organization will want to do the right thing and help the company succeed, they must be trained. Their training can be on a wide range of topics, from ethics to acceptable use to social engineering. Training helps employees know what the proper actions are and understand the security practices of the organization. The overall goal of this domain is to ensure confidentiality, integrity, and availability of an organization's assets and information.

Security Governance

Security management has changed throughout the years. In the 1970s, the focus was on computer security, whereas in the 1980s and 1990s, the focus shifted to data and information security systems. Only during the past few decades have organizations begun to look at security more holistically.

Today, there is a focus on governance, which encompasses all of security. Good governance requires total enterprise protection, often referred to as a *holistic enterprise security program*, which includes physical, logical, and administrative components. Luckily for security management, there are many guidance documents available to help build an effective security management program. Such a program is considered a code of practice for information security.

U.S. Legal System and Laws

The U.S. legal system can trace its roots to the United Kingdom. The United States, United Kingdom, and Canada all use a *common law* system. Common law is based on previous rulings and principles, such as *stare decisis*—the concept that court cases that are similar should be decided in a consistent manner. Common law also recognizes the rule of reasonable doubt and that a defendant is innocent until proven guilty. Common law includes several categories:

- **Criminal law**: *Criminal law* exists to punish someone who violates the government's laws and is therefore considered to have committed crimes against society. Cases are brought forth by the state or federal government. Punishment can include financial penalties, imprisonment, or both. Broadly speaking, felonies are more serious crimes that can result in large fines and more than one year of imprisonment, while misdemeanors are less serious crimes that result in smaller fines and no more than one year of imprisonment. Penalties for both felonies and misdemeanors are designed to punish criminals and deter criminal activity.

- **Civil law**: *Civil law* has no ability to prescribe prison time. Cases are brought forth by victims or individuals who believe they have been wronged. Victims are compensated by means of financial awards of punitive, compensatory, or statutory damages if the defendant is found guilty. Punitive damages are determined by a jury. Compensatory damages are payments based on actual damage, whereas statutory damages are awarded based on law and preset limits.

- **Administrative (regulatory) law**: *Administrative law* establishes standards of performance and conduct that governmental agencies expect from industries, organizations, officials, and officers. Individuals and organizations that violate these laws can be punished by financial penalties and/or imprisonment. These laws typically apply to healthcare, financial, industrial, petrochemical, and pharmaceutical industries.

Note

Hearsay evidence is generally not admissible in court as it is considered secondhand information.

Relevant U.S. Laws and Regulations

Security professionals should be aware of the laws that pertain to them locally and understand terms such as *due care* and *due diligence*. Due care involves taking reasonable care to protect the assets of an organization. For example, think of it as information gathering. Doing the right thing over a period of time—implementation—is due diligence.

The CISSP exam does not test you on country-specific laws, but you should have an understanding of laws in your region of the world. The following are important U.S. laws and guidelines:

- **Computer Fraud and Abuse Act (CFAA) of 1986**: Amended in 1996, this act makes distribution of malware illegal. It deals with computers used by the federal government but can include others.
- **Federal Sentencing Guidelines of 1991**: These rules provide guidance to judges to ensure that sentences are handed down in a more uniform manner for crimes dealing with computers.
- **Economic Espionage Act of 1996**: This act defines strict penalties for those accused of espionage.
- **U.S. Child Pornography Prevention Act of 1996**: The goal of this act is to combat and reduce the use of computer technology to produce and distribute child pornography.
- **U.S. Patriot Act of 2001**: This act strengthens computer crime laws to expand law enforcement's capability to fight terrorism.

International Legal Systems and Laws

Legal systems vary throughout the world in terms of the rights of the accused, the role of the judge, the nature of evidence, and other essential legal concepts. Claims and cases can be handled quite differently in different places. Figure 3.1 shows some of the various systems used in the world.

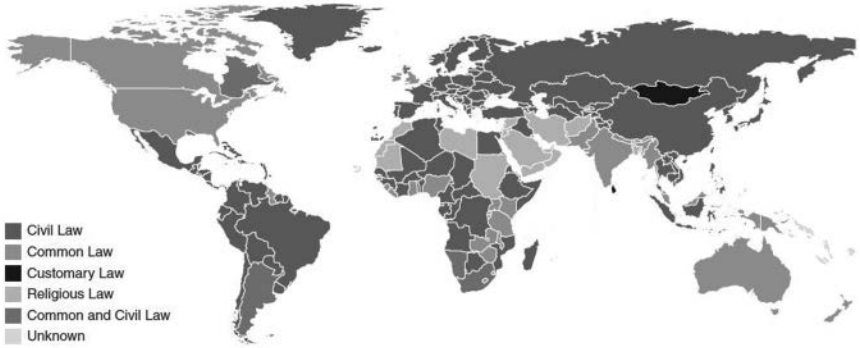


FIGURE 3.1 **Legal Systems of the World**

Much of Europe is based on civil (code) law, also known as *Napoleonic law*. Civil law evolved in Europe around the time of the Roman Empire. The Romans used *Corpus Juris Civilis*, which featured a comprehensive system of written rules of law that serves as the basis of civil law used today. The major difference between civil law and common law is that civil law uses legislation as the main source of legal rulings in court cases.

Religious law is based on religious tenets. Examples include *halakha* in Judaism and *sharia* in Islam. The Islamic system is an autonomous legal system based on religious tenets and references the Qur'an. China and some African countries use *customary law*, which is based on the concept of what is considered customary and normal conduct.

If two or more of these legal systems are combined, the result is a *mixed law* system. Mixed law systems are noted for their inclusion of more than one type of legal framework and might feature components of two or more basic types. As an example, Louisiana has features of both civil law and common law, and parts of the Middle East mix customary law with religious law.

This international patchwork of legal systems is superimposed on international property laws that affect data handling, so although the CISSP exam will most likely focus on common law, it is important that you understand the differences between the various legal systems used around the world.

International Laws to Protect Intellectual Property

Data owners typically have legal rights over the data they create and own. Data owners are typically responsible for understanding the intellectual property rights and copyright of their data. Intellectual property is agreed on and enforced worldwide by various organizations, including the United Nations Commission on International Trade Law (UNCITRAL), the European Union (EU), and the World Trade Organization (WTO). International property laws protect trade secrets, trademarks, patents, and copyrights:

- **Trade secret**: A *trade secret* is a confidential design, practice, or method that is proprietary or business related. For a trade secret to remain valid, the owner must take precautions to ensure that the data remains secure. Examples of these precautions include encryption, document marking, and physical security.
- **Trademark**: A *trademark* is a symbol, word, name, sound, or something else that identifies the origin of a product or service in a particular trade. The (ISC)^2 logo is an example of a trademarked logo. The term *service mark* is sometimes used to distinguish a trademark that applies to a service rather than to a product.
- **Patent**: A *patent* documents a process or synthesis and grants the owner a legally enforceable right to exclude others from practicing or using the invention's design for a defined period of time.
- **Copyright**: A *copyright* is a legal device that provides the creator of a work the right to control how the work is used and protects that person's expression on a specific subject. This includes the reproduction rights, distribution rights, music, right to create, and right to public display. The length of a copyright in the United States and the EU is life plus 70 years. Copyrights to intellectual property are agreed on and enforced worldwide by various organizations, including UNCITRAL, the EU, and the WTO.

Note

Although copyright law generally defines the ownership and use of material, fair use allows for use of material in a limited manner. Fair use is intended to balance the interests of copyright holders with those of the public. Limited use of material is allowed to situations that might otherwise be considered infringement.

Global Legal and Regulatory Issues

One global legal issue is privacy laws. These laws are of critical importance because technology has simplified the process of accumulating large amounts of data about individuals. An example of this can be seen in the Chinese social credit system, which is designed to establish a unified record system for individuals, businesses, and the government that tracks and evaluates credit scores. This is a massive database, and there are important privacy concerns about how this data is stored and whether it can be breached.

Throughout the world, commercial and government databases contain tremendous amounts of data that can be used to infringe on people's sense of privacy and anonymity. The misuse of these databases can lead to targeted advertising and disclosure of personal preferences that some individuals believe is intrusive. Privacy is increasingly being recognized as a fundamental right in many countries, and organizations that hold personal information are being required to protect it.

The EU, which has been on the forefront in developing laws that protect individual privacy, deals with privacy on the federal level. Its *Data Protection Authority* has the power to enforce privacy directives. EU privacy guidelines enacted in 1998 state the following:

- Data is to be used only for the purposes for which it was collected and within a reasonable time.
- Individuals are entitled to request and receive reports on data about them.
- An individual's personal data cannot be disclosed to third parties unless authorized by statute or consent of the individual.
- Persons have a right to make corrections to their personal data.
- Data transmission to locations where equivalent personal data protection cannot be assured is prohibited.

The EU has also implemented a concept known as the *right to be forgotten*, which has been in practice in the EU and Argentina since 2006. On request, information that is irrelevant, private, or no longer relevant must be removed from Internet searches.

In the United States, the federal government reacts only to obvious abuses of laws when they are reported. Privacy laws are driven by government actions.

The Fourth Amendment to the U.S. Constitution is the basis of privacy law in the United States. Two laws are worth mentioning include the following to laws:

- **The Privacy Act of 1974**: This act limits the personal information a federal agency can collect, maintain, and disclose.

- **The Identity Theft and Assumption Deterrence Act of 1998**: This act raises the penalties for identity theft and establishes that the person whose identity was stolen is a true victim. Before passage of this act, only a credit grantor who suffered monetary losses was considered a victim.

Even with these laws in place, it is still possible to obtain a large amount of information about individuals in the United States. To get a better idea about what types of information are available, take a moment to review Table 3.1. Most of these sites will give you some information for free, and for just a few dollars you can get much more. This is just a short list; there are many more sites from which to gather personal information.

TABLE 3.1 **Personal Information Websites**

Type of Information	Usage	URL
Location of individual	Used to find location, address, age, and other information	www.zabasearch.com
Informants	Used to identify informants	www.whosarat.com
Police crime tracking	Used to report misconduct and abuse	www.copblaster.com

Note

Although the United States and the EU take different approaches to privacy, U.S. companies handling information from customers based in the EU must be aware of the European Commission's 1998 Directive on Data Protection (Safe Harbor) and must provide a standard for privacy protection equal to what would be provided in the EU.

Computer Crime and Hackers

An important global legal issue is multinational hacking and computer crime. Hackers, or threat actors, may be based in one county, use servers in another, and then use those resources to target yet another country. Attribution is difficult. CISSP candidates must be prepared to deal with these threat actors.

It's commonly thought that only one-tenth or so of all the computer crimes committed are detected and prosecuted. It is difficult to develop accurate numbers regarding the detection and reporting of computer crime. Many crimes go undetected and others are detected but never reported to law-enforcement agencies or the general public. Some companies do not report because they are worried about gaining a negative reputation and losing customers; others do not report because they are afraid that they might appear vulnerable. One good source of information about computer crime and data breaches is https://informationisbeautiful.net, which lists the top data breaches each year (see Figure 3.2).

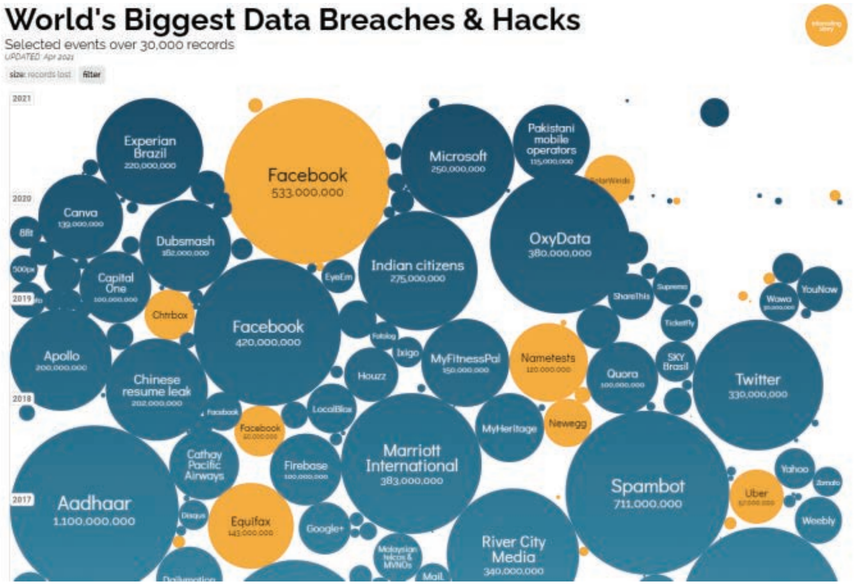


FIGURE 3.2 **World's Biggest Data Breaches**

Computer criminals use multiple attack vectors:

- **Physical security attack**: Physically accessing systems
- **Personnel security attack**: Harassing, extorting, or threatening employees
- **Communications attack**: Eavesdropping on wired, wireless, or satellite communications
- **Logical attack**: Logically accessing systems
- **Social engineering attack**: Tricking employees or others into providing access or information

No discussion of computer crime would be complete without a review of the criminals. Most security professionals think of computer criminals as hackers. Originally, the term *hacker* was used to mean a computer enthusiast who enjoyed understanding the internal workings of a system, computer, or computer network. Over time, the popular press began to use the term *hackers* for individuals who broke into computers with malicious intent. The industry responded by developing the term *cracker*, which is short for *criminal hacker*. The term *cracker* was meant to describe individuals who seek to compromise the security of a system without permission from an authorized party; however, the public continues to use the term *hacker* for a computer criminal. There are actually many other terms that can be used to identify a criminal and to categorize criminal activities, including the following:

- **Hacker/threat actor**: This generic term describes an individual who is partially or wholly responsible for an incident that impacts or has the potential to impact an organization's security and breach the confidentiality, integrity, or availability of the resource.
- **Script kiddies**: This term is used to describe less experienced hackers, who often use widely available freeware vulnerability assessment tools, existing code, and hacking tools designed for attacking purposes only. These attackers typically have very limited programming or hacking skills and depend on tools written by others.
- **Disgruntled employees**: Employees who have lost respect for their employer may attack the organization. These individuals might or might not have more skills than script kiddies. Insiders or former insiders are a real risk because of the knowledge they have and the access they might possess.
- **Cyberterrorists/cybercriminals**: Individuals or groups are sometimes funded to conduct clandestine or espionage activities on governments, organizations, and people in an unlawful manner. These individuals are typically engaged in sponsored acts of defacement, DoS/DDoS (denial of service/distributed denial of service) attacks, identity theft, and financial theft. They may also compromise critical infrastructure, such as nuclear power plants, electric plants, water treatment plants, and so on.
- **Corporate spy/nation-state hackers**: These are elite hackers who have specific expertise in attacking vulnerabilities in systems and networks. Out of all the adversaries discussed so far, these are by far the most sophisticated and capable, and they have access to the greatest resources. Government-sponsored threat actors have the funding, tools, and resources to go to great lengths to gain access to a targeted resource. Examples of organizations that support these types of these actors include Cozy Bear, Clever Kitten, Deep Panda, and Mythic Leopard.

Tip

If you want to learn more about hacking and all the players in the security realm—including hackers, security professionals, and law enforcement—consider local options such as Information Systems Security Association (ISSA) and INFRAGARD or security conferences such as Black Hat or DEF CON. You can attend conferences to gain $(ISC)^2$ continuing professional education (CPE) credits and learn more about current security trends and exposures.

Sexual Harassment

U.S. law requires companies to provide a safe workplace where employees are free from sexual harassment and offensive behavior. Progress has been made in recent years on issues such as sexual harassment in the workplace.

For example, the #MeToo movement directed a spotlight on sexual harassment and sexual assault in the workplace. Many who have survived sexual harassment in the workplace have come forward to speak out about their experiences. Companies that fail to enforce acceptable use policies (AUPs) could find themselves in legal jeopardy for not addressing these issues.

One of the key documents that can be used to achieve good governance is ISO/IEC 27002, which is discussed in more detail later in this chapter.

U.S. Governance

Risk management is the ultimate requirement in support of all information security activities. The following sections examine some U.S. laws and mandates to help with risk management.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA, which was signed into law in 1996, has two areas. Title I of the act protects health insurance coverage for workers and their families when they change or lose their jobs. Title II requires the U.S. Department of Health and Human Services (DHHS) to establish national standards for electronic healthcare transactions and national identifiers for providers, health plans, and employers.

The HIPAA Privacy Rule dictates controls that organizations must put in place to protect personal information. The privacy rule defines three major purposes:

- "To protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information."
- "To improve the quality of health care in the United States by restoring trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of care."
- "To improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals."

Gramm-Leach-Bliley Act (GLBA)

GLBA, which was signed into law in 1999, resulted in the most sweeping overhaul of financial services regulation in the United States to date.

Title V of GLBA addresses financial institutional privacy. Subtitle A of the act requires financial institutions to make certain disclosures about their privacy policies and to give individuals an opt-out capability. Subtitle B criminalizes the practice known as *pretexting*, which is the practice of obtaining personal information under false pretenses.

Under GLBA, financial institutions are required to protect the confidentiality of individual privacy information. As specified in GLBA, a financial institution must develop, implement, and maintain a comprehensive information security program with appropriate administrative, technical, and physical safeguards. Administrative controls include items such as background checks and separation of duties. Technical controls can be hardware or software, such as encryption or an intrusion detection system (IDS). Physical controls include gates, guards, and fences. An information security program must include the following controls:

- The assignment of a designated program manager for the organization's information security program
- A periodic risk and vulnerability assessment and audit
- A program of regular testing and monitoring
- The development of policies and procedures for control of sensitive information and personally identifiable information (PII)

Federal Information Security Management Act (FISMA)

FISMA was signed into law in 2002. One of the big changes that FISMA brought about was a set of clear guidelines for information security designed for the protection of federal government IT infrastructure and data assets. FISMA requirements specify the following responsibilities:

- Develop and maintain an information assurance (IA) program with an entire IT security architecture and framework.
- Ensure that information security training is conducted to keep technical and management personnel properly trained and certified in accordance with DoD 8570.
- Implement accountability for personnel with significant responsibilities for information security.

FISMA also requires periodic risk assessments, risk assessment policies and procedures, periodic (at least annual) testing and evaluation, and proper training for senior management so that proper security awareness programs can be deployed.

Sarbanes-Oxley Act (SOX)

SOX, which was signed into law in 2002, mandates a number of reforms to enhance corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud. Sections 302 and 404 are the two sections that address IT infrastructure and information security. Section 302 requires the CEO and CFO to personally certify that their organization has the proper internal controls. It also mandates that the CEO and CFO report on effectiveness of internal controls around financial reporting.

Section 404 sets requirements on management's structure, control objectives, and control procedures. Staying compliant with Section 404 requires companies to establish an infrastructure that is designed to archive records and data and protect them from destruction, loss, unauthorized alteration, or other misuse. It requires that a set of comprehensive controls be put in place and holds CEOs and CFOs accountable.

National Institute of Standards and Technology (NIST)

NIST started as the National Bureau of Standards and changed its name in 1989 to the National Institute of Standards and Technology (see www.csrc.nist.gov). The following are some of the NIST documents a security professional should have knowledge of:

- **NIST 800-37**: This is a guide for applying risk management.
- **NIST 800-53**: This government publication provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. Many organizations in private industry use NIST SP 800-53 as a guide for their security management.
- **NIST 800-60**: This is a guide for mapping types of information and information.

Federal Information Processing Standards (FIPS)

FIPS are publicly announced standards developed by the U.S. government for use in computer systems by non-military government agencies and government contractors. The following are some of the standards you should be familiar with for the CISSP exam:

- **FIPS 199**: This standard establishes security categories of information systems used by the federal government.
- **FIPS 200**: This standard lists mandatory security requirements for government systems.

> **ExamAlert**
>
> CISSP exam candidates must understand and know how to apply security concepts such as security governance and the frameworks used.

International Governance

International governance is an issue that has grown in importance as more data is shared globally. One framework for managing this huge amount of information is Information Technology Infrastructure Library.

ITIL (formerly Information Technology Infrastructure Library) provides a framework for identifying, planning, delivering, and supporting IT services for business.

ITIL has a process that begins with setting objectives for the enterprise's IT, providing the initial direction, and then evolving into a continuous loop.

ITIL presents a service lifecycle that includes the following:

- Continual service improvement
- Service strategy
- Service design
- Service transition
- Service operation

Another international standard is International Organization for Standardization (ISO) 27002, which provides best practice guidance on information security management. It is divided into 12 main sections:

- Risk Assessment and Treatment
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

ISO 27002 is written for individuals responsible for initiating, implementing, and/or maintaining information security management systems. Its goal is to provide a template for protectors, provide technical guidance, and help train those tasked with protecting an organization's assets.

The following are additional standards from the ISO 27000 family that you should be familiar with for the CISSP exam:

- **ISO 27001**: This standard describes requirements related to establishing, implementing, operating, monitoring, reviewing, and maintaining an information security management system (ISMS); it is based on British Standards Institute BS 7799.
- **ISO 27003**: This standard focuses on implementation of an ISMS.
- **ISO 27004**: This standard covers information security measurements.
- **ISO 27005**: This standard describes how to implement solutions based on risk management.
- **ISO 27799**: This standard describes how to protect personal health information.

ISO 9001 is a quality management standard that has garnered widespread support and attention. ISO 9001 describes how production processes are to be managed and reviewed. It is not a standard of quality but focuses on how well a system or process is documented. Companies that wish to obtain 9001 certification need to perform a gap analysis to determine areas that need improvement. ISO 9001 includes six documents:

- Control of Documents
- Control of Records
- Control of Non-conforming Product
- Corrective Action
- Preventive Action
- Internal Audits

Tip

To achieve ISO 9001:2000 certification, an organization must perform a gap analysis to identify shortcomings that need to be addressed in order to obtain certification.

Being ISO certified means that the organization has the capability to provide products that meet specific requirements and includes a process for continual improvement. It may also have a direct bearing on an audit as it places strong controls on documented procedures. Another ISO standard that you should be aware of is ISO 27001, which used to be known as BS 17799. ISO 27001 is divided into 12 main sections:

- Risk Assessment and Treatment
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

> **Tip**
>
> For the CISSP exam, you should have a basic understanding of ISO standards and their purpose; however, the exam does not cover U.S. laws.

The Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) rating validates best practices and the security posture of cloud providers. It is divided into three tiers:

- **Tier 1**: Self-assessment through a questionnaire
- **Tier 2**: A third-party assessment
- **Tier 3**: Continuous monitoring by a certified independent organization

The Organisation for Economic Co-operation and Development (OECD) has developed privacy guidelines that are approved by 30 nations, including EU countries, the United States, Mexico, Australia, Japan, and Czech Republic. The OECD framework contains eight driving principles:

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle

- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

For the CISSP exam, you also need to know about two more European documents:

- **10 Steps to Cyber Security**: This document provides detailed cybersecurity information and advice across 10 critical technical and procedural areas. It was created by Communications-Electronics Security Group (CESG), the information security arm of Government Communication Headquarters (GCHQ), and the National Technical Authority for Information Assurance within the United Kingdom.
- **Cybersecurity Strategy of the European Union**: This document developed by the EU describes an approach to preventing and responding to cybersecurity attacks.

Caution

Proclaiming you are compliant with a known standard is not enough. Most entities expect attestation. Attestation means providing evidence or proof. For example, cloud hosting providers use attestation to assure customers that they have gone through third-party verification and review. ISO 27001, Statement on Auditing Standards (SAS) 70, and PCI-DSS use PCI Qualified Security Assessor (QSA) for attestation.

Risk Management Concepts

Risk management is a systematic ongoing approach to analyzing risk, identifying threats, and implementing controls to mitigate risk. Risk management should be driven by senior management, who appoint someone to lead the risk assessment process. When senior management is driving the process, a company has top-down support for a security program; this is the preferred method. Sometimes senior management might not see the value of a structured risk assessment process. In such situations, a bottom-up process might still be able to drive the risk assessment process.

It is imperative that individuals driving the risk assessment process gain the support of senior management. One way to secure senior management commitment and support is to educate them using a formal presentation that communicates key aspects of the overall risk management program and reminds senior management that they are ultimately responsible.

After senior management is on board, the risk management process can begin. The goal of this process is for the organization to build the controls necessary to protect the organization's staff and assets while meeting stakeholder expectations. Major parts of risk management are developing the risk management team, identifying threats and vulnerabilities, placing a value on the organization's assets, and determining how you will deal with the risk you uncover.

Risk Management Frameworks

A risk management framework supports the risk management process. For example, British Standards Institute BS 31100 provides guidance on the objectives, mandate, and commitment to manage risk. As another example, NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, details a six-step risk management framework (RMF). The steps of the RMF are as follows (see Figure 3.3):

1. Categorize
2. Select
3. Implement
4. Assess
5. Authorize
6. Monitor

A number of other approaches to risk management and assessment have been developed, including the following:

- **Factor Analysis of Information Risk (FAIR)**: This approach to risk management involves developing baselines of probabilities for the frequency and magnitude of loss events. It's considered an add-on to existing risk frameworks.
- **Risk factor analysis**: This is another approach to risk analysis that uses a six-step methodology to identify factors that drive the behavior of the project schedule, cost, and technical performance.
- **Probabilistic risk assessment**: This approach is designed for use with large-scale complex projects where risk is defined as a feasible detrimental outcome of an activity or action. The results are expressed numerically.

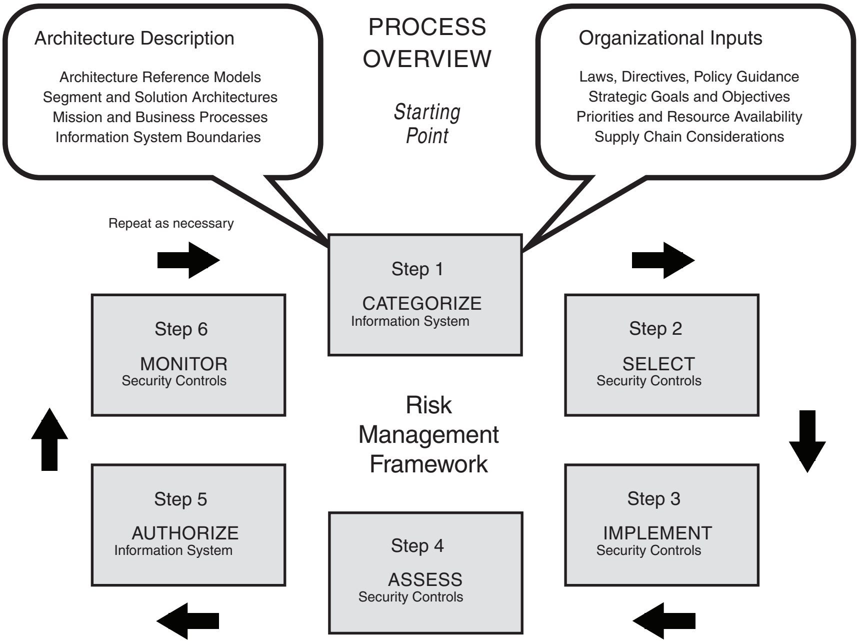


FIGURE 3.3 **NIST Risk Management Framework**

> **Note**
>
> A risk register is a tool you can use as a repository of identified risk and the nature of each one. You can see an example of a risk register at www.slideshare.net/KashifMastan/risk-register-34631122.

Risk Assessment

Whereas risk management is ongoing, a *risk assessment* has start and stop dates. A risk assessment involves identifying and prioritizing risks to a business. Completing a risk assessment is crucial. Without it, you cannot design good security policies or procedures to defend your company's critical assets. Risk assessment requires individuals to take charge of the risk management process.

For the CISSP exam, it is important to understand the concepts of risk, threat, and vulnerability.

Risk is the probability or likelihood of an occurrence or realization of a threat. There are three basic elements of risk from an IT infrastructure perspective:

- **Asset**: A component or an item of value to an organization, such as a data asset

- **Threat**: Any circumstance that could potentially cause loss or damage to an asset
- **Vulnerability**: A weakness in infrastructure, design, or components that might be exploited by a threat to destroy, damage, or compromise an asset

A *threat* is any agent, condition, or circumstance that could potentially cause harm, loss, damage, or compromise to an asset. From an IT perspective, threats can be categorized as circumstances that can affect the confidentiality, integrity, or availability of an asset. Threats can be natural, human caused, or technical. Threats can result in destruction, disclosure, modification, or corruption of corporate resources or can lead to denial of service.

A *vulnerability* is a weakness in the design of a product, a weakness in the implementation of a product, or a weakness in how a product's software or code was developed. Vulnerabilities can be reduced or even possibly eliminated through the implementation of safeguards, controls, and security countermeasures.

> **Note**
>
> Controls are mechanisms used to restrain, regulate, or reduce vulnerabilities. Controls can be corrective, detective, preventive, or deterrent.

Risk Management Team

Before you start to fret over how one person could ever accomplish risk management alone, understand that risk management is a big job. You'll need coworkers and employees from other departments to help. To do an effective job of risk management analysis, you must involve individuals from all the different departments of the company. It's hard for any one person to understand the inner workings of all departments. As an IT or security administrator, you understand the logical risks the IT infrastructure faces, but do you really have a grasp of the problems HR might have (such as employee controls, effective termination practices, and control of confidentiality information)? Bringing in key employees from other functional areas is required if you expect the risk management process to be successful.

Consider including employees from each of the following groups on a risk management team:

- Information system security
- IT and operations management

- System and network administration
- Internal audit
- Physical security
- Business process and information owners
- Human resources
- Legal
- Physical safety

Asset owners should also be represented on the team. Because the asset owners are responsible for assets, they should have a voice in the types of controls that are implemented. Having asset owners on the team ensures that the team is aware of, and can address, the many threats it will need to examine.

The team must also be kept informed and guided by personnel knowledgeable about the legal and regulatory requirements of the organization. For example, a team may be established specifically to examine ways to decrease insurance costs, reduce attacks against the company's technical infrastructure, or verify compliance with government standards such as GLBA, SOX, or HIPAA.

After the risk management team has been established, it must perform the following tasks:

- Perform asset valuation
- Perform threat analysis
- Perform quantitative or qualitative risk assessment
- Choose remedial measures
- Reduce, assign, or accept the risk

The key security management practices necessary to assess risk can be broken into six broad steps (see Figure 3.4):

1. Asset identification
2. Risk assessment
3. Policy development
4. Implementation
5. Training and education
6. Auditing the security infrastructure

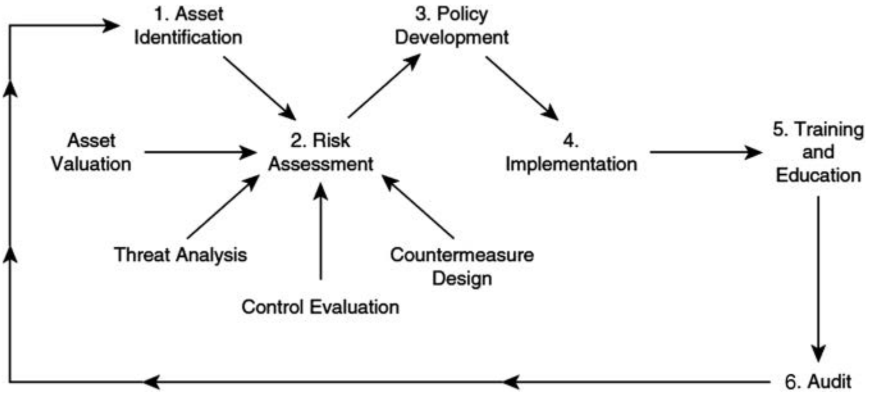


FIGURE 3.4 **Risk Management Strategy**

Asset Identification and Valuation

Once you have a risk management team that has the support of senior management, the next step is to list the value of the organization's assets. A proper *asset valuation* enables the organization's risk management team to start making business decisions regarding deployment of security controls and security countermeasures.

One of the most important steps in securing an organization's assets is to identify and inventory all those assets. For example, say that you work for a bank that is in charge of protecting a customer database containing names, Social Security numbers, and addresses. You would want to place a much higher level of control over these assets than you would another database that contained locations, manager names, and phone numbers for all your bank's local branches. However, you would not know the level of protection if you were unaware of the database asset. Without a complete and accurate inventory of all assets, an asset valuation cannot be performed.

Keep in mind that assets can be both tangible and intangible. When recording information about an organization's assets, you should include the following information:

- Identification
- Location
- Risk
- Protection
- Group
- Owner

One final important aspect offered by documented asset management is demonstrated due care. To value an asset properly, you need to appreciate that the value is often based on more than just the cost to create or purchase that item. Consider the following:

- What did it cost to acquire or create the asset?
- What liability would the organization face if the asset were compromised?
- What would be the production cost if the asset became unavailable?
- What is the value of the asset to competitors and foreign governments?
- How critical is the asset, and how would its loss affect the company?
- What skill sets and how many hours per day, week, or month are required to maintain the asset?
- What subsystems, applications, hardware, or software does this asset depend on?

After listing the values of assets, the risk management team can determine the organization's most critical systems, resources, applications, and data. This information allows the team to prioritize investments for security controls and security countermeasures. Controls are not cost free but require expenditure of limited funds. Most organizations must justify the investment needed for proper security controls and security countermeasures.

Without an asset valuation, it is difficult to understand a control's return on investment (ROI) or make a cost–benefit analysis of the investment in security countermeasures. Knowing the value of assets that you are trying to protect is also important because it would be foolish to exceed the value of an asset by spending more on the countermeasure than the asset is worth or spending more on a control than you stand to lose if a threat targets a vulnerability. A common problem is failing to take into account how the secondary and tertiary systems affect value assigned to key assets.

Remember that you can't protect everything. When defining scope, organizations must keep in mind that they have only limited funds and resources, and countermeasures must be strategically deployed to guard what has been deemed most critical. Focus should first be given to protect assets that face high levels of risk, as illustrated in Figure 3.5.

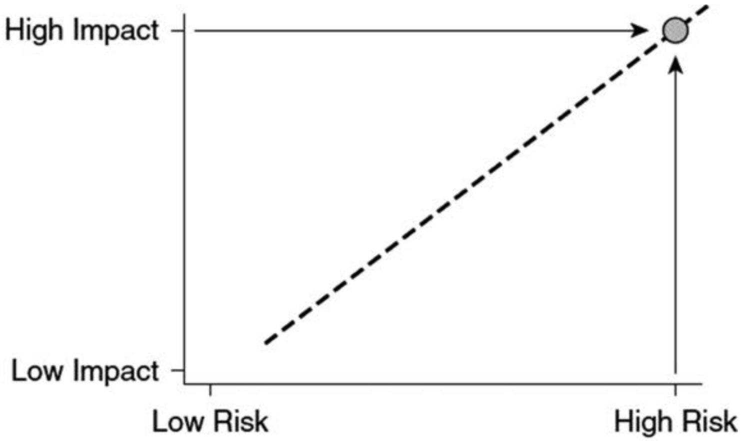


FIGURE 3.5 **High-Risk, High-Impact Assets**

It is often necessary to do asset identification and evaluation for insurance purposes. An organization might determine that some risks should be transferred to third parties, and asset valuation enables an organization to accurately assess its business insurance requirements. Some companies now offer technical and cyber risk coverage, popularly known as *hacker insurance*.

Threats Analysis

Earlier in this chapter, we discussed the negative impacts threats can have on an organization. This section looks at where threats might originate. Threats can occur because of technical failures or natural factors, or they can be caused by humans, either maliciously or accidentally. Identifying all potential threats is a huge responsibility. You don't want to randomly brainstorm on potential threats; after all, why list a hurricane as a threat if you live in Kansas? A good place to start is to think about threats you might face in the following common categories:

- Natural catastrophes
- Physical threat/theft
- Human error/insider threat
- Application error/buffer overflow
- Equipment malfunction
- Environmental hazards
- Malicious software/covert channels

- Hacker attacks
- Disclosure of confidential information
- Stolen, lost, damaged, or modified data
- Unauthorized access
- Terrorism
- Viruses, worms, and malware
- Denial of service

A threat coupled with a vulnerability and a threat agent can lead to a loss. A threat agent is an individual or a group that can manifest a threat. As mentioned earlier, vulnerabilities are flaws or weaknesses in security systems, software, or procedures. An example of a vulnerability is lack of employee training; an improperly trained help desk employee could, for example, unknowingly give a password to a potential hacker, which could result in a loss. Examples of losses or impacts include the following:

- Financial loss
- Loss of reputation
- Endangerment or injury of staff, clients, or customers
- Loss of business opportunity
- Breach of confidence or violation of law

Losses might have immediate or delayed impact. A delayed loss has a negative effect on an organization well after the period of loss. This could perhaps be a few days, a few months, or even a few years. For example, an organization could have its website hacked and thus suffer an immediate loss. No e-commerce transactions can occur until technical support is brought in to rebuild the web server; all normal processing is halted. But these immediate losses might not be the only effects the company feels. Later, when the local news channel reports that the company was hacked and that personal information was lost, the company's reputation could be hurt, leading to a loss of customers in the future. State laws vary, and some states, such as California, might require the company to report a breach. Customers might remember such an event for years to come and choose to use a competitor. These are examples of delayed loss.

Take a moment to review Figure 3.6, which displays the relationships among threats, vulnerabilities, and controls. Notice that a threat by itself does not represent a danger and is not sufficient for a successful attack. A threat agent can be described as the actual circumstance or event that does cause harm to information assets through destruction, disclosure, or modification. The sample threat in Figure 3.6 is a web application being hacked. The threat is the possibility that someone might hack the web application. The threat agent is the skilled hacker who will perform that attack, the vulnerability is the unpatched buffer overflow on the web application, and the risk is a measure of how probable it is that this attack will be successful.

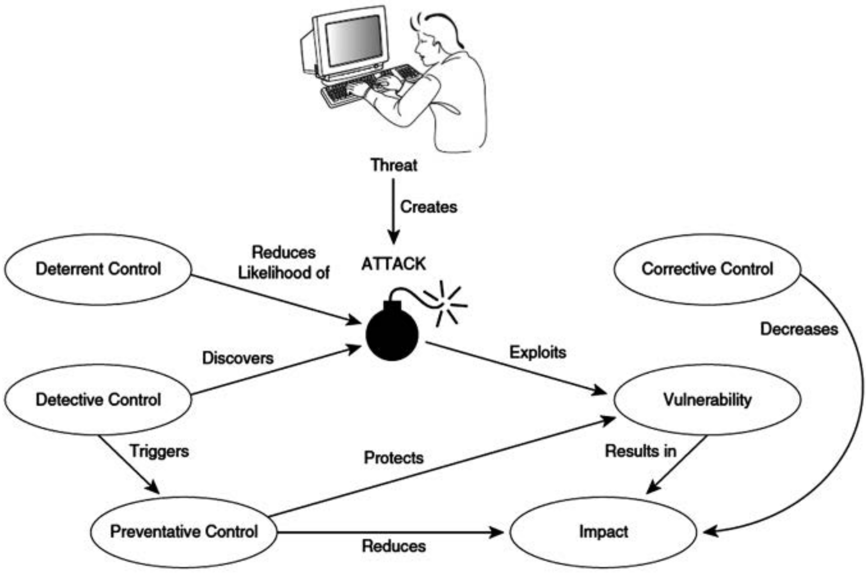


FIGURE 3.6 **Threats, Vulnerabilities, and Controls**

Identifying threats, vulnerabilities, and controls is just part of the risk management process. Without determining dollar values or using some other metric to assess these variables, how can you start to analyze the threats and vulnerabilities that an organization faces? One approach is to develop a table such as the one shown in Table 3.2, which helps demonstrate the relationships among threats, vulnerabilities, and risks. For example, an intruder can represent a threat that might expose the organization to the theft of equipment because there is a vulnerability due to the lack of security guard or controlled entrance. We will look at dollar costs a little later in the chapter, but for now consider the relationships between these items.

TABLE 3.2 **Threat, Vulnerability, and Risk**

Threat Type	Threat	Exploit/Vulnerability	Exposed Risk
Human factor: internal threat	Intruder	No security guard or controlled entrance	Theft
Human factor: external threat	Hacker	Misconfigured firewall	Stolen credit card information
Human factor: internal threat	Current employee	Poor accountability; no audit policy	Loss of integrity; altered data
Natural threat	Fire	Insufficient fire prevention	Damage or loss of life
Natural threat	Hurricane	Insufficient preparation	Damage or loss of life
Malicious external threat	Virus	Out-of-date antivirus software	Virus infection and loss of productivity
Technical internal threat	Hard drive failure	No data backup	Data loss and unrecoverable downtime

The risk management team must gather input from a range of sources in order to identify threats. Sources that might be consulted or considered to help identify current and emerging threats include the following:

- Asset owners
- Network administrators
- Security administrators
- Operations group
- Facility records
- Government records and watchdog groups, such as Computer Emergency Response Team (CERT) and Bugtraq
- Private organizations, such as SANS Institute

A risk management team can examine assets and their associated risks by using dollar or non-dollar methods. By using a quantitative assessment, a team can assign costs (monetary values) to assets and anticipated exposures caused by threats identified in the risk analysis. By using a qualitative assessment method, a team can use scenarios to drive a prioritized list of critical concerns rather than focusing on dollar amounts. Qualitative and quantitative assessment techniques are described in more detail in the following sections.

Quantitative Assessments

Quantitative assessments deal with numbers and dollar amounts. The goal is to assign a cost or a numeric value to the elements of risk assessment and to the assets and threats of a risk analysis.

> ExamAlert
>
> When you hear the word *quantitative*, just remember "quantity." This will help you remember for the CISSP exam that quantitative assessment involves numbers.

To fully complete a quantitative risk assessment, all elements of the process—that is, asset value, impact, threat frequency, safeguard effectiveness, safeguard costs, uncertainty, and probability—are quantified. The problem with purely quantitative risk assessment is that it is difficult, if not impossible, to assign dollar values to all elements. Therefore, some qualitative types of measurements often augment quantitative elements. A quantitative assessment requires substantial time and personnel resources. The quantitative assessment process involves determining several metrics in the following order:

1. **Single loss expectancy (SLE)**: First, you need to determine the single amount of loss you could lose on an asset if a threat were realized. SLE is calculated as follows:

   Single loss expectancy = Asset value × Exposure factor

   Factors to consider when calculating the SLE include the physical destruction or theft of assets, the loss of data, the theft of information, and threats that might cause delays in processing. The exposure factor is the measure or percentage of damage that a realized threat would have on a specific asset.

2. **Annual rate of occurrence (ARO)**: The next step is to determine the likelihood that an unwanted event will occur annually. Simply stated, how many times is this expected to happen in one year?

3. **Annual loss expectancy (ALE)**: This third and final step of the quantitative assessment seeks to combine the potential loss and rate per year to determine the magnitude of the risk. This is expressed as the annual loss expectancy, which is calculated as follows:

   ALE = SLE × ARO

When performing the calculations discussed in this section, you should include all associated costs, such as the following, and ensure that they are considered during the SLE calculation:

- Lost productivity
- Cost of repair
- Value of the damaged equipment or lost data
- Cost to replace the equipment or reload the data

Caution

Quantitative assessment is difficult because it is hard to place a dollar amount on every possible event and to extrapolate all the costs associated with that event.

When these costs are accumulated and specific threats are determined, the ALE can be calculated. This helps you build a complete picture of the organization's risk and allows the organization to plan an effective strategy.

Using the information in Table 3.3, this section works through a computer virus risk example. First, you need to calculate the SLE, which means you need to multiply the asset value by the exposure factor. The asset value is the value you have determined the asset to be worth. The exposure factor is the amount of damage that the risk poses to the asset. For example, the risk-management team might consult with its experts and determine that 17% of Word documents and data could be destroyed due to a virus. The calculation would look as follows:

$\$9,450 \times 0.17 = \$1,650$

Next, you calculate the ARO, which is the frequency at which this event is expected to happen within a given period. For example, the experts might have determined that there is a 90% chance of this event occurring within a one-year period. These numbers are not always easy to determine because insurance and historical records, although helpful, do not always provide a complete picture. This is still a scientific guess with a degree of uncertainty.

Finally, you calculate the ALE by multiplying the SLE by the ARO:

$\$1,650 \times 0.90 = \$1,485$

In this third and final step of the quantitative assessment, you combine the potential loss with the rate per year to determine the magnitude of the risk. You can interpret this figure to mean that the business should expect to lose an average of $1,485 each year due to computer viruses.

TABLE 3.3 **How SLE, ARO, and ALE Are Used**

Asset	Risk	Asset Value	Exposure Factor	SLE	ARO	ALE
Customer database	Hacked	$432,000	0.74	$320,000	0.25	$80,000
Word documents and data files	Ransomware	$90,450	0.17	$10,650	0.90	$1,485
Domain controller	Server failure	$82,500	0.88	$72,500	0.25	$18,125
E-commerce website	DDoS	$250,000	0.44	$110,000	0.45	$49,500

Automated tools that minimize the manual effort required are available. These programs enable you to rerun the analysis with different parameters to answer "what-if" questions. They perform calculations quickly, and you can use them to estimate future expected losses more easily than you could by performing the calculations manually.

Note

Quantitative and qualitative risk assessment can be combined for a comprehensive hybrid risk assessment approach.

Using Quantitative Formulas

In real life, quantitative assessment requires many different variables to be determined. Although these issues are beyond the scope of the CISSP exam, it is important that you see the big picture of risk assessment. For example, let's say that Vandelay Industries has an SQL database that is valued at $850,000. The asset value was derived from the IT systems, resources, applications, and hardware. This would also include the profit potential from the customer database for projected revenue and profitability.

If the SQL database faces a potential threat from a critical software bug that Microsoft has just identified, the potential for a threat being realized is real. Because of this critical security defect, the vendor releases a security bulletin, advising customers of the problem. Because of this known vulnerability, the risk assessment team assigns an exposure factor of 35%. That is, there is a 35% probability that this known vulnerability could be exploited by an attacker. The SLE would be calculated as follows:

SLE = $850,000 (Asset value) × 0.35 (Exposure factor)

= $297,500

If this database also faces a threat from malicious code or malicious software, and the server that the customer database resides in does not have antivirus or other security controls, this could result in a significantly higher exposure factor. The assessment team might provide an 80% probability that a virus, worm, or Trojan may attack the production server and customer database. The SLE would be calculated as follows:

SLE = \$850,000 (Asset value) × 0.80 (Exposure factor)

= \$680,000

It is most important to define a consistent and standard method for probability of occurrence. Doing so allows for consistent and standard SLE calculations so that you can accomplish a ranking and prioritization of IT assets' SLE values. In reality, many sources are used to gather this information. Most teams rely heavily on tools and software to aid in evaluating risk.

Although you do not need to know this information for the CISSP exam, the following are some of the companies that offer tools to aid in the risk assessment process and help with the project management aspects of such tasks:

- **Method123**: www.method123.com
- **Palisade**: www.palisade.com
- **ProjectManagement.com**: www.projectmanagement.com

ExamAlert

Math is a big component of quantitative assessment, and the CISSP exam might require you to use basic formulas such as those for SLE, ALE, and ARO. Memorizing and understanding these formulas will help you fully prepare for the exam.

Qualitative Assessments

Purely quantitative risk assessment is hard to achieve because some items are difficult to tie to fixed dollar amounts. A *qualitative assessment*, as mentioned earlier in this chapter, is scenario driven and does not require assignment of dollar values to components of the risk analysis. Absolute qualitative risk analysis is possible because it involves ranking the seriousness of threats and sensitivity of assets into grades or classes such as low, medium, and high. Table 3.4 provides a sample qualitative scale.

TABLE 3.4 **Qualitative Assessment Impact Scale**

Score	Damage	Trigger Time	Potential Impact
High	Critical	Minutes to hours	Loss of life, failure of business, civil or criminal charges
Medium	Disruptive	Hours to days	Bad PR, loss of customers, loss of prestige, loss of income
Low	Moderate	Days to weeks	Requires workaround, reduces output, might result in a reduction in profit
Insignificant	Minor	Up to one month	Inconvenience

It's important to make consistent and subjective assessments of the risks to specific IT assets. Doing so typically involves a group or team of members participating in the assessment. Asset owners responsible for maintaining the confidentiality, integrity, and availability of an IT asset should have a voice in the process.

The basic steps for a qualitative assessment are as follows:

1. List all the organization's critical IT assets in a spreadsheet.
2. Specify the critical threats and vulnerabilities for each IT asset in the spreadsheet. There might be more than one critical threat or vulnerability for a given IT asset.
3. Develop a consistent exposure severity scale to measure impact. A value from the scale should be assigned according to the IT asset and the specific threat that can be exploited.
4. Organize and prioritize the risk assessment results from the most critical to the least. This will immediately bring to the top of the list those assets that have the greatest risk of exploitation from a threat or vulnerability.
5. Prioritize funds for security controls and security countermeasures for the IT assets that have the greatest importance to the organization and have the greatest exposure to risk.
6. Ensure that the organization's critical IT assets achieve the appropriate confidentiality, integrity, and availability controls, according to the threat and security policy.

The result of the qualitative assessment process is a prioritized list that might look something like the information provided in Table 3.5. Notice in this table that facility power is identified as a critical concern.

TABLE 3.5 **Qualitative Assessment Results**

Asset	Threat	Exposure
Facility power	Loss of power	High
Customer database	Software vulnerability	Medium
Email server	Virus attack	Medium
File server	Loss of data	Low
File server	Hard drive failure	Low

A disadvantage of performing a qualitative assessment is that when you are not working with dollar values, it is harder to communicate the results of the assessment to management personnel, who are used to working with dollar amounts. However, qualitative assessments can be completed quickly.

Qualitative assessment is subjective, based on opinions from the team or experts in the company, but it does not always provide an exact assessment that senior management will want to receive from you. For example, when predicting the possibility of a natural disaster or even human-caused incidents, it is never possible to establish exact numeric certainty.

Qualitative Assessment Types

Qualitative assessments can include many techniques, such as brainstorming, surveys, questionnaires, checklists, one-on-one meetings with asset owners, and interviews. Several particular options are discussed next.

One approach to qualitative risk assessment is the Delphi technique, which is a group approach that is designed to allow individuals to contribute anonymous opinions. The goals with this technique are to avoid being swayed by pushy people, to find synergy, and to allow participants to be honest.

Facilitated Risk Analysis Process (FRAP) is a subjective process that obtains results by asking questions. It is designed to be completed in a matter of hours, so it is a quick process to perform.

The INFOSEC Assessment Methodology (IAM), developed in 1998, is used to review an organization's information security posture, identify potential vulnerabilities, and provide recommendations on eliminating or mitigating those vulnerabilities. It uses confidentiality, integrity, and availability as a basis of assessment.

Another resource for qualitative risk assessment methodologies, NIST 800-53, defines confidentiality, integrity, and availability as categories of loss and ranks each loss based on a subjective ranking that can be any of the following:

- **Low**: Minor inconvenience that could be tolerated for a short period of time.
- **Medium**: Could result in damage to the organization or cost a moderate amount of money to repair.
- **High**: Would result in loss of goodwill between the company and clients or employees. Could result in a legal action or fine or cause the company to lose revenue or earnings.

Table 3.6 provides an example of how this assessment is performed. As you can see, no dollar amounts are used, and potential loss is ranked only as high, medium, or low.

TABLE 3.6 **Performing a Qualitative Assessment**

Asset	Loss of Confidentiality	Loss of Integrity	Loss of Availability
Customer database	High	High	Medium
Internal documents	Medium	Medium	Low
Advertising literature	Low	Medium	Low
HR records	High	High	Medium

Regardless of the method used—quantitative or qualitative—the results of the risk assessment process provide the risk management team with the information needed to make a decision about how to handle risk.

Table 3.7 summarizes the differences between quantitative and qualitative risk assessments.

TABLE 3.7 **Quantitative and Qualitative Risk Assessment**

Property	Quantitative	Qualitative
Provides dollar values	✓	—
Can be automated	✓	—
Very little guesswork	✓	—
No complex math	—	✓

Property	Quantitative	Qualitative
Is user objective	–	✓
Low volume of info	–	✓
Short preparation time	–	✓
Easy to communicate to management	✓	–

Note

There are many ways to perform a qualitative risk assessment. For example, New Zealand uses the ANZ 4360 standard for qualitative risk assessment.

Selecting Countermeasures

After identifying potential risk and estimating its impact, the team must determine how to handle the potential risk. There are three acceptable ways in which the team can respond:

- **Risk acceptance**: This approach involves accepting the fact that you might face costs related to loss if the risk occurs. This option can be chosen when no other options are available or when the potential loss is small compared to the project's benefits. If this is the chosen approach, it is important to prepare contingency plans to make sure you will be able to deal with the risk if it occurs. For example, if your daughter were planning a wedding and had her heart set on a summer wedding on the beach in The Bahamas, you might agree to the location but get the hotel to agree to allow you to hold the event indoors if the weather turns bad. This type of contingency plan can make the situation easier to handle if the risk of bad weather becomes a reality.
- **Risk transference**: The most common example of *risk transference* is insurance, which can transfer a portion or all of the potential cost of a loss to a third party. To transfer the risk, you move ownership of the risk to a third party. The third party assumes the risk, but the organization is saddled with the cost of the insurance. In the case of your daughter's wedding, you might transfer some of the risk by buying hurricane, travel, and hotel insurance. In the real world, risk transference may be a viable option for a continuity of operations (COOP) plan when it comes to replacing tangible items such as furniture, hardware, and buildings for recovery operations following a disaster; however, risk transference really doesn't

work for data protection and reputation. For data protection, encryption and backups are crucial.

- **Risk mitigation**: This approach could mean implementing a countermeasure to alter or reduce the risk. Examples of risk reduction include firewalls and encryption, increased frequency of patch management, and/or stronger authentication. Consider again the example of your daughter's wedding. To reduce the risk, you might ask her to postpone the wedding until next spring to reduce the chance of encountering a major storm.

> **Note**
>
> Some sources list risk avoidance as another option. This simply means that you avoid the activity to avoid the risk. Depending on the situation, however, risk avoidance may not be possible.

What approach is the right one? It depends on the cost of the countermeasure, the value of the asset, and the amount by which risk reduction techniques reduce the total risk to a value that is acceptable.

Acceptable risk or *risk tolerance* is the minimum acceptable risk that an organization is willing to tolerate. When assessing safeguards, it's important to look at the total cost of ownership (TCO), which includes purchase price, maintenance fees, updates, insurance, and all other costs. The risk assessment team must try to find a solution that provides the greatest risk reduction while maintaining the lowest annual cost. These concepts are expressed numerically by the following formula:

Threat × Vulnerability × Asset value = Total risk

No organization can ever be 100% secure. There will always be some risk left after safeguards and controls have been put in place; this is known as *residual risk*. The formula for residual risk is as follows:

(Threat × Vulnerability × Asset value) × Controls gap = Residual risk

The objective is to balance the cost of control against the value of the asset and potential for loss—and to avoid spending more on the control than the cost of the asset itself (see Figure 3.7).

> **Note**
>
> Any risk involving human life is extremely high and should be given the highest priority.

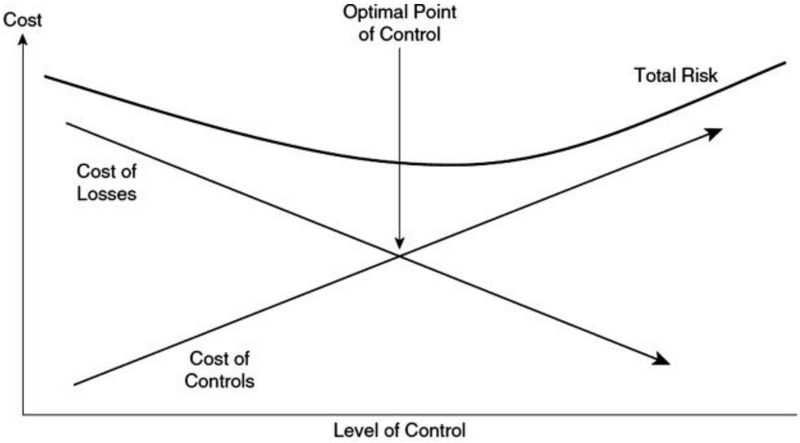


FIGURE 3.7 **Cost of Risk Versus Level of Control**

At the completion of the risk-handling step, the risk assessment team produces a final report that presents all the findings, information, assessments, and recommendations for the organization. The final assessment report becomes the instrument used by management to make sound business decisions pertaining to the organization's overall risk and vulnerability assessment; it is the basis for how the organization will mitigate the identified risks, threats, and vulnerabilities.

Note

The cost–benefit analysis of a safeguard or protection measure is measured as the control gap:

> ALE before the safeguard – ALE after the safeguard = Control gap (value of the safeguard to the organization)

This formula can be used to evaluate the cost-effectiveness of a safeguard or to compare various safeguards to determine which are most effective. The higher the resulting value, the more cost-effective the safeguard. In most cases, you want to avoid spending more funds on a control than the cost of the asset itself. However, this is not always true. For example, federal, state, and local governments may sometimes provide controls to protect critical systems regardless of the cost of the controls. As discussed earlier in this chapter, it is not always easy to measure the potential for damage with a numeric value.

ExamAlert

Some organizations use a risk analysis matrix, which looks at likelihood and impact. For an example, see MITRE's Risk Matrix, at https://www.mitre.org/research/technology-transfer/open-source-software/risk-matrix.

Threat Modeling Concepts and Methodologies

Threat modeling is a structured approach to evaluating threats. Threat modeling is typically used during the planning, design, and implementation of security controls to validate that countermeasures are effective and placed where needed. When done periodically, threat modeling can also help security teams ensure that protections are sufficient based on known or emerging threats. If threat modeling is not done on a periodic basis, new threats may remain unsecured, leaving systems and data vulnerable.

Threat Modeling Steps

The general steps in the threat modeling process are as follows:

1. **Identify assets**: This step includes making an inventory of what applications are used, where those assets are located, and what security measures are in place. Knowing such things as when new assets are brought online or whether assets go live without the prescribed security controls is key to managing and reducing risk.

2. **Conduct threat intelligence**: Threat intelligence should be focused on three areas: assets, attackers, and software. You should have a good understanding of the tools and techniques used to exploit vulnerabilities and the motivations of the attackers. Another approach is to build an attack tree.

3. **Model and categorize threats**: You can use multiple methodologies to categorize and catalog threats. Two methodologies, STRIDE and DREAD, are discussed later in this chapter.

4. **Map and diagram potential attacks**: One approach to this step is to use a process flow diagram, which provides a high-level view of the system and focuses on the ways users and executing code move through a system. Another approach is to build an attack tree, which consists of a series of parent and child nodes representing different events. The root node, which is the topmost parent in the diagram, is the overall goal of the attack. The child nodes must test as true in order for the parent nodes to be true. The goal is for threat modelers to see what set of circumstances must come together in order for a threat to be successful.

5. **Mitigate threats**: Mitigation capabilities generally refer to technology to protect, detect, and respond to a certain type of threat. For threat mitigation to be successful, the threat modeling team must decompose the application, understand trust boundaries and input points, and rank the discovered threats. Identified threats need to be prioritized, and controls need to be deployed to remediate identified threats.

Note

Some of the common ways to reduce threats identified during threat modeling include the following:

- Providing more training to staff
- Changing business processes or procedures
- Implementing administrative controls such as rotation of duties or dual controls
- Changing an application's configuration
- Modifying source code
- Using technical controls such as web application firewalls, proxies, or other screening and filtering devices

Threat Modeling Tools and Methodologies

As mentioned earlier, a number of threat modeling tools and methodologies are in use. For example, Microsoft developed STRIDE, which stands for the following.

- **Spoofing**: Using a falsified identity
- **Tampering**: Making unauthorized changes
- **Repudiation**: Ensuring plausible deniability
- **Information disclosure**: Distributing information to external or unauthorized entities
- **Denial of service (DoS)**: Preventing unauthorized use of a resource
- **Elevation**: Using a limited user account to gain greater access

Another methodology is OpenStack's DREAD, which provides a rating system and is designed to be flexible. DREAD considers the following:

- **Damage potential**: How severe is the damage likely to be?
- **Reproducibility**: How complicated is it for attackers to reproduce the exploit?
- **Exploitability**: How hard is it to perform the attack?
- **Affected users**: What percentage of users are going to be affected?
- **Discoverability**: How hard is it for an attacker to discover this weakness?

PASTA (Process for Attack Simulation and Threat Analysis) is a seven-step process focused on aligning technical security requirements with business objectives. Each step consists of several substeps. The sequence is as follows:

1. Define the objectives.
2. Define the technical scope.
3. Perform application decomposition.
4. Conduct threat analysis.
5. Conduct vulnerability and weaknesses analysis.
6. Conduct attack modeling.
7. Conduct risk and impact analysis.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a threat modeling methodology developed at Carnegie Mellon University that focuses on organizational risks rather than technological risks. It consists of three phases:

1. Build asset-based threat profiles.
2. Identify infrastructure vulnerabilities.
3. Develop a security strategy and plans.

VAST (Visual, Agile, and Simple Threat Modeling) is an automated threat modeling platform that distinguishes between application and operational threat models. VAST was created to be integrated into workflows built around the DevOps philosophy.

Trike is a threat modeling platform that operates from a defensive viewpoint rather than trying to emulate the thought process of the threat actor. It is different from the other methodologies in that it has you model the system you are trying to defend.

Regardless of which methodology you deploy, it is most important to start this process in system development. It is cheaper to build in controls early than to wait until later and attempt to add them.

Managing Risk with the Supply Chain and Third Parties

Today, multinational corporations often operate in different parts of the world and use a variety of vendors, contractors, and suppliers. As reliance on these third parties continues to grow, so does the need to manage a number of relationships.

For example, say that you are the CISO for a company that manages a natural gas pipeline and a power generating plant. You would have many supervisory control and data acquisition (SCADA) devices, IP cameras, automated pumps, sensors, computers, and so on as a part of your production control system. In this case, you would be concerned with who are you buying these from and can the vendor be trusted and whether these devices are compliant with your needs.

This is where supply chain risk management comes in. Supply chain risk management involves applying techniques to manage and understand risk along the supply chain. In our example, a large portion of the power plant's equipment is commercially available technology that uses either Microsoft Windows or the Linux operating system, which are common targets for hackers. To reduce the supply chain risk, you might carry out a continuous risk assessment to reduce vulnerabilities and ensure continuity of operations.

Supply chain risk management (SCRM) is but one small piece of the process you must consider. Third-party entities must verify compliance with all stated security objectives, requirements, regulations, and contractual agreements. The following are some of the documents, agreements, and memorandums used for third-party governance:

- **Interconnection security agreement (ISA)**: An ISA is a security document that specifies the requirements for establishing, maintaining, and operating an interconnection between systems or networks or between an agency and eternal systems. The document lists the requirements for connecting the systems and networks and details what security controls are to be used to protect the systems and sensitive data with external systems. An ISA typically maintains a drawing of the network topology and details how specific systems and networks are connected with external systems.

- **Interoperability agreement (IA)**: An IA is a document that specifies any and all requirements for sharing and maintaining information between companies so they can exchange and share data. For example, if United Airlines code-shares flights with Hawaiian Airlines, both companies need access to a common data set.
- **Memorandum of understanding (MOU)**: An MOU is a document that specifies terms and conditions for outsourcing partner organizations that must share data and information resources. To be legally binding, an MOU must be signed by a representative from each organization that has the legal authority to sign. Such documents are typically secured, as they are considered confidential.
- **Authorization to operate (ATO)**: An ATO is a formal statement that authorizes operation of an information system and/or application and indicates agreement with the system security plan to include the associated risks.
- **Continuity of operations plan (COOP)**: Things will go wrong, and a COOP specifies the processes and procedures that an organization must put in place to ensure that the business can continue to operate when those problems arise.
- **Service-level agreement (SLA)**: An SLA is sometimes used in conjunction with an ISA or an MOU. If an outsourcing provider with which you have signed an MOU is going to provide a time-sensitive service, implementing an SLA is one way to obtain guarantees of the level of service the partner is agreeing to provide. The SLA should specify the uptime, response time, and maximum outage time that the provider is agreeing to. For a service fee, the provider agrees to repair or replace the equipment within the contracted time.
- **Operating-level agreement (OLA)**: AN OLA functions in conjunction with SLAs in that it supports the SLA process. The OLA defines the responsibilities of each partner's internal support group. For example, while an SLA may promise no more than five minutes of downtime, an OLA would define which group and resources will be used to meet that downtime goal.
- **Uptime agreement (UA)**: A UA details the agreed amount of uptime, usually as a percentage. For example, UAs can be used for network services, such as a WAN link, or equipment, such as a server. It's common to see uptimes like 99.999%, which is equal to about five minutes' downtime per year.

- **Nondisclosure agreement (NDA)**: An NDA is used to protect confidential information. For example, before taking the CISSP exam, you will be asked to sign an NDA, stating that you will not reveal exam questions to others.
- **Business partnership agreement (BPA)**: A BPA is a legally binding document that is designed to provide safeguards and compel certain actions among business partners in relation to specific security-related activities. A BPA is a written agreement created by lawyers along with input from the partners; it contains standard clauses related to security and cooperation.

Note

One item you should review when dealing with business partners is the Statement of Auditing Standards 70 (SAS 70). The SAS 70 report verifies compliance and ensures that the outsourcing or business partner has had its control objectives and activities examined by an independent accounting and auditing firm.

Reducing Risk in Organization Processes

Risk management requires an understanding of an organization and its time-sensitive business requirements. Nothing stays static in business. Organizational units change, products and services are added and removed, and portions of a business may be spun off or divested. This section discusses some of the common types of events that a security professional may have to deal with.

First, there are mergers and acquisitions. A *merger* is a combination of two or more commercial entities into a single surviving entity. From the standpoint of risk, many things can go wrong with a merger. Businesses typically look for synergy, but some businesses just don’t fit together. Regardless of the situation, some questions must be asked before a merger. Is the merger a win for both companies? Is the purpose of the merger to siphon off resources, such as talent and intellectual property, and then spin off a much weaker company later?

Sometimes companies enter a merger or acquisition phase without an adequate plan of action. Doing so can potentially lead to security exposures and increased expenditures.

In addition, many people don’t like change. Once a company culture is established and people become set in their ways, attitudes can be hard to change. Mergers are all about change, and that goes against what many employees expect.

Security professionals are commonly asked to quickly establish connectivity with proposed business partners. While there is a need for connectivity, security should remain a driving concern. You need to understand the proposed merger partner's security policies and what controls are being enforced. You do not want to allow an attacker's entry into your network through the merging company's network.

There will always be security concerns when it comes to merging diverse companies. You should be concerned with items such as the following:

- **Rules**: What is or is not allowed by each individual company?
- **Policies**: High-level documents outline the security goals and objectives of the company.
- **Regulations**: Diverse entities may very well be governed by different regulatory entities or regulations, such as PCI-DSS or HIPAA.
- **Geography**: A company that is located in London, England, will be operating on different standards than one that is based in San Jose, California.
- **Demerger/divestiture**: Any time businesses break apart, you must deal with many of the same types of issues as when they merge.
- **Trust or clearance level**: It is important to know the level of access or control of any current or new employees accessing information.
- **Skill set, training, and awareness**: It is important to know the level of training among users and employees who have access to company information systems.

Identifying and Prioritizing Business Continuity Requirements Based on Risk

There are many different approaches to business continuity plans (BCPs). Some companies address these processes separately, whereas others focus on a continuous process that interweaves the plans. NIST offers a good example of the contingency process in SP 800-34, *Continuity Planning Guide for Information Technology Systems*. This publication defines the BCP/disaster recovery plan (DRP) process as follows:

ExamAlert

A disaster recovery plan (DRP) is part of a business continuity plan (BCP) but deals more with technology and short-term issues such as what to do immediately to get critical systems and services running. A BCP, in contrast, lays out what a company does to stay in business and return to normal operations. You must know the difference for the CISSP exam.

1. Develop the contingency planning policy statement.
2. Conduct the business impact analysis (BIA).
3. Identify preventive controls.
4. Develop recovery strategies.
5. Develop an IT contingency plan.
6. Test the plan, train employees, and hold exercises.
7. Maintain the plan.

Before we go further, we should define the terms *disaster* and *business continuity*. A *disaster* is any sudden, unplanned calamitous event that brings about great damage or loss. Entire communities have concerns following a disaster; however, businesses face special challenges because they have responsibilities to protect the lives and livelihoods of their employees and to guard company assets on behalf of shareholders. In the business realm, a disaster can be seen as any event that prevents the continuance of critical business functions for a predetermined period of time. In other words, an outage might force the declaration of a disaster.

ExamAlert

For the CISSP exam, keep in mind that human safety always comes first and has priority over all other concerns.

Business continuity is the process of sustaining the operation of a critical business function (CBF) to keep the company in business for the long term. The goal of business continuity is to reduce or prevent outage time and optimize operations. The Business Continuity Institute (www.thebci.org), a professional body for business continuity management, defines *business continuity* as a holistic management process that identifies potential impacts that threaten an organization, provides a framework for building resilience, ensures an effective response, and safeguards its reputation, brand, value, and the interests of key stakeholders.

Although a number of methodologies can be used to complete the BCP/DRP process, this chapter describes the steps that most closely align with reference documentation recommended by (ISC)^2. Figure 3.8 provides an overview of the process, which includes the following steps:

1. Project initiation
2. Business impact analysis (BIA)
3. Recovery strategy
4. Plan design and development
5. Implementation
6. Testing
7. Monitoring and maintenance

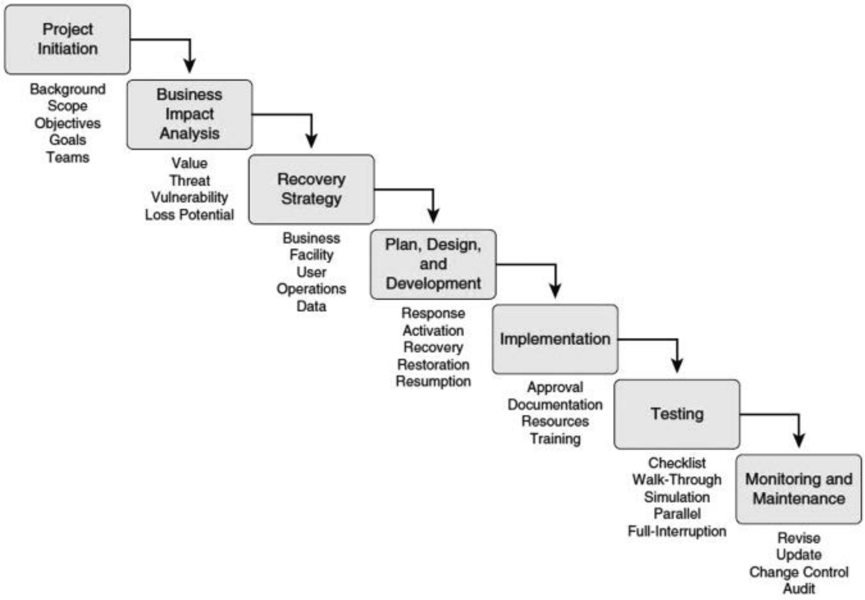


FIGURE 3.8 **BCP/DRP Process**

We discuss project initiation and business impact analysis in this chapter and the other steps illustrated here in Chapter 8, "Security Operations."

Project Management and Initiation

Before the BCP process can begin, it is essential to have the support of senior management because they are responsible for setting the budget, determining the team leader, and starting the BCP process.

Without senior management support, you will not have funds to successfully complete the project, and your efforts will be at best marginally successful. One way to gain their support is to prepare and present a seminar for them that overviews the risks the organization faces, identifies basic threats, and documents the costs of potential outages. This is a good time to remind them that, ultimately, they are legally responsible. Customers, shareholders, stockholders, or anyone else could bring civil suits against senior management if they feel the company has not practiced due care.

Senior management must choose a team leader. This individual must have enough credibility with senior management to influence them in regard to BCP results and recommendations. After the team leader is appointed, an action plan can be established, and the team can be assembled. Members of the team should include representatives from management, legal staff, recovery team leadership, the information security team, various business units, the networking team, and the physical security team. It is important to include asset owners and the individuals who would be responsible for executing the plan.

Next, you need to determine the project scope. A properly defined scope is of tremendous help in maximizing the effectiveness of a BCP. You cannot protect everything, and you really do not need to, either. For example, if you are planning for a company that has offices in California, Florida, New York, and North Dakota, you would not have contingency plans for hurricanes for all offices.

It is important to be sensitive to interoffice politics, which can derail the planning process. Another problem to avoid is *project creep*, which occurs when more and more items that were not part of the original project plan are added to it. Creep can delay completion of the project and can also cause it to run over budget.

A BCP benefits from adherence to traditional project plan phases. Issues such as resources (personnel and financial), time schedules, budget estimates, and any critical success factors must be managed. You can schedule an initial meeting to kick off the process.

Finally, the team can get to work. The team can expect to have a host of duties and responsibilities, including the following:

- Identifying regulatory and legal requirements that must be complied with
- Identifying all possible threats and risks

- Estimating the probability of these threats and correctly identifying the loss potential of each one
- Performing a BIA
- Outlining the priority order in which departments, systems, and processes must be up and running
- Developing procedures and outlining steps for resuming business functions following a disaster
- Assigning crisis situation tasks to employee roles or individuals
- Documenting plans, communicating plans to employees, and performing necessary training and drills

It's important for everyone on the team to realize that the BCP is the most important corrective control the organization will have and to use the planning period as an opportunity to shape it. The BCP is more than just corrective controls; the BCP also needs to reflect preventive and detective controls:

- **Preventive controls**: Including controls to identify critical assets and prevent outages
- **Detective controls**: Including controls to alert the organization quickly in the event of outages or problems
- **Corrective controls**: Including controls to restore normal operations as quickly as possible

Business Impact Analysis

The next task is to create the BIA, which measures the impact each type of disaster could have on critical or time-sensitive business functions. It is necessary to evaluate time as a metric, just as you would the importance of the function. For example, paying employees is not critical from the perspective of business activities, but if you don't pay them on time, your company will likely go out of business because it will lose its employees.

Creating the BIA is an important step in the process because it involves considering all threats and the implications of those threats. For example, the city of Galveston, Texas, is on an island known to be prone to hurricanes. Although it might be winter in Galveston and the possibility of a hurricane is extremely low, planning can still take place to reduce the potential negative impact of a hurricane in the future. It is important to think through all possible disasters, assess the risks of those disasters, quantify the impacts, determine the potential losses, and identify and prioritize operations that would require disaster recovery planning in the event of those disasters.

The BIA must answer three vital questions:

- **What is most critical?**: Prioritization is important for determining what processes are most critical to the organization.
- **What is the longest outage the company can endure?**: The downtime estimation is performed to determine which processes must resume first, second, third, and so on and to determine which systems must be kept up and running.
- **What resources are required?**: Resource requirements must be identified and require correlation of system assets to business processes. For example, a generator can provide backup power but requires fuel to operate.

> **Note**
>
> Criticality prioritization is something that companies do all the time. Consider the last time you phoned your favorite computer vendor to order new equipment. How long were you placed on hold? Your call was probably answered within a few minutes. In contrast, how long was the wait the last time you phoned the same company to speak to the help desk? It was likely much longer.

The development of multiple scenarios should provide a clear picture of what is needed to continue operations in the event of a disaster. The team creating the BIA needs to look at the organization from many different angles and use information from a variety of sources. Different tools can be used to help gather data. Strohl Systems' BIA Professional and SunGard's Paragon software can automate portions of the data input and collection process. Although the CISSP exam will not require that you know the names of various tools, it does expect you to understand how the BIA creation process works, and it helps to know what tools are available.

Whether the BIA is created manually or with the assistance of tools, its completion will take some time. Any time individuals are studying processes, techniques, and procedures they are not familiar with, a learning curve is involved.

As you might be starting to realize, creating a BIA is no easy task. It requires not only knowledge of business processes but also a thorough understanding of the organization itself, including IT resources, individual business units, and the interrelationships between them. This task requires the support of senior management and the cooperation of IT personnel, business unit managers, and end users. The general steps within in the BIA creation process are as follows:

1. Determine data-gathering techniques.
2. Gather BIA data.
3. Identify critical business functions and resources that support these functions.
4. Verify the completeness of data.
5. Establish the recovery time for operations.
6. Define recovery alternatives and costs.

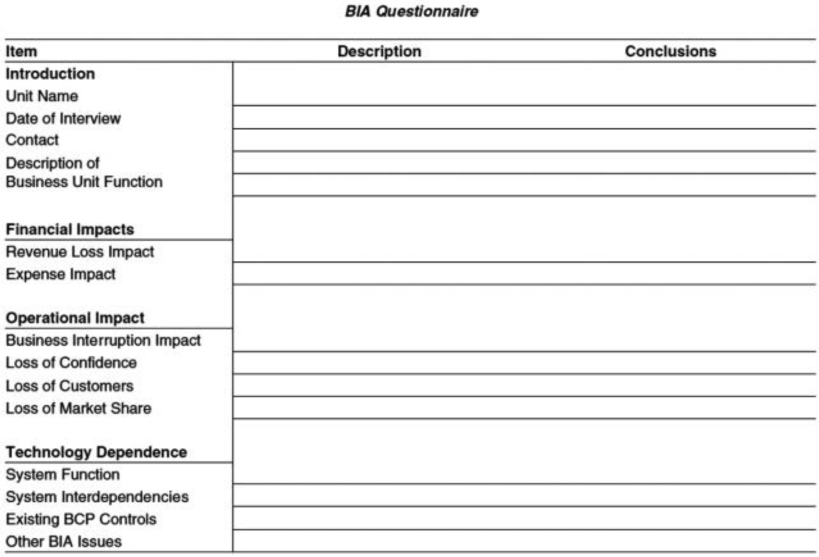
Note

A vulnerability assessment is often included in a BIA. Although this assessment is conducted in much the same way as a risk assessment (see Chapter 7, "Security Assessment and Testing"), a vulnerability assessment focuses on providing information specifically for the business continuity plan.

Assessing Potential Loss

There are a variety of approaches to assessing potential loss. One of the most popular methods is to use a questionnaire that is distributed to senior management and end users. The objective of the questionnaire is to maximize the identification of potential loss by the people engaged in business processes that would be jeopardized by a disaster. This questionnaire might be distributed and independently completed or filled out during an interactive interview process. Figure 3.9 shows a sample of this type of questionnaire.

The questionnaire can also be completed in a round table setting. In fact, this sort of group completion can add synergy to the process, as long as the dynamics of the group allow for open communication and the required key individuals can all schedule and meet to discuss the impact that specific types of disruptions would have on the organization. It is crucial to include all key individuals because management might not be aware of critical key tasks for which they do not have direct oversight.



BIA Questionnaire

Item	Description	Conclusions
Introduction		
Unit Name		
Date of Interview		
Contact		
Description of Business Unit Function		
Financial Impacts		
Revenue Loss Impact		
Expense Impact		
Operational Impact		
Business Interruption Impact		
Loss of Confidence		
Loss of Customers		
Loss of Market Share		
Technology Dependence		
System Function		
System Interdependencies		
Existing BCP Controls		
Other BIA Issues		

FIGURE 3.9 BIA Questionnaire

Using a questionnaire is a qualitative technique for assessing risk. Qualitative assessments are scenario driven and do not attempt to assign dollar values to anticipated losses. A qualitative assessment ranks the seriousness of an impact using grades or classes, such as low, medium, high, or critical:

- **Low**: This is a minor inconvenience that customers might not notice. Outages could last for up to 30 days without any real inconvenience.
- **Medium**: Loss of service would impact the organization after a few days to a week. Longer outages could affect the company's bottom line or result in loss of customers.
- **High**: Only short-term outages of a few minutes to hours could be endured. Longer outages would have severe financial impacts. Negative press might also reduce the outlook for future products and services.
- **Critical**: Outage of any duration cannot be endured. Systems and controls must be in place or must be developed to ensure redundancy so that no outage occurs.

This sort of grading process enables quicker progress in the identification of risks and provides a means of classifying processes that might not easily be assigned dollar values. This will also help you understand the appropriate recovery techniques or technologies based on the level of criticality. Table 3.8 provides an example of qualitative ranking.

TABLE 3.8 **Example of Qualitative Ranking**

Asset or Resource	Availability	Integrity	Confidentiality
Application server	High	Medium	Critical
Firewall	High	Low	Low
Web server	Medium	High	Low
HR database	High	High	Critical

The BIA can also be undertaken using a quantitative approach. This method of analysis involves attempting to assign a monetary value to every asset, exposure, and process identified during the risk assessment. These values are then used to calculate the material impact of a potential disaster, including both loss of income and expenses. A quantitative approach requires the following steps:

1. Estimate the potential losses and determine the single loss expectancy (SLE).
2. Complete a threat frequency analysis and calculate the annual rate of occurrence (ARO).
3. Determine the annual loss expectancy (ALE).

The process of performing a quantitative assessment is covered in much more detail earlier in this chapter. It is important that a quantitative study include all associated costs resulting from a disaster, including those related to the following:

- Lost productivity
- Delayed or canceled orders
- Repairs
- The value of the damaged equipment or lost data
- Rental equipment
- Emergency services
- Equipment replacement and data reloading

Both quantitative and qualitative assessment techniques require the BIA team to examine how the loss of service or data would affect the company. Both methods seek to reduce risk and plan for contingencies, as shown in Figure 3.10.

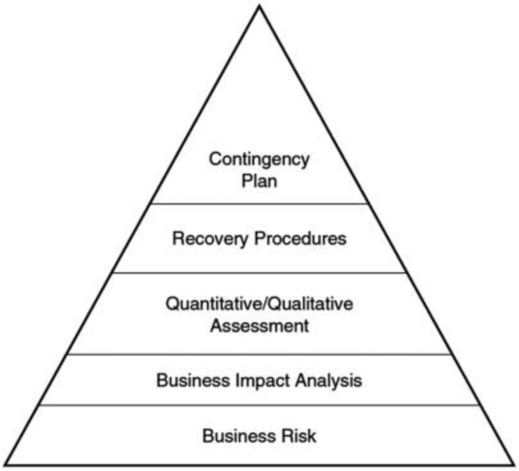


FIGURE 3.10 Risk Reduction Process

The severity of an outage is generally measured by considering the *maximum tolerable downtime* (*MTD*) that the organization can survive without that resource, function, or service.

Tip

For the CISSP exam, you need to know the term *maximum tolerable downtime (MTD)* and understand that this is the maximum time that a business can survive without a service.

Will there be a loss of revenue or operational capital, or will the organization be held legally liable? Although the BIA team might be focused on what the immediate effect of an outage would be, costs are not necessarily immediate. For example, an organization's reputation could be tarnished. In addition, many organizations are subject to regulatory requirements; in such a case, the result of an outage could be a legal penalty or fine.

The Value of a Reputation

Although some organizations might focus solely on dollar amounts when working through a BIA, reputation also needs to be considered. As Benjamin Franklin said, "It takes many good deeds to build a good reputation, and only one bad one to lose it." To illustrate this point, consider the following brand names and their business reputations:

1. **Cisco**: An industry leader of quality networking equipment
2. **Ruth's Chris Steak House**: An upscale eatery known for serving high-quality steaks seared at 1800° Fahrenheit

3. **Tesla**: The bestselling electric car manufacturer from 2018 to 2020
4. **Enron**: A symbol of corporate fraud and corruption
5. **Samsung**: The world's largest smartphone maker, which was forced to discontinue and recall the Galaxy 7 after some devices burst into flames, costing the company more than $5 billion
6. **Volkswagen**: A well-known auto maker that was scarred by a public relations thrashing over its "Dieselgate" scandal

Perhaps your vision of the companies listed is different from what I've written here. My goal in presenting this list is to demonstrate that well-known corporate names generate visions when people hear and read them. Companies work hard for years to gain respect and positive reputation. Catastrophes don't just happen. Most occur because of human error or as a result of a series of overlooked mistakes. Will a mistake be fatal to your organization? Reputations can be easily damaged. That is why disaster recovery is so important: The very future of your organization may rest on it.

Developing and Implementing Security Policy

Security is truly a multilayered process. After an assessment is completed, administrative controls should be reviewed. Policies can be created or modified based on the results of the risk assessment. The assessment should help drive policy creation on items such as the following:

- Passwords
- Patch management
- Employee hiring and termination practices

Note

Low-level checks refer to checks completed for employees starting at low-level jobs. Before these employees move to higher-level positions, additional checks should be performed. Some companies are even moving to conducting rolling and continuous background checks.

- Backup practices and storage requirements
- Security awareness training
- Antivirus
- System setup and configuration
- System hardening

For security to be effective, it must start at the top of an organization and permeate every level of the hierarchy. Senior management must make decisions on what should be protected, how it should be protected, and to what extent it should be protected. Their decisions should then be crafted into written documents.

Before these documents are locked in as policies, they must be researched to verify that they will be compliant with all federal, state, and local laws. These documents should also clearly state what is expected from employees and how the company will deal with policy violations.

Security Policy

Policies are high-level documents developed by senior management to transmit the guiding strategy and philosophy of management to employees. Management and business process owners are responsible for the organization and for designing policies that will guide it toward success. Policies apply a strong emphasis to words spoken by management. They define, detail, and specify what is expected from employees and how management intends to meet the needs of customers, employees, and stakeholders. A policy is a high-level document that provides a general statement about the organization's assets and what level of protection they should have. Well-written policies spell out who's responsible for security, what needs to be protected, and what is an acceptable level of risk. They are much like a strategic plan in that they outline what should be done but don't specifically dictate how to implement the stated goals. Security policies can be written to meet advisory, informative, and regulatory needs. Each policy has a unique role or function. Table 3.9 shows the relationships between policies, standards, and procedures and strategic, tactical, and operational control.

TABLE 3.9 **Documentation/Level of Control**

Level/Document	Policy	Standard	Procedure
Strategic	✓	—	—
Tactical	—	✓	—
Operational	—	—	✓

One specific type of policy is the organization's *security policy*. A security policy codifies management's commitment to the use, operation, and security of information systems. It specifies the role security plays within the organization. A security policy should be driven by business objectives and should meet all applicable laws and regulations. It should also be used as a basis to integrate security into all business functions. It serves as a high-level guide to develop lower-level documentation such as procedures (see Figure 3.11). A security policy must be balanced in order to help an organization implement adequate security without hindering productivity.

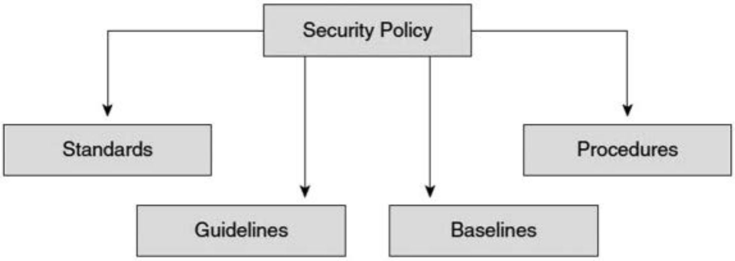


FIGURE 3.11 **Policy Structure**

Policies can come in many forms. Policies can be advisory, informative, or regulatory. The following sections review these types of policies and should help you understand how policies can be designed to meet a variety of goals.

Advisory Policy

The job of an advisory policy is to ensure that all employees know the consequences of certain behavior and actions. Here's an example of an advisory policy:

> Illegal copying: Employees should never download or install any commercial software, shareware, or freeware onto any network drives or disks unless they have written permission from the network administrator. Be prepared to be held accountable for your actions, including the loss of network privileges, written reprimand, probation, or employment termination if the Rules of Appropriate Use are violated.

Informative Policy

An informative policy is not designed with enforcement in mind; it is developed for educational purposes, to inform and enlighten employees. The following is an example of an informative policy:

> In partnership with Human Resources, the employee ombudsman's job is to serve as an advocate for all employees, providing mediation between employees and management. This job is to help investigate complaints and mediate fair settlements when a third party is requested.

Caution

Good policy strikes a balance and is both relevant and understandable. If a policy is too generic, no one will care what it says because it doesn't apply to the company. If a policy is too complex, no one will understand it, and many will be unlikely to read it.

Regulatory Policy

Regulatory policies are used to make certain that the organization complies with local, state, and federal laws. Regulatory policy reinforces applicable laws and administrative laws, such as HIPAA, FERPA, and SOX; it also explains the applicable parts of specific laws in a way that employees can understand. A security professional should work closely with the HR and legal departments in formulating this type of policy. The following is an example of a regulatory policy:

> Because of recent changes to Texas State law, the Company will now retain records of employee inventions and patents for 10 years; all email messages and any backup of such email associated with patents and inventions will also be stored for 10 years.

Standards

Standards are much more specific than policies. Standards are tactical documents that lay out specific steps or processes required to meet certain requirements. For example, a standard might set a mandatory requirement that all email communication be encrypted. Although the standard does specify encryption, it doesn't spell out how it will be accomplished; that is left for the procedure.

Baselines

A *baseline* is a minimum level of security that a system, network, or device must adhere to. Baselines are usually mapped to industry standards. For example, an organization might specify that all computer systems comply with a minimum Trusted Computer System Evaluation Criteria (TCSEC) C2 standard. TCSEC standards are discussed in detail in Chapter 4, "Security Architecture and Engineering." A security policy might also address the minimum baseline standard for encryption requirements for sensitive data.

Guidelines

A guideline points to a statement in a policy or procedure by which to determine a course of action. It is a recommendation or suggestion of how things should be done. A guideline is meant to be flexible so that it can be customized for individual situations.

Caution

Don't confuse guidelines with best practices. Whereas guidelines are used to determine a recommended course of action, best practices are used to gauge liability. Best practices state what other competent security professionals would have done in the same or similar situation.

Procedures

A procedure is the most specific of security documents. A *procedure* is a detailed, in-depth, step-by-step document that details exactly what is to be done. As an analogy, when my mom sent my wife the secret recipe for a German chocolate cake, it described step-by-step what needed to be done and how. It even specified a convection oven, which was listed as an absolute requirement.

Procedures are detailed documents that are tied to specific technologies and devices. You should expect to see procedures change as equipment changes. For example, imagine that your company replaces its Check Point border device, such as a firewall, VPN, or IDS, with a Cisco border device. Although the policies and standards dictating the device's role in your organization probably will not change, the procedure for configuring the firewall will.

It's unfortunate, but sometimes policies and procedures are developed in response to a negative event or an audit. The audit or policy shouldn't be driving the process; the risk assessment should be. The purpose of the assessment is to give management the tools needed to examine all currently identified concerns. From this, management can prioritize the level of exposure they are comfortable with and select an appropriate level of control. This level of control should then be locked into policy.

Types of Controls

One of the main reasons an organization should have a variety of control types is to provide true defense in depth. Each control type provides a different level of protection, and because each level can be tweaked to meet the needs of the organization, a security administrator has a very granular level of control over the security mechanisms. Security mechanisms can serve many purposes, although they are primarily used to prevent, detect, or recover from problems. The best approach is for an organization to focus the bulk of its controls on prevention because this allows the organization to stop problems before they start.

The three access control types—administrative, technical, and physical controls—are covered in the following sections.

Administrative Controls

Administrative controls are the policies and procedures implemented by an organization. Preventive administrative controls can include security awareness training, strong password policies, HR practices, and robust pre-employment checks.

The Need for Robust HR Practices

On February 20, 2006, Dave Edmondson resigned his position as CEO of RadioShack. What would cause a CEO to step down?

Mr. Edmondson had come under increasing pressure to explain errors noted in his educational background. Although company records indicated that Edmondson had received a college degree, the college listed could not confirm that Mr. Edmondson had, in fact, earned a degree. RadioShack downplayed the incident by stating that, at the time Edmondson was hired in 1994, the company did not perform educational checks on employees even if they were hired into senior management positions.

Although it would be nice to think that this was an isolated incident, in May 2012, the CEO of Yahoo! stepped down due to a misrepresentation in his resume and errors in the listing of his degrees. Although many of us might see good HR practices as a nonissue, the truth is that they play a key role in ensuring that the right person is hired for a specific job (articles.latimes.com/2012/may/14/business/la-fi-yahoo-thompson-resigns-20120514).

Note

Does your company enforce acceptable use policies (AUPs)? Using AUPs is considered one of the best ways to deter unacceptable activity.

Technical Controls

Technical controls are logical controls put in place to protect the IT infrastructure. Technical controls include strong authentication (such as biometrics or two-factor authentication), encryption, network segmentation, DMZs, and antivirus controls.

Physical Controls

Physical controls are controls that you can most likely see. These controls protect against theft, loss, and unauthorized access. Examples of physical access controls include guards, gates, locks, guard dogs, closed-circuit television (CCTV), and alarms.

Access Control Categories

Access controls can be used with different levels of granularity to provide different levels of control. There are several categories of access controls (see Table 3.10):

- **Deterrent**: These controls deter users from committing security violations.
- **Preventive**: These controls prevent incidents. An example of this control could be the use of encryption.
- **Detective**: These controls alert and aid in identification after an incident.
- **Corrective**: These controls repair damage and restore systems after an incident. An example might be applying patches.
- **Recovery**: These controls restore normal operations. An example might be the deployment of backups.
- **Compensating**: These controls limit the damage or act to contain an event or incident.

> **Note**
>
> Some controls can fit in more than one category. For example, locks are not a preventive control but can be a deterrent.

TABLE 3.10 **Access Control Types and Examples**

Attribute	Deterrent	Preventive	Detective	Corrective	Recovery	Compensating
Administrative	AUP	User registration	Audit policy	Reassignment or termination	Incident response plan	Supervision and monitoring
Technical	Warning banner	ACLs	Antivirus	Reboot or restart	Hot site	Redundant server
Physical	Electric fence sign	Eight-foot fence	Motion detector	Fire extinguisher	Restoration of backups	Defense in depth (layers)

ExamAlert

Be sure you understand the three types of controls that can be used to limit access—administrative, technical, and physical—and what is contained within each type. This is required knowledge for the CISSP exam. The controls vary from domain to domain. On the exam, be sure to read each question carefully.

Implementing Personnel Security

An organization's personnel security process should begin before an employee is ever hired. During the recruitment process, a prospective employee's background needs to be reviewed to make sure the right person is hired for the job. The following are some of the checks to include:

- Background check
- Reference check
- Educational verification/certification check
- Criminal, financial, and credit checks
- Driving record or other types of verification, depending on the specific job

Performing these tasks up front can save the company time and money in the recruitment process and can help prevent loss of time and effort due to hiring the wrong person for a job.

The Role of Social Networking in Background Checks

The Internet has changed the way background checks are performed. No longer must a company spend hundreds of dollars trying to assess a candidate. Many online tools allow an organization to scour the Web, searching for public data about an individual.

One of the first places many employers now start their search is at popular social networking sites such as Facebook, Instagram, and Twitter. Social networking sites allow employers to see anything that a candidate has made public, including lifestyle choices, sexuality, and after-work activities. An employer that finds out a candidate likes to skydive and race performance motorcycles might see the person as a high insurance risk and decide not to hire that person. Even if the candidate's social networking site doesn't have anything objectionable, links placed there by friends or acquaintances might point to sites or materials others might find offensive. Maybe your college roommate was photographed in front of a poster that read "Bong hits for Jesus."

Even business-oriented sites such as LinkedIn can be used to dig up background and associate information. Employers must use caution as it's always possible that someone may have set up a fake social networking profile that's not a true identity. Companies must also make sure that mistakes are not made when people have similar names. Although not typically the default, users of such sites should consider making all their information private and should control who can view their information.

New-Hire Agreements and Policies

One great way to make sure your employees know what is expected of them is to perform a new-hire orientation. This is the time to discuss issues such as *nondisclosure agreements* (*NDAs*), good security practices, and AUPs. The goal of this training is to teach employees your established security policies and procedures. As part of the training, an employee should agree to and sign an AUP. Organizations benefit when each employee actively participates in the security of the organization.

Practices that keep employees focused on security include handing out pens, notepads, or other items that outline a few of the organization's security policies. Companies should hold semiannual reviews that refresh employees' knowledge of current policies and require updated signatures. Posters can help reinforce good security practices. Another idea is to send out periodic security-awareness emails or newsletters that reinforce good security practices.

Separation of Duties

Separation of duties describes the process of dividing duties so that one person cannot perform a critical task alone. This can mean having dual controls in place, which require more than one person to complete a critical task. This concept closely ties to the principle of least privilege, which advocates giving someone only the minimum level of access or rights needed. For example, some banks divide the safe combination numbers between two employees so that each employee has three of the six numbers needed to unlock the safe. Without some form of collusion, there is no way one person can obtain access to the safe's contents.

Organizations that have titles, roles, and duties clearly defined by policy are able to better highlight conflicts of interest and develop a separation of duties matrix. Separation of duties usually falls into four areas of control:

- **Authorization**: Verifying cash, approving purchases, and approving changes
- **Custody**: Accessing cash, merchandise, or inventories
- **Record keeping**: Preparing receipts, maintaining records, and posting payments
- **Reconciliation**: Comparing dollar amounts, counts, reports, and payroll summaries

Job Rotation

Although it's always nice to have cross-trained employees, job rotation is about more than redundancy and control. Its primary benefit is that it allows an organization to maintain backup personnel to more easily identify fraudulent activities. For example, if John is stealing money from the company, and Steve is rotated into John's position and discovers these activities, only extreme circumstances would keep Steve from telling the boss that John is a thief.

Least Privilege

The principle of *least privilege* is another important concept that can go a long way toward helping an organization achieve its security goals. Least privilege means that individuals have just enough resources to accomplish their required tasks.

For example, imagine that your company has just added computer terminals to several of the conference rooms. These terminals have been placed where meeting attendees, consultants, and sales representatives can access product information. Least privilege dictates that these computers be allowed limited Internet access but that all other Web activities be blocked. In other words, services such as network browsing, email, File Transfer Protocol (FTP), and Telnet are not available. This design reduces the opportunity for resource misuse.

Over time, even the principle of least privilege can result in authorization creep, which means that employees moving from job to job keep picking up more rights and access. Rights and access that are no longer needed should be removed.

Tip

Least privilege is not a concept strictly for individuals. In fact, it is extremely important to apply it to sensitive systems, facilities, and applications. All applications and processes should run with the minimum amount of privilege necessary to avoid further exploitation in the event that they are ever compromised. For example, Internet Information Services (IIS) used to operate with system permissions, which was far too much privilege for a web server. (This issue has been corrected since Windows Server 2003 and IIS 6.0.)

Mandatory Vacations

Even though everyone thinks it's great that Jane hasn't taken a vacation in 10 years, the fact that the accountant is always at work might be a problem. Jane appears to be a dedicated employee but might not have taken a vacation because she is performing fraudulent activities. By remaining on the job, she is able and available to provide cover for her scheme. Fraudulent activities are much easier to uncover when employees are required to take vacation time. Mandatory vacations provide time for audits and for illicit activities to be discovered.

Termination

Employees eventually leave organizations for one reason or another. Employees might leave of their own free will or might leave because they are terminated. *Termination* sometimes is necessary, but many surveys show that it is one of the most disliked tasks managers are required to do. To protect the organization, managers should use standardized termination procedures. Using a structured process helps ensure that everyone is treated equally and that employees don't have the opportunity to destroy or damage company property. Some prudent steps to incorporate into this process include the following:

1. Disable computer and facility access immediately when an employee is terminated.

2. Monitor the employee while he or she packs belongings.
3. Ensure that at no time is the employee left alone after the termination process has started.
4. Verify that the employee returns company identifications and other company property, including access tokens, smartphones, and laptops.
5. Escort the employee from the building.

It is important to avoid making this process adversarial. A contentious termination gives the employee more reason to retaliate.

Security Education, Training, and Awareness

Employees look to their employers to provide training. Without proper training, employees are generally unaware of how their actions or activities can affect the security of the organization. One of the weakest links in security is the people who work for the company. Social engineering attacks prey on the fact that users are often poorly educated in good security practices; therefore, the greatest defenses against these types of attacks are training, education, and awareness (see Figure 3.12).

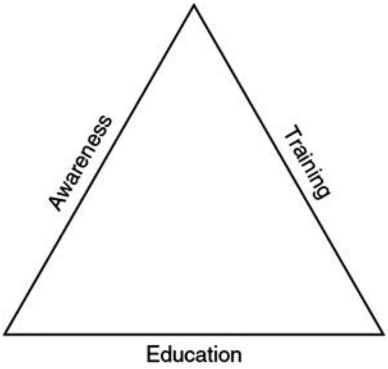


FIGURE 3.12 **Training, Education, and Awareness Triad**

You might find that your staff needs more in-depth training in matters of organizational security. This might be remedied with in-house training programs that teach new employees needed security skills or offsite CISSP education programs for security staff.

Tip

Employee-awareness programs work best when they are run for short periods and changed frequently.

Seven steps can help identify what type of security training is appropriate in an organization:

1. Establish organizational technology objectives.
2. Conduct a needs assessment.
3. Find a training program that meets these needs.
4. Select the training methods and mode.
5. Choose a means of evaluating the training.
6. Administer the training.
7. Evaluate the training.

Types of training include the following:

- In-house training
- Web-based training
- Classroom training
- Vendor training
- On-the-job training
- Apprenticeship programs
- Degreed programs
- Continuing education programs

Caution

Training and education are not the same. Training programs are of short duration and usually teach individuals a specific skill. Education is broader based and longer term (for example, degree programs).

Security Awareness

Awareness programs can be effective in increasing employee understanding of security. *Security awareness* training helps employees understand how their behavior affects the organization. Security awareness also outlines what is expected of employees. Awareness training must be developed differently for the various groups of employees in an organization. Not only will the training vary, but the topics and types of questions you'll receive from the participants will also vary.

Successful employee awareness programs tailor the message to fit the audience. These are three of the primary groups that security awareness training should be targeted to:

- **Senior management**: Don't try presenting an in-depth technical analysis to this group; its members are typically interested in the bigger picture. They want to know the costs, benefits, and ramifications of not following good security practices.
- **Data custodians**: This group requires a more structured presentation on how good security practices should be implemented, who is responsible, and the individual and departmental costs for noncompliance.
- **Users**: Training for this group must align with employees' daily tasks and map to the users' specific job functions.

> **Note**
>
> The goal of security awareness is to increase management's ability to hold employees accountable for their actions and to modify employee behavior toward security.

Social Engineering

Social engineering is the art of tricking someone into giving you something they should not. Those skilled in the art of social engineering can use their skills to gain access or information that they should not have. As organizations develop better physical and technical controls, attackers are always going to look for the easiest path to gain access. This very well could be the manipulation of people. An organization can have the best firewalls, IDS, network design, authentication system, or access controls and still be successfully attacked by a social engineer.

To gain a better understanding of how social engineering works, let's look at the different approaches these attacks use. In his work *The Science and Practice of*

Persuasion, Robert Cialdini describes the following six types of approaches for positive response to social engineering:

- **Scarcity**: This approach operates on the belief that something (such as time) is in short supply. An example of this approach might be, "I need the password now because my work is past due, and the boss is waiting. Can you please help me this one time?"
- **Authority**: This approach operates on the premise of power. An example of this approach might be, "Hi, is this the Help Desk? I work for the senior VP, and he needs his password reset to access important email!"
- **Liking**: We tend to do more for people we like than we do for people we don't like. An example of this approach might be, "Come on, we are friends. You know I would not misuse your password."
- **Consistency**: People like to be consistent. An example of this approach might be someone asking a series of questions that you will answer yes to. "Do you want a new car, is your car getting old, would you like buy our car today?"
- **Social validation**: This approach is based on the idea that if one person does it, others will, too. As an example, "Why should I badge in when everyone else just walks in once someone opens the door?"
- **Reciprocation**: If someone gives you a token or small gift, you may feel pressured to give something in return. An example of this approach might be, "You have already won a free gift. All you must do is take a few minutes to answer a few questions for our survey about your current security infrastructure."

Keep in mind that social engineering attacks can be launched from person to person or from computer to person. Knowing the various techniques that social engineers use can go a long way toward defeating their potential scams. The primary defenses against social engineering are training and awareness. A good resource for more information on social engineering is *The Art of Deception: Controlling the Human Element of Security*, by Kevin D. Mitnick and William L. Simon.

Professional Ethics Training and Awareness

This section reviews some of the ethical standards and codes that a security professional should be aware of. *Ethics* is a set of principles for conduct. Ethical standards are sometimes different from legal standards: Laws define what we *must* do, whereas ethics define what we *should* do. Keep in mind that not everyone will always act ethically.

Security professionals should uphold high ethical standards and promote high ethical standards in others. Some of the ways security professionals can help promote proper ethical behavior include making sure that organizations have guidelines on computer ethics, ensuring that ethical issues are included in employee handbooks, promoting computer ethics training, and helping to develop ethical policies on issues such as email and other privacy-related topics. There are several ethical standards that a security professional should be aware of to help point the way toward proper behavior, including the following:

- (ISC)^2 Code of Ethics (www.isc2.org)
- Ten Commandments of Computer Ethics (http://cpsr.org/issues/ethics/cei/)
- RFC 1087, *Ethics and the Internet* (www.ietf.org/rfc/rfc1087.txt)

(ISC)^2 Code of Ethics

CISSP candidates must subscribe to and support the (ISC)^2 Code of Ethics, which states that a security professional should do the following:

- Protect society, the commonwealth, and the infrastructure
- Act honorably, honestly, justly, responsibly, and legally
- Provide diligent and competent service to principals
- Advance and protect the profession

Dan Farmer: The Ethics of Vulnerability Assessment

In 1995, some wondered whether Dan Farmer had sold his soul to the devil. While working with Wietse Venema, Mr. Farmer released the program Security Administrator Tool for Analyzing Networks (SATAN), which was the first vulnerability assessment software created.

Although Mr. Farmer saw a great need for such software, his employer at the time did not and fired him. Some individuals also did not like the name of the software. To address this issue, Mr. Farmer actually created an add-on for the tool that renamed the program SANTA. By running the add-on package before running the tool, all the occurrences of the word *Satan* were changed to *Santa*, and all images were converted from a graphic image to a picture of Santa Claus.

Regardless of the name, the need for the tool was apparent. At the time of its release, nearly two-thirds of websites that were scanned were insecure. So, although some worried that such a tool could be used by attackers to target vulnerable networks, the need was real.

Today, many other tools have been created to perform network assessments, including SAINT, SARA, Nessus, and Retina. Each owes its existence to SATAN, the first vulnerability assessment tool ever created.

ExamAlert

You should read the full (ISC)^2 Code of Ethics because the exam may include one or two questions related to the code. You can find this document by searching for "Code of Ethics" at www.isc2.org.

Computer Ethics Institute

The Computer Ethics Institute was a group that focuses specifically on ethics in the technology industry. It defined the following Ten Commandments of Computer Ethics:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

ExamAlert

For the CISSP exam, you should read the Ten Commandments of Computer Ethics and be able to differentiate these rules from the (ISC)^2 Code of Ethics.

Internet Architecture Board

The Internet Architecture Board (IAB) is an advisory body of the Internet Society (ISOC). Figure 3.13 shows the layout of the ISOC. The Internet Engineering Steering Group (IESG) is responsible for technical management of IETF activities and the overall Internet standards process. The IAB is responsible for the Internet Standards Process and is the request for comments (RFC) editor. Working groups chartered by the Internet Engineering Task Force (IETF) develop new standards and protocols for the Internet.

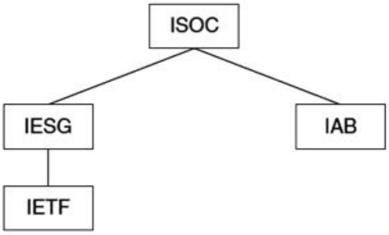


FIGURE 3.13 **ISOC and the IAB**

An RFC is an engineering white paper that describes the operation of a protocol, an application, a behavior, or the design of an Internet-connected system. The IAB also has responsibility for architectural oversight of IETF activities. One RFC that you should have knowledge of is RFC 1087. The goal of RFC 1087, published by the IAB in January 1987, is to characterize unethical and unacceptable behavior. It states that the following activities are unethical:

- Seeking to gain unauthorized access to the resources of the Internet
- Disrupting the intended use of the Internet
- Wasting resources (including people, capacity, and computer resources) through such actions
- Destroying the integrity of computer-based information
- Compromising the privacy of users

ExamAlert

Print and review RFC 1087 before you attempt the CISSP exam. It is available at www.faqs.org/rfcs/rfc1087.html.

NIST SP 800-14

While it is now retired, NIST SP 800-14, *Generally Accepted System Security Principles*, was another early attempt to define the responsibilities of organizations that use electronic systems. NIST SP 800-14 made a number of important points, including the following:

- Security supports the mission of the organization.
- Security is an integral element of sound management.
- Security should be cost-effective.
- Systems owners have security responsibilities outside their own organizations.
- Security responsibilities and accountability should be made explicit.
- Security requires a comprehensive and integrated approach.
- Security should be periodically reassessed.
- Security is constrained by societal factors.

Common Computer Ethics Fallacies

Most hackers profess to having ethical standards, and many even state that their actions are not ethically wrong. When interviewed, many hackers state that they have their own set of ethical standards. Some of the reasons often used to rationalize their illegal behavior include the following common ethical fallacies:

- **Computer game**: If they don’t protect it, it’s fair game to attack it.
- **Law-abiding citizen**: It’s not physical theft, so it’s not illegal.
- **Shatterproof**: If I don’t do damage or if it can be repaired, what’s the problem?
- **Candy-from-a-baby**: If it is that easy, how could it be wrong?
- **Hackers**: If I learn from this, it will benefit society and me.
- **Free information**: All information should be free.

Tip

While it is true that writing a computer virus is not illegal, distributing it for malicious purposes is illegal according to the CFAA. For example, Robert T. Morris was not charged with writing the first Internet worm; he was charged and prosecuted for using the code for malicious purposes.

Regulatory Requirements for Ethics Programs

As previously discussed, different people see ethics in different ways. Therefore, there are regulatory requirements in some countries to address ethics and to address proper behaviors and attitudes. In the United States, the Federal Sentencing Guidelines for Organizations (FSGO) outlines ethical requirements and may impose different sentences depending on the ethics programs and culture of the organization.

The following are several examples of regulatory requirements related to ethics:

- **Foreign Corrupt Practices Act (FCPA)**: This act imposes civil and criminal penalties if publicly held organizations fail to maintain sufficient controls over their information systems and data. FCPA requires these companies to have adequate systems of internal accounting controls.
- **Sarbanes-Oxley Act (SOX)**: This U.S. financial and accounting disclosure and accountability legislation has requirements for ethics. Section 406 of the Sarbanes-Oxley Act outlines code of ethics requirements for senior financial officers.
- **Committee for Sponsoring Organizations of the Treadway Commission (COSO)**: This is an internal control framework used by auditors and others that includes expected standards of conduct and ethics.

Note

Although questions dealing with laws specific to any one country are not common on the CISSP exam, it is still important to have a good understanding of the applicable laws under which your organization does business.

Tip

When it comes to hackers, in addition to considering ethics, it is important to consider motivation. Hackers are motivated by many different things, ranging from money to the desire to have fun. Some hackers claim that they carry out their activities simply for a cause. Hacking for a cause is known as *hacktivism*. For example, in 2020 the hacker group known as Anonymous claimed responsibility for the BlueLeaks breach, in which over 250 GB of police department files were exposed.

Exam Prep Questions

1. Which standard discussed contains the following statement?

“Systems Owners Have Security Responsibilities Outside Their Own Organization.”

❍ **A.** Ethics and the Internet

❍ **B.** RFC 1087

❍ **C.** (ISC)^2 Code of Ethics

❍ **D.** NIST 800-14

2. Which of the following methods of handling risk involves using a third party to absorb a portion of the risk?

❍ **A.** Risk reduction

❍ **B.** Risk transference

❍ **C.** Risk acceptance

❍ **D.** Risk rejection

3. You have been asked to calculate the annualized loss expectancy (ALE) for the following variables:

Single loss expectancy = $25

Exposure factor = 0.90

Annualized rate of occurrence = 0.40

Residual risk = $30

Which of the following is the resulting ALE?

❍ **A.** $9.00

❍ **B.** $22.50

❍ **C.** $10.00

❍ **D.** $14.27

4. Which of the following is the proper order?

❍ **A.** Determine ALE, residual risk, SLE, and ARO

❍ **B.** Determine ALE, ARO, SLE, and residual risk

❍ **C.** Determine ARO, SLE, ALE, and residual risk

❍ **D.** Determine SLE, ARO, ALE, and residual risk

5. Which of the following is the formula for residual risk?

❍ **A.** (Threat × Vulnerability × Asset value) × Controls gap = Residual risk

❍ **B.** (Threat × Vulnerability × Asset value) = Residual risk

❍ **C.** (Threat / Vulnerability × Asset value) × Control = Residual risk

❍ **D.** (Risk × Vulnerability × Asset value) × Controls gap = Residual risk

6. Which of the following is the length of time for copyright in the United States and the European Union?

❍ **A.** Life plus 20 years

❍ **B.** Life plus 30 years

❍ **C.** Life plus 70 years

❍ **D.** Life plus 100 years

7. Which of the following formulas represents total risk?

❍ **A.** Risk × Vulnerability × Asset value = Total risk

❍ **B.** Threat × Vulnerability × Asset value = Total risk

❍ **C.** Risk × Value / Countermeasure = Total risk

❍ **D.** Threat – Vulnerability / Asset value = Total risk

8. Which of the following is a flaw, a loophole, an oversight, or an error that makes an organization susceptible to attack or damage?

❍ **A.** Risk

❍ **B.** Vulnerability

❍ **C.** Threat

❍ **D.** Exploit

9. Which of the following is the most general of the security documents?

❍ **A.** Procedures

❍ **B.** Standards

❍ **C.** Policies

❍ **D.** Baselines

10. Which of the following groups is responsible for the development of new standards and protocols such as RFC 1087?

❍ **A.** IESG

❍ **B.** ISOC

❍ **C.** IAB

❍ **D.** IETF

11. Which organizational role is tasked with assigning sensitivity labels?

❍ **A.** Management

❍ **B.** Auditor

❍ **C.** User

❍ **D.** Owner

12. When the cost of a countermeasure outweighs the value of the asset, which of the following is the best approach?

❍ **A.** Take no action

❍ **B.** Transfer the risk

❍ **C.** Mitigate the risk

❍ **D.** Increase the cost of exposure

13. Which ISO document is used as a standard for information security management?

❍ **A.** ISO 27001

❍ **B.** ISO 27002

❍ **C.** ISO 27004

❍ **D.** ISO 27799

14. TCO does not include which of the following?

❍ **A.** Software updates

❍ **B.** Subscription costs

❍ **C.** Maintenance costs

❍ **D.** Cost of not implementing a control

15. It is important that a CISSP candidate understand the differences between the various legal systems used around the world. One early system was *Corpus Juris Civilis*, which featured a comprehensive system of written rules of law. For which legal system was *Corpus Juris Civilis* the basis?

❍ **A.** Civil law

❍ **B.** Religious law

❍ **C.** Common law

❍ **D.** Customary law

16. Planning for business continuity and disaster recovery is likely to be a very large, complex, and multidisciplinary project that brings together key associates within an organization. Which of the following best describes the role of senior management?

❍ **A.** To plan for money for the disaster recovery project manager, technology experts, process experts, or other financial requirements from various departments within the organization

❍ **B.** To be willing to make creating the disaster recovery plan a priority, commit and allow staff time for it, and set hard dates for completion

❍ **C.** To manage people from different disciplines to keep them all on the same page

❍ **D.** To be experts and understand specific processes that require special skill sets

17. Which of the following does a business impact analysis do?

❍ **A.** Determine the maximum outage time before the company is permanently damaged

❍ **B.** Detail how training and awareness will be performed and how the plan will be updated

❍ **C.** Establish the need for a BCP

❍ **D.** Select recovery strategies

18. Which term best describes a symbol, word, name, sound, or thing that uniquely identifies a product or service?

❍ **A.** Trade secret

❍ **B.** Copyright

❍ **C.** Patent

❍ **D.** Trademark

19. Which of the following is one of the most important steps to take before developing a business continuity plan?

❍ **A.** Perform a BIA

❍ **B.** Perform quantitative and qualitative risk assessment

❍ **C.** Get senior management buy-in

❍ **D.** Determine membership of the BCP team

20. When developing a business continuity plan, what should be the number-one priority?

❍ **A.** Minimize outage time

❍ **B.** Mitigate damage

❍ **C.** Document every conceivable threat

❍ **D.** Protect human safety

Answers to Exam Prep Questions

1. **D.** NIST 800-14 states that responsibilities exceed the network you are in charge of. Answers A and C both point to RFC 1087, *Ethics and the Internet*. This statement is also not in the (ISC)^2 Code of Ethics.

2. **B.** The purchase of insurance to transfer a portion or all of the potential cost of a loss to a third party is known as risk *transference*. All other answers are incorrect: Risk reduction involves implementing a countermeasure, risk acceptance deals with risk by accepting the potential cost, and risk rejection pretends the risk doesn't exist.

3. **C.** $25 × 0.40 = $10, or Single loss expectancy (SLE) × Annualized rate of occurrence (ARO) = Annualized loss expectancy (ALE).

4. **D.** The quantitative assessment process involves the following steps: Estimate potential losses (SLE), conduct a threat analysis (ARO), determine annual loss expectancy (ALE), and determine the residual risk after a countermeasure has been applied.

5. **A.** The formula for residual risk is (Threat × Vulnerability × Asset value) × Controls gap = Residual risk.

6. **C.** Life plus 70 years is the length of a copyright in the United States and the European Union. Keep in mind that copyright terms can vary depending on the country and time they were granted.

7. **B.** Risk is expressed numerically as follows:

   Threat × Vulnerability × Asset value = Total risk

   The other answers do not properly present the formula for total risk.

8. **B.** VA vulnerability is a flaw, a loophole, an oversight, or an error that makes an organization susceptible to attack or damage. All other answers are incorrect: A risk can be defined as the potential harm that can arise from some present process or from some future event; an event is an action of a threat agent that can result in harm to an asset or a service; and an exploit takes advantage of a bug, glitch, or vulnerability.

9. **C.** Policies are high-level documents. A procedure is a detailed, in-depth, step-by-step document that lays out exactly what is to be done and is tied to specific technologies and devices. Standards are tactical documents. Baselines are minimum levels of security that a system, network, or device must adhere to.

10. **D.** The development of new standards and protocols for the Internet is carried out by working groups chartered by the IETF. Answers A, B, and C are incorrect.

11. **D.** Data classification should be performed by the owner. When a data item or object is identified, the owner is responsible for assigning a security label. If the military data-classification system is used, that label might be top secret, secret, sensitive, or unclassified. It is not the responsibility of the auditor, management, or the user to assign a label to the data.

12. **A.** When the cost of a countermeasure outweighs the value of the asset, the best approach is to take no action because the asset would cost more to protect than it is worth. Answers B, C, and D are incorrect because there would be a loss of value in transferring the risk. In such cases, there would be no reason to mitigate the risk because the cost would be prohibitive—and that violates good security practices.

13. **C.** ISO 27004 is the standard for security management. ISO 27001 is focused on requirements. ISO 27002 was developed for BS 7799, and ISO 27799 is focused on health.

14. **D.** TCO includes all costs, including software, update, and maintenance costs. The only thing that is not included is the cost of not implementing the control.

15. **A.** Much of Europe is based on civil (code) law, also known as Napoleonic law. The Romans used *Corpus Juris Civilis*, which featured a comprehensive system of written rules of law and serves as the basis of the civil law used today. Answers B, C, and D are incorrect as the major difference between civil law and common law is that civil law uses legislation as the main source of laws. Religious law is based on religious tenets. China and some African countries use customary law, which may be combined with other legal systems and is based on the concept of what is customary and considered normal conduct. It is important that a CISSP candidate understand the differences between the various legal systems used around the world.

16. **B.** The best answer is B. If senior management does not get behind the DRP and fully support it, the DRP will likely fail. Answer A is not the best answer because it describes the roles of a budget manager or budget department. Answer C is not the best answer because it describes the roles of a project manager. Answer D is not the best answer as it describes the roles of a subject matter expert.

17. **A.** A BIA is a process used to help business units understand the impact of a disruptive event. Part of that process is determining the maximum outage time before the company is permanently harmed. The other answers are part of the BCP process but are not specifically part of the BIA portion, so answers B, C, and D are incorrect.

18. **D.** A trademark is a symbol, word, name, sound, or thing that identifies the origin of a product or service in a particular trade. Answers A, B, and C are incorrect as they do not properly describe a trademark.

19. **C.** Before the BCP/DRP process can begin, you must get senior management buy-in. Answers A, B, and D are important, but activities like developing the team occur after management buy-in, and the risk assessment process is performed during the BIA.

20. **D.** The protection of human safety is always the number-one priority of a security professional. Answers A, B, and C are incorrect. Minimizing outages is important but not number one. Preventing damage is also important, but protection of human safety is more important.

Need to Know More?

Keeping pre-employment checks legal: www.eeoc.gov/laws/guidance/background-checks-what-employers-need-know

Supply chain risk management planning: riskpulse.com/blog/supply-chain-risk-management-plan-what-you-need-to-include/

Security configuration guides: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/

Site security: www.faqs.org/rfcs/rfc2196.html

Self-audits of employment practices: library.findlaw.com/2000/Aug/1/127767.html

Business continuity best practices: www.eci.com/blog/472-a-best-practices-guide-to-business-continuity-planning.html

Building effective policy: csrc.nist.gov/nissc/1997/panels/isptg/pescatore/html/

Policy templates and information: www.sans.org/security-resources/policies/

Legal systems of the world: www.hmtlaw.com/international-business/legal-systems-of-the-world/

Threat modeling methodologies: blog.eccouncil.org/threat-modeling-methodologies-tools-and-processes/

CHAPTER 4

Security Architecture and Engineering

Terms you'll need to understand:

- Buffer overflows
- Security models
- Rings of protection
- Public key infrastructure
- Digital signatures
- Common Criteria
- Reference monitor
- Trusted computing base
- Open and closed systems
- Emanations
- Encryption

Topics you'll need to master:

- How to select controls based on system security requirements
- Use of confidentiality models such as Bell-LaPadula
- How to identify integrity models such as Biba and Clark-Wilson
- Common flaws and security issues associated with security architecture designs
- Cryptography and how it is used to protect sensitive information
- The need for and placement of physical security controls

Introduction

The CISSP exam Security Architecture and Engineering domain deals with hardware, software, security controls, and documentation. When hardware is designed, it needs to be built to specific standards that should provide mechanisms to protect the confidentiality, integrity, and availability of the data. The operating systems (OS) that will run on the hardware must also be designed in such a way as to ensure security.

Building secure hardware and operating systems is just a start. Both vendors and customers need to have a way to verify that hardware and software perform as stated, to rate these systems, and to have some level of assurance that such systems will function in a known manner. Evaluation criteria allow the parties involved to have a level of assurance.

This chapter introduces cryptography and how it can be used at multiple layers to enhance security. To pass the CISSP exam, you need to understand system hardware and software models and how physical and logical controls can be used to secure systems. This chapter also covers cryptography (both symmetric and asymmetric), hashing, and digital signatures, which are also potential test topics.

Secure Design Guidelines and Governance Principles

Building in security from the beginning of an architecture build is much cheaper than attempting to add it later. Part of this proactive approach should include an assessment to determine whether sensitive assets require any additional levels of security pertaining to confidentiality and integrity. Figure 4.1 illustrates the defense-in-depth design process.

There are two types of security controls:

- **Physical security controls**: These controls can be used to restrict work areas, provide media security controls, restrict server room access, and maintain proper data storage and access.
- **Logical security controls**: These controls can be deployed through the application of cryptographic controls.

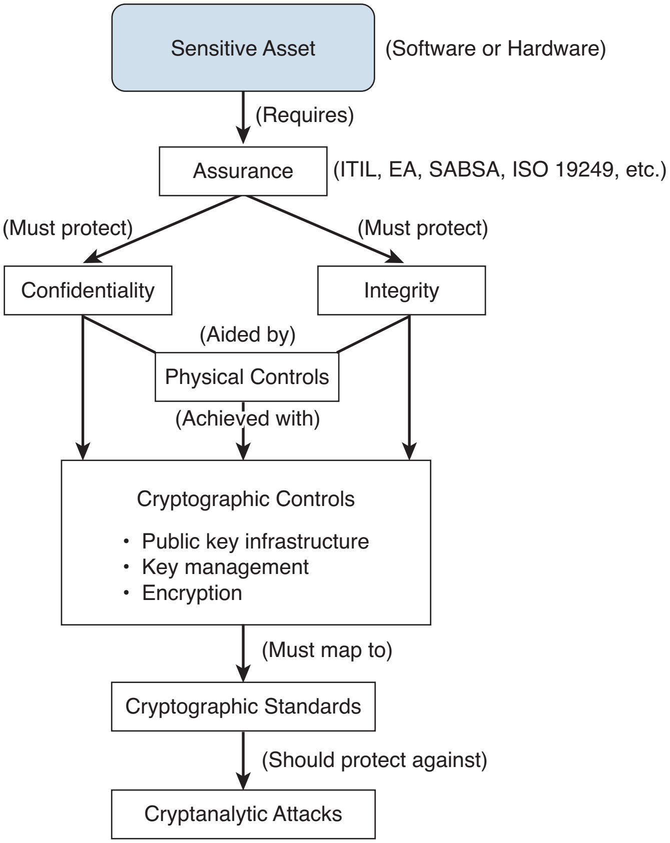


FIGURE 4.1 **Defense-in-Depth Design Process for Security Architecture**

Various types of cryptographic controls can be used. Choosing the appropriate type requires determining specific characteristics, such as the type of algorithm used, the key length, and the application.

A public key infrastructure (PKI) is an industry standard framework that establishes third-party trust between two different parties. Key management is a critical component of a PKI and includes cryptographic key generation, distribution, storage, validation, and destruction, all of which are critical components for key management.

It is important to remember that all systems can be attacked, and it is critical to choose a cryptographic system that is strong enough. Cryptographic keys can be compromised. Compromises can be due to weak algorithms or weak keys. Many methods of cryptanalytic attacks exist to compromise keys.

Note

Data at rest can be protected with a *Trusted Platform Module* (*TPM*) chip, which is a cryptographic hardware processor that can be used to provide a greater level of security than is provided through software encryption. A TPM chip installed on the motherboard of a client computer can also be used for system state authentication. A TPM chip can also be used to store encryption keys.

TPM chips are addressed in ISO 11889-1:2009 and can be used with other forms of data and system protections to provide a layered approach referred to as *defense in depth*.

A framework is used to categorize an information system or business and used to guide which controls or standards are applicable. These frameworks are typically tied to *governance*, which should focus on the availability of services, integrity of information, and protection of data confidentiality.

One early framework is Saltzer and Schroeder's principles for effective security titled "The Protection of Information in Computer Systems." This 1975 paper may seem somewhat dated today, but it is still relevant and often covered in college and university courses. In this paper, Saltzer and Schroeder define a framework for secure systems design that is based on eight architectural principles:

- Complete mediation
- Economy of mechanism
- Fail-safe defaults
- Least privilege
- Least common mechanism
- Open design
- Psychological acceptability
- Separation of privilege

Another approach is the ISO/IEC 19249, *Security Techniques—Catalogue of Architectural and Design Principles for Secure Products, Systems and Applications*, which breaks out design principles into two groupings, each with five items:

- Architectural principles:
  - Domain separation
  - Layering

  - Encapsulation
  - Redundancy
  - Virtualization
- Design principles:
  - Least privilege
  - Attack surface minimization
  - Centralized parameter validation
  - Centralized general security services
  - Preparing for error and exception handling

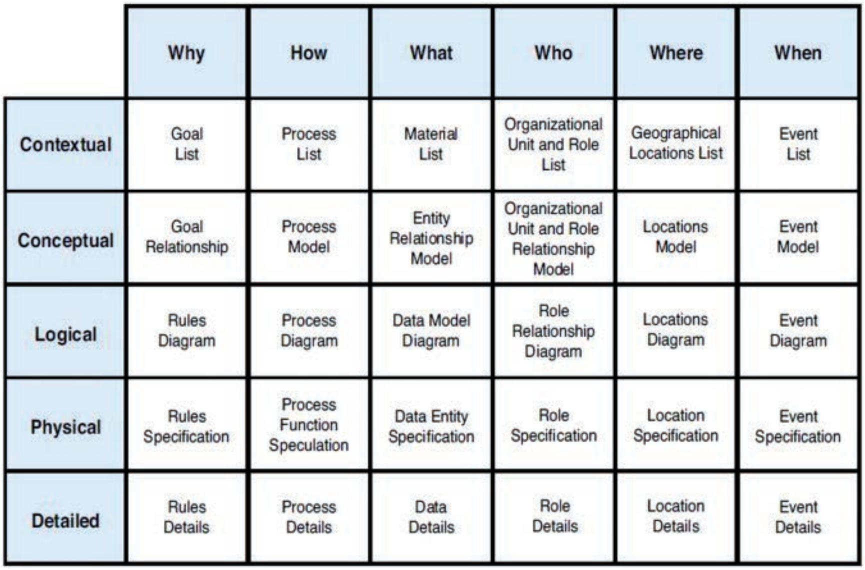
Another governance framework is the IT Infrastructure Library (ITIL). ITIL specifies a set of processes, procedures, and tasks that can be integrated with an organization's strategy to deliver value and maintain a minimum level of competency. ITIL can be used to create a baseline from which the organization can plan, implement, and measure its governance progress. ITIL presents a service lifecycle that includes the following components:

- Continual service improvement
- Service strategy
- Service design
- Service transition
- Service operation

Enterprise Architecture

Security and governance can be enhanced by implementing an *enterprise architecture* (*EA*) plan. EA is the practice in information technology of organizing and documenting a company's IT assets to enhance planning, management, and expansion. The primary purpose of using EA is to ensure that business strategy and IT investments are aligned. The benefit of EA is that it provides a means of traceability that extends from the highest level of business strategy down to the fundamental technology.

One early EA model is the Zachman Framework, which was designed to allow companies to structure policy documents for information systems so they focus on who, what, where, when, why, and how (see Figure 4.2).



	Why	How	What	Who	Where	When
Contextual	Goal List	Process List	Material List	Organizational Unit and Role List	Geographical Locations List	Event List
Conceptual	Goal Relationship	Process Model	Entity Relationship Model	Organizational Unit and Role Relationship Model	Locations Model	Event Model
Logical	Rules Diagram	Process Diagram	Data Model Diagram	Role Relationship Diagram	Locations Diagram	Event Diagram
Physical	Rules Specification	Process Function Speculation	Data Entity Specification	Role Specification	Location Specification	Event Specification
Detailed	Rules Details	Process Details	Data Details	Role Details	Location Details	Event Details

FIGURE 4.2 **Zachman Model**

Federal law requires each government agency to set up its EA and a structure for its governance. This process is guided by the Federal Enterprise Architecture (FEA) framework, which is designed to use five models:

- **Performance reference model**: A framework used to measure performance of major IT investments
- **Business reference model**: A framework used to provide an organized, hierarchical model for day-to-day business operations
- **Service component reference model**: A framework used to classify service components with respect to how they support business or performance objectives
- **Technical reference model**: A framework used to categorize the standards, specifications, and technologies that support and enable the delivery of service components and capabilities
- **Data reference model**: A framework used to provide a standard means by which data can be described, categorized, and shared

An independently designed, but later integrated, subset of the Zachman Framework is the Sherwood Applied Business Security Architecture (SABSA). Like the Zachman Framework, the SABSA model and methodology was developed for risk-driven enterprise information security architectures. It asks what, why, how, and where. For more information on the SABSA model, see www.sabsa-institute.org.

The ISO 27000 series is part of a family of governance standards that can trace their origins back to BS 7799. Organizations can become ISO 27000 certified by verifying their compliance with an accredited testing entity. Some of the core ISO standards include the following:

- **ISO 27001**: This document describes requirements for establishing, implementing, operating, monitoring, reviewing, and maintaining an information security management system (ISMS). It follows the Plan-Do-Check-Act model.
- **ISO 27002**: This document, which began as the BS 7799 standard and was republished as the ISO 17799 standard, describes ways to develop a security program within an organization.
- **ISO 27003**: This document focuses on implementation.
- **ISO 27004**: This document describes the ways to measure the effectiveness of an information security program.
- **ISO 27005**: This document describes the code of practice in information security.

True security is a layered process and requires more than governance. The items discussed in the following sections can be used to build a more secure organization.

Regulatory Compliance and Process Control

One area of concern for a security professional is protection of sensitive information, including financial data. One attempt to provide this protection is the Payment Card Industry Data Security Standard (PCI-DSS). This multinational standard, which was first released in 2004, was created to enforce strict standards of control for the protection of credit card, debit card, ATM card, and gift card numbers by mandating policies, security devices, controls, and network monitoring. PCI also sets standards for the protection of personally identifiable information that is associated with the cardholder on an account. Participating vendors include American Express, MasterCard, Visa, and Discover.

Whereas PCI is used to protect financial data, Control Objectives for Information and Related Technology (COBIT) was developed to meet the requirements of business and IT processes. It is a standard used for auditors worldwide and was developed by the Information Systems Audit and Control Association (ISACA). COBIT is divided into four control areas:

- Planning and Organization
- Acquisition and Implementation
- Delivery and Support
- Monitoring

Fundamental Concepts of Security Models

Modern computer systems can be broken down into four groupings, or layers:

- Hardware
- Kernel and device drivers
- Operating system
- Applications

Hardware interacts with software, such as the operating system kernel, and operating systems and applications do the things we need done. At the core of every computer system are the central processing unit (CPU) and the hardware that makes it run. The CPU is just one of the items that you can find on the motherboard, which serves as the base for most crucial system components.

The following sections examine the various parts of a computer system, starting at the heart of the system.

Central Processing Unit

The CPU is the heart of a computer system and serves as the brain of the computer. The CPU consists of the following:

- **Arithmetic logic unit (ALU)**: The ALU performs arithmetic and logical operations. It is the brain of the CPU.
- **Control unit**: The control unit manages the instructions it receives from memory. It decodes and executes the requested instructions and determines what instructions have priority for processing.

- **Memory**: Memory is used to hold instructions and data to be processed. CPU memory is not typical memory; it is much faster than non-CPU memory.

A CPU is capable of executing a series of basic operations, including fetch, decode, execute, and write operations. Pipelining combines multiple steps into one process. A CPU has the capability to fetch instructions and then process them. A CPU can operate in one of four states:

- **Supervisor state**: The program can access the entire system.
- **Problem state**: Only non-privileged instructions can be executed.
- **Ready state**: The program is ready to resume processing.
- **Wait state**: The program is waiting for an event to complete.

Because CPUs have very specific designs, the operating system as well as applications must be developed to work with the CPU. CPUs also have different types of registers to hold data and instructions. The base register contains the beginning address assigned to a process, and the limit address marks the end of the memory segment. Together, these components are responsible for the recall and execution of programs.

CPUs have made great strides, as illustrated in Table 4.1. As the size of transistors has decreased, the number of transistors that can be placed on a CPU has increased. Thanks to increases in the total number of transistors and in clock speed, the power of CPUs has increased exponentially. Today, a 3.06 GHz Intel Core i7 can perform about 18 million instructions per second (MIPS).

TABLE 4.1 **CPU Advancements**

CPU	Year	Number of Transistors	Clock Speed
8080	1974	6,000	2 MHz
80386	1986	275,000	12.5 MHz
Pentium	1993	3,100,000	60 MHz
Intel Core 2	2006	291,000,000	2.66 GHz
Intel Core i7	2009	731,000,000	4.00 GHz
Intel Core M	2014	1,300,000,000	2.6 GHz

Note

Processor speed is measured in MIPS (millions of instructions per second). This standard is used to indicate how fast a CPU can work.

Two basic designs of CPUs are manufactured for modern computer systems:

- **Reduced instruction set computer (RISC)**: Uses simple instructions that require a reduced number of clock cycles
- **Complex instruction set computer (CISC)**: Performs multiple operations for a single instruction

The CPU requires two inputs to accomplish its duties: instructions and data. The data is passed to the CPU for manipulation, where it is typically worked on in either the problem state or the supervisor state. In the *problem state*, the CPU works on the data with non-privileged instructions. In the *supervisor state*, the CPU executes privileged instructions.

ExamAlert

A *superscalar processor* is a processor that can execute multiple instructions at the same time; a *scalar processor* can execute only one instruction at a time. You need to know this distinction for the CISSP exam.

A CPU can be classified into one of several categories, depending on its functionality. When the computer's CPU, motherboard, and operating system all support the functionality, the computer system is also categorized according to the following:

- **Multiprogramming**: Can interleave two or more programs for execution at any one time
- **Multitasking**: Can perform one or more tasks or subtasks at a time
- **Multiprocessor**: Supports one or more CPUs

A multiprocessor system can work in symmetric or asymmetric mode. With *symmetric mode*, all processors are equal and can handle any tasks equally with all devices (peripherals being equally accessible) or no specialized path is required for resources. With *asymmetric mode*, one CPU schedules and coordinates tasks between other processes and resources.

The data that CPUs work with is usually part of an application or a program. These programs are tracked using a process ID (PID). Anyone who has ever looked at Task Manager in Windows or executed a ps command on a Linux machine has probably seen a PID number. You can manipulate the priority of these tasks as well as start and stop them. Fortunately, most programs do much more than the first C code you wrote, which probably just said "Hello World." Each line of code or piece of functionality that a program has is known as a *thread*.

A program that has the capability to carry out more than one thread at a time is referred to as *multithreaded* (see Figure 4.3).

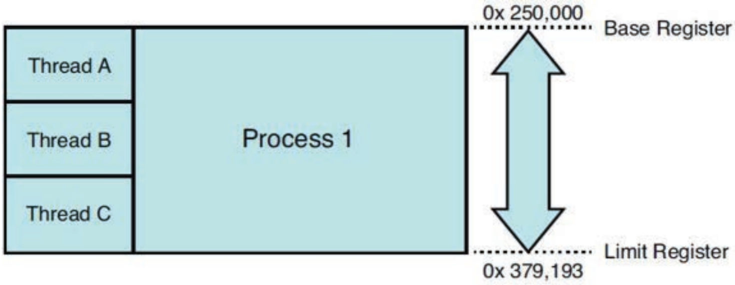


FIGURE 4.3 **Processes and Threads**

Process activity uses process isolation to separate processes. Four process isolation techniques are used to ensure that each application receives adequate processor time to operate properly:

- **Encapsulation of processes or objects**: Other processes do not interact with the application.
- **Virtual mapping**: The application is written in such a way that it believes it is the only application running.
- **Time multiplexing**: This allows the application or process to share the computer's resources.
- **Naming distinctions**: Processes are assigned their own unique names.

ExamAlert

To get a good look at naming distinctions, run ps -aux from the terminal of a Linux system and note the unique PID values.

An *interrupt* is another key piece of a computer system. It is an electrical connection between a device and a CPU. The device can put an electrical signal on this connection to get the attention of the CPU. The following are common interrupt methods:

- **Programmed I/O**: Used to transfer data between a CPU and a peripheral device
- **Interrupt-driven I/O**: A more efficient input/output method that requires complex hardware
- **I/O using DMA**: I/O based on direct memory access that can bypass the processor and write the information directly to main memory
- **Memory-mapped I/O**: A method that requires the CPU to reserve space for I/O functions and to make use of the address for both memory and I/O devices
- **Port-mapped I/O**: A method that uses a special class of instruction that can read and write a single byte to an I/O device

ExamAlert

Interrupts can be maskable and non-maskable. Maskable interrupts can be ignored by the application or the system, whereas non-maskable interrupts cannot be ignored by the system. An example of a non-maskable interrupt in Windows is the interrupt that occurs when you press Ctrl+Alt+Delete.

There is a natural hierarchy to memory, and there must therefore be a way to manage memory and ensure that it does not become corrupted. That is the job of the memory management system. Memory management systems on multitasking operating systems are responsible for the following tasks:

- **Relocation**: The system maintains the ability to copy memory contents from memory to secondary storage as needed.
- **Protection**: The system provides control to memory segments and restricts what process can write to memory.
- **Sharing**: The system allows sharing of information based on a user's security level for access control. For instance, Mike may be able to read an object, whereas Shawn may be able to read and write to the object.

- **Logical organization**: The system provides for the sharing of and support for dynamic link libraries.
- **Physical organization**: The system provides for the physical organization of memory.

Storage Media

A computer is not just a CPU; memory is also an important component. The CPU uses memory to store instructions and data. Therefore, memory is an important type of storage media. The CPU is the only component that can directly access memory. Systems are designed this way because the CPU has a high level of system trust.

A CPU can use different types of addressing schemes to communicate with memory, including *absolute addressing* and *relative addressing*. In addition, memory can be addressed either physically or logically. *Physical addressing* refers to the hard-coded address assigned to memory. Applications and programmers writing code use *logical addresses*. *Relative addressing* involves using a known address with an offset applied.

Not only can memory be addressed in different ways, but there are also different types of memory. Memory can be either *nonvolatile* or *volatile*. The sections that follow provide examples of both of these types.

Tip

Two important security concepts associated with storage are protected memory and memory addressing. For the CISSP exam, you should understand that protected memory prevents other programs or processes from gaining access or modifying the contents of address space that has previously been assigned to another active program. Memory can be addressed either physically or logically. *Memory addressing* describes the method used by the CPU to access the contents of memory. This is especially important for understanding the root causes of buffer overflow attacks.

RAM

Random-access memory (*RAM*) is volatile memory. If power is lost, the data in RAM is destroyed. Types of RAM include *static RAM*, which uses circuit latches to represent binary data, and *dynamic RAM*, which must be refreshed every few milliseconds. RAM can be configured as *dynamic random-access memory* (*DRAM*) or *static random-access memory* (*SRAM*).

SRAM doesn't require a refresh signal, as DRAM does. SRAM chips are more complex and faster, and thus they are more expensive. DRAM access times are around 60 nanoseconds (ns) or more; SRAM has access times as fast as 10 ns. SRAM is often used for cache memory.

DRAM chips can be manufactured inexpensively. *Dynamic* refers to the memory chips' need for a constant update signal (also called a *refresh signal*) to retain the information that is written there. Currently, there are five popular implementations of DRAM:

- **Synchronous DRAM (SDRAM)**: SDRAM shares a common clock signal with the transmitter of the data. The computer's system bus clock provides the common signal that all SDRAM components use for each step to be performed.
- **Double data rate (DDR)**: DDR supports a double transfer rate compared to ordinary SDRAM.
- **DDR2**: DDR2 splits each clock pulse in two, doubling the number of operations it can perform.
- **DDR3**: DDR3 is a DRAM interface specification that offers the ability to transfer data at twice the rate (eight times the speed of its internal memory arrays), enabling higher bandwidth or peak data rates.
- **DDR4**: DDR4 offers higher speed than DDR2 or DDR3 and is one of the latest variants of DRAM. It is not compatible with any earlier type of RAM.

ExamAlert

Memory leaks occur when programs or processes use RAM but cannot release it. Programs that suffer from memory leaks will eventually use up all available memory and can cause a system to halt or crash.

ROM

Read-only memory (*ROM*) is nonvolatile memory that retains information even if power is removed. ROM is typically used to load and store firmware. Firmware is embedded software much like BIOS or UEFI.

Tip

Most modern computer systems use Unified Extensible Firmware Interface (UEFI) instead of BIOS. UEFI offers several advantages over BIOS, including support for remote diagnostics and repair of systems even if no OS is installed.

Some common types of ROM include the following:

- Erasable programmable read-only memory (EPROM)
- Electrically erasable programmable read-only memory (EEPROM)
- Flash memory
- Programmable logic devices (PLDs)

Secondary Storage

Memory plays an important role in the world of storage, but other long-term types of storage are also needed. One of these is *sequential storage*. Tape drives are a type of sequential storage that must be read sequentially from beginning to end.

Another well-known type of secondary storage is *direct-access storage*. Direct-access storage devices do not have to be read sequentially; the system can identify the location of the information and go directly to it to read the data. A hard drive is an example of a direct-access storage device: A hard drive has a series of platters, read/write heads, motors, and drive electronics contained within a case designed to prevent contamination. Hard drives are used to hold data and software. *Software* is an operating system or application that you've installed on a computer system.

Compact discs (CDs) are a type of *optical media*. They use a laser/opto-electronic sensor combination to read or write data. A CD can be read-only, write-once, or rewriteable. CDs can hold up to around 800 MB on a single disk. A CD is manufactured by applying a thin layer of aluminum to what is primarily hard clear plastic. During manufacture or when a CD/R is burned, small bumps or pits are placed in the surface of the disc. These bumps or pits are converted into binary ones or zeros. Unlike a floppy disk, which has tracks and sectors, a CD comprises one long spiral track that begins at the inside of the disc and continues toward the outer edge.

Digital video discs (DVDs) are very similar to CDs in that both are optical media: DVDs just hold more data. The current version of optical storage is the Blu-ray disc. These optical disks can hold 50 GB or more of data.

More and more systems today are moving to solid-state drives (SSDs) and flash memory storage. Sizes up to 2 TB are now common.

I/O Bus Standards

The data that a CPU is working with must have a way to move from the storage media to the CPU. This is accomplished by means of a bus. A *bus* is lines of conductors that transmit data between the CPU, storage media, and other hardware devices. You need to understand two bus-related terms for the CISSP exam:

- **Northbridge**: The northbridge, which is considered the memory controller hub (MCH), connects CPU, RAM, and video memory.
- **Southbridge**: The southbridge is used by the I/O controller hub (ICH) to connect input/output devices such as the hard drive, DVD drive, keyboard, mouse, and so on.

From the point of view of the CPU, the various adapters plugged in to a computer are external devices. These connectors and the bus architecture used to move data to the devices have changed over time. The following are some bus architectures with which you need to be familiar:

- **Industry Standard Architecture (ISA)**: The ISA bus started as an 8-bit bus designed for IBM PCs. It is now obsolete.
- **Peripheral Component Interconnect (PCI)**: The PCI bus was developed by Intel and served as a replacement for ISA and other bus standards. PCI Express is now the standard.
- **Peripheral Component Interface Express (PCIe)**: The PCIe bus was developed as an upgrade to PCI. It offers several advantages, such as greater bus throughput, smaller physical footprint, better performance, and better error detection and reporting.
- **Serial ATA (SATA)**: The SATA standard is the current standard for connecting hard drives and solid-state drives to computers. It uses a serial design and smaller cables and offers greater speeds and better airflow inside the computer case.

- **Small Computer Systems Interface (SCSI)**: The SCSI bus allows a variety of devices to be daisy-chained off a single controller. Many servers use the SCSI bus for their preferred hard drive solution.

Universal Serial Bus (USB) has gained wide market share. USB overcame the limitations of traditional serial interfaces. USB 2.0 devices can communicate at speeds up to 480 Mbps or 60 MBps, whereas USB 3.0 devices have a maximum bandwidth rate of 5 Gbps or 640 MBps. Devices can be chained together so that up to 127 devices can be connected to one USB slot of one hub in a "daisy chain" mode, eliminating the need for expansion slots on the motherboard. The newest USB standard is 3.2. The biggest improvement for the USB 3.2 standard is a boost in data transfer bandwidth of up to 10 Gbps.

USB is used for flash memory, cameras, printers, external hard drives, and phones. USB has two fundamental advantages: It has broad product support and devices are typically recognized immediately when connected.

Many Apple computers make use of the Thunderbolt interface, and a few legacy FireWire (IEEE 1394) interfaces are still found on digital audio and video equipment.

Virtual Memory and Virtual Machines

Modern computer systems have developed specific ways to store and access information. One of these is *virtual memory*, which is the combination of the computer's primary memory (RAM) and secondary storage (the hard drive or SSD). When these two technologies are combined, the OS can make the CPU believe that it has much more memory than it actually has. Examples of virtual memory include the following:

- Page file
- Swap space
- Swap partition

These virtual memory types are user defined in terms of size, location, and other factors. When RAM is nearly depleted, the CPU begins saving data onto the computer's hard drive in a process called *paging*. Paging takes a part of a program out of memory and uses the page file to save those parts of the program. If the system requires more RAM than paging provides, it *writes* an entire process out to the swap space. This process uses a paging file/swap file so that the data can be moved back and forth between the hard drive and RAM as needed. A specific drive can even be configured to hold such data and is therefore called a *swap partition*. Individuals who have used a computer's hibernation function or who have ever opened more programs on their computers than they've had enough memory to support are familiar with the operation of virtual memory.

Closely related to virtual memory are virtual machines, such as VMware Workstation and Oracle VM VirtualBox. VMware is one of the leaders in the machine virtualization market. A *virtual machine* enables the user to run a second OS within a virtual host. For example, a virtual machine can let you run another Windows OS, Linux x86, or any other OS that runs on x86 processor and supports standard BIOS/UEFI booting.

Virtual systems make use of a hypervisor to manage the virtualized hardware resources to run a guest operating system. A Type 1 hypervisor runs directly on the hardware, with VM resources provided by the hypervisor, whereas a Type 2 hypervisor runs on a host operating system above the hardware. Virtual machines can be used for development and system administration, production, and to reduce the number of physical devices needed. Hypervisors are also being used to design virtual switches, routers, and firewalls.

Tip

Virtualization has been very important in the workplace, but cloud-based systems have more recently begun to take the place of VMs. Cloud-based systems enable employees to work from many different locations. The applications and data can reside in the cloud, and a user can access this content from any location that has connectivity. The potential disadvantage of cloud computing is that security can be an issue. It is important to consider who owns the cloud. Is it a private cloud (owned by company) or a public cloud (owned by someone else)? In addition, what is the physical location of the cloud, who has access to the cloud, and is it shared (co-tenancy)? It is critical to consider each of these factors before placing any corporate assets in the cloud.

Computer Configurations

The following are some of the most commonly used computer and device configurations:

- **Print server**: Print servers are usually located close to printers and allow many users to access the same printer and share its resources.
- **File server**: File servers allow users to have a centralized site to store files. A file server provides an easy way to perform backups because it

can be done on one server rather than on all the client computers. It also allows for group collaboration and multiuser access.

- **Application server**: An application server allows users to run applications that are not installed on an end user's system. It is a very popular concept in thin client environments, which depend on a central server for processing power. Licensing is an important consideration with application servers.
- **Web server**: Web servers provide web services to internal and external users via web pages. A sample web address or URL (uniform resource locator) is www.thesolutionfirm.com.
- **Database server**: Database servers store and access data, including information such as product inventories, price lists, customer lists, and employee data. Because databases hold sensitive information, they require well-designed security controls. A database server typically sits in front of a database and brokers requests, acting as middleware between the untrusted users and the database holding the data.
- **Laptops and tablets**: These are mobile devices that are easily lost or stolen. Mobile devices have become very powerful and must be properly secured.
- **Smartphones**: Today's smartphones are handheld computers that have large amounts of processing capability. They can take photos and offer onboard storage, Internet connectivity, and the ability to run applications. These devices are of particular concern as more companies start to support *bring your own device* (*BYOD*) policies. Such devices can easily fall outside of company policies and controls.
- **Industrial control systems (ICS)**: ICSs are typically used for industrial process control, such as with manufacturing systems on factory floors. ICSs can be used to operate and/or automate industrial processes. There are several categories of ICSs, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), and field devices.
- **Embedded devices / Internet of Things (IoT)**: Embedded devices / IoT include ATMs, point-of-sale terminals, and smartwatches. More and more devices include embedded technology, such as smart refrigerators and Bluetooth-enabled toilets. The security of embedded devices is a growing concern, as these devices may not be patched or updated on a regular basis.

Note

We can expect more and more devices to have embedded technology as the Internet of Things (IoT) grows. Several companies even sell toilets with Bluetooth and SD card technology built in; like other devices, they are not immune to hacking (see www.extremetech.com/extreme/163119-smart-toilets-bidet-hacked-via-bluetoothgives-new-meaning-to-backdoor-vulnerability).

Security Architecture

Although a robust functional architecture is a good start, real security requires that you have a security architecture in place to control processes and applications. Concepts related to security architecture include the following:

- Protection rings
- Trusted computing base (TCB)
- Open and closed systems
- Security modes of operation
- Operating states
- Recovery procedures
- Process isolation

Protection Rings

An operating system knows who and what to trust by relying on *protection rings*. Protection rings work much like your network of family members, friends, coworkers, and acquaintances. The people who are closest to you, such as your spouse and children, have the highest level of trust. Those who are distant acquaintances or are unknown to you probably have a lower level of trust. For example, when you see a guy on Canal Street in New York City hawking new Rolex watches for $100, you should have little trust in him and his relationship with the Rolex company!

Protection rings are conceptual rather than physical entities. Figure 4.4 illustrates the protection rings schema. The first implementation of such a system was in MIT's Multics time-shared operating system.

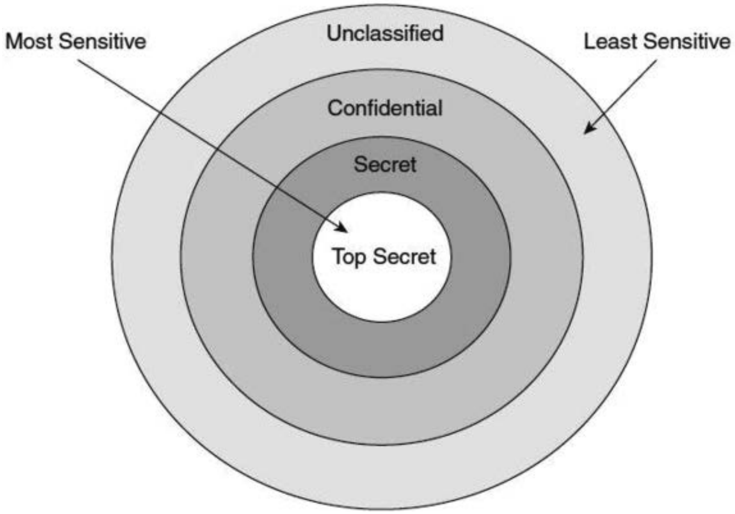


FIGURE 4.4 **Protection Rings**

The protection rings model provides the operating system with various levels at which to execute code or to restrict that code's access. The idea is to use engineering design to build in layers of control using secure design principles. The rings provide much greater granularity than a system that just operates in user and privileged modes. As code moves toward the outer bounds of the model, the layer number increases, and the level of trust decreases. This model includes the following layers:

- **Layer 0**: This is the most trusted level. The operating system kernel resides at this level. Any process running at layer 0 is said to be operating in *privileged mode*.
- **Layer 1**: This layer contains non-privileged portions of the operating system.
- **Layer 2**: This is where I/O drivers, low-level operations, and utilities reside.
- **Layer 3**: This layer is where applications and processes operate. It is the level at which individuals usually interact with the operating system. Applications operating here are said to be working in *user mode*, which is often referred to as *problem mode* because this is where the less-trusted applications run; it is, therefore, where most problems occur.

Not all systems use all rings in the protection rings model. Most systems that are used today operate in two modes: *user mode* and *supervisor* (privileged) mode.

Items that need high security, such as the operating system security kernel, are located in the center ring. This ring is unique because it has access rights to all domains in the system. Protection rings are part of the trusted computing base concept, which is described next.

Trusted Computing Base

The *trusted computing base* (TCB) is the sum of all the protection mechanisms within a computer and is responsible for enforcing the security policy. The TCB includes hardware, software, controls, processes and is responsible for confidentiality and integrity. The TCB is the only portion of a system that operates at a high level of trust. It monitors four basic functions:

- **Input/output (I/O) operations**: I/O operations are a security concern because operations from the outermost rings might need to interface with rings of greater protection. These cross-domain communications must be monitored.
- **Execution domain switching**: Applications running in one domain or level of protection often invoke applications or services in other domains. If these requests are to obtain more sensitive data or service, their activity must be controlled.
- **Memory protection**: To truly provide security, the TCB must monitor memory references to verify confidentiality and integrity in storage.
- **Process activation**: Registers, process status information, and file access lists are vulnerable to loss of confidentiality in a multiprogramming environment. This type of potentially sensitive information must be protected.

ExamAlert

For the CISSP exam, you should understand not only that the TCB is tasked with enforcing security policy but also that the TCB is the sum of all protection mechanisms within a computer system that have also been evaluated for security assurance. It consists of hardware, firmware, and software.

Components that have not been evaluated are said to fall outside the security perimeter.

The TCB monitors the functions in the preceding list to ensure that the system operates correctly and adheres to security policy. The TCB follows the *reference monitor* concept. The reference monitor is an abstract machine that is used to implement security. The reference monitor's job is to validate access to objects by authorized subjects. The reference monitor operates at the boundary between the trusted and untrusted realms. The reference monitor has three properties:

- It cannot be bypassed and controls all access, as it must be invoked for every access attempt.
- It cannot be altered and is protected from modification or change.
- It must be small enough to be verified and tested correctly.

ExamAlert

For the CISSP exam, you should understand that the reference monitor enforces the security requirement for the security kernel.

The reference monitor is much like the bouncer at a club, standing between each subject and object and verifying that each subject meets the minimum requirements for access to an object (see Figure 4.5).

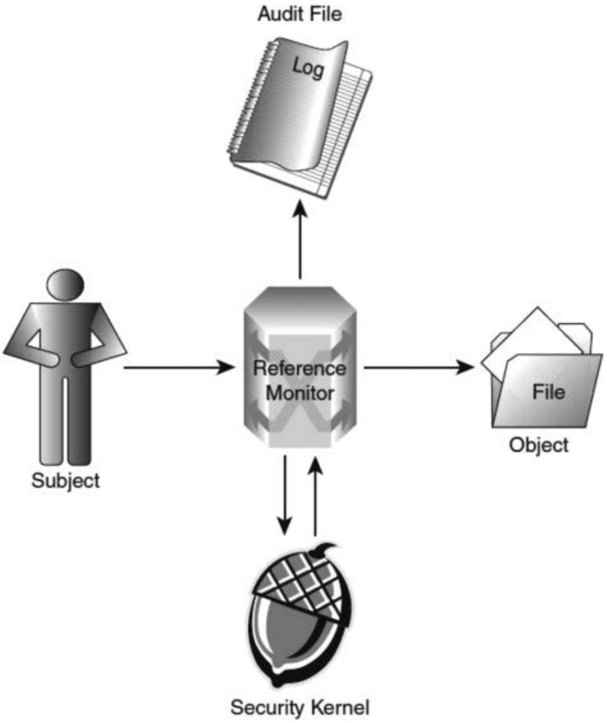


FIGURE 4.5 **Reference Monitor**

Note

Subjects are active entities such as people, processes, or devices.

Objects are passive entities that are designed to contain or receive information. Objects can be processes, software, or hardware.

The reference monitor can be designed to use tokens, capability lists, or labels:

- **Tokens**: Communicate security attributes before requesting access
- **Capability lists**: Offer faster lookup than security tokens but are not as flexible
- **Security labels**: Used by high-security systems because these labels offer permanence

At the heart of the operating system is the *security kernel*. The security kernel handles all user/application requests for access to system resources. A small security kernel is easy to verify, test, and validate as secure. However, in real life, the security kernel might be bloated with some unnecessary code because processes located inside can function faster and have privileged access. Vendors have taken different approaches to developing operating systems. For example, DOS used a monolithic kernel. Several of these designs are shown in Figure 4.6 and are described here:

- **Monolithic architecture**: All of the OS processes work in kernel mode.
- **Layered OS design**: This design separates system functionality into different layers.
- **Microkernel**: A smaller kernel supports only critical processes.
- **Hybrid microkernel**: The kernel structure is similar to a microkernel but implemented in terms of a monolithic design.

Although the reference monitor is conceptual, the security kernel can be found at the heart of every system. The security kernel is responsible for running the required controls used to enforce functionality and resist known attacks. As mentioned previously, the reference monitor operates at the *security perimeter*: the boundary between the trusted and untrusted realms. Components outside the security perimeter are not trusted. All trusted access control mechanisms are inside the security perimeter.

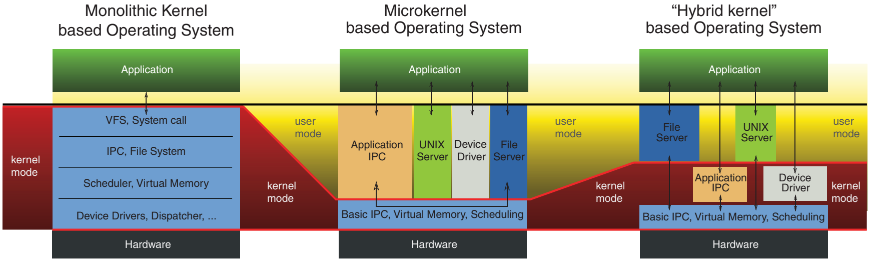


FIGURE 4.6 **Operating System Architecture**

Source: http://upload.wikimedia.org/wikipedia/commons/d/d0/OS-structure2.svg

Open and Closed Systems

Open systems accept input from other vendors and are based on standards and practices that allow connection to different devices and interfaces. The goal is to promote full interoperability whereby the system can be fully utilized.

Closed systems are proprietary. They use devices that are not based on open standards and that are generally locked. They lack standard interfaces to allow connection to other devices and interfaces.

For example, in the U.S. cell phone industry, AT&T and T-Mobile cell phones are based on the worldwide Global System for Mobile Communications (GSM) standard and can be used overseas easily on other networks with a simple change of the subscriber identity module (SIM). These are open-system phones. Phones that use Code Division Multiple Access (CDMA), such as Sprint and Verizon phones, do not have the same level of support and have almost completely been phased out. In 2010, carriers worldwide started this process when agreeing to switch to LTE, a 4G network with 2023 listed as the final drop date.

Note

The concept of open and closed can apply to more than just hardware. With open software, others can view and/or alter the source code, but with closed software, they cannot. For example, a Samsung Galaxy phone runs the open-source Android operating system, whereas an Apple iPhone runs the closed-source iOS.

Security Modes of Operation

Several security modes of operation are based on Department of Defense (DoD) 5220.22-M classification levels. According to the DoD, information being processed on a system and the clearance level of authorized users can be classified into one of four modes (see Table 4.2):

- **Dedicated**: A need to know is required to access all information stored or processed. Every user requires formal access with clearance and approval and must have executed a signed nondisclosure agreement (NDA) for all the information stored and/or processed. This mode must also support enforced system access procedures. All hard-copy output and media removed will be handled at the level for which the system is accredited until reviewed by a knowledgeable individual. As the system is dedicated to processing of one particular type or classification of information all authorized users can access all data.

- **System high**: All users have a security clearance; however, a need to know is required only for some of the information contained within the system. Every user requires access approval and needs to have signed NDAs for all the information stored and/or processed. Access to an object by users not already possessing access permission must only be assigned by authorized users of the object. This mode must be capable of providing an audit trail that records time, date, user ID, terminal ID (if applicable), and filename. All users can access some data based on their need to know.

- **Compartmented**: Valid need to know is required for some of the information on the system. All users must have formal access approval for all information they will access on the system and require proper clearance for the highest level of data classification on the system. All users must have signed NDAs for all information they will access on the system. All users can access some data based on their need to know and formal access approval.

- **Multilevel**: Every user has a valid need to know for some of the information that is on the system, and more than one classification level can be processed at the same time. Users must have formal access approval and must have signed NDAs for all information they will access on the system. Mandatory access controls provide a means of restricting access to files based on their sensitivity label. All users can access some data based on their need to know, clearance, and formal access approval.

TABLE 4.2 **Security Modes of Operation**

Mode	Dedicated	System High	Compartmented	Multilevel
Signed NDA	All	All	All	All
Clearance	All	All	All	Some
Approval	All	All	Some	Some
Need to know	All	Some	Some	Some

Note

The term *sensitivity or security labels* denotes high-security Mandatory access control (MAC)-based systems.

Operating States

When systems are used to process and store sensitive information, there must be some agreed-on methods for how this will work. Generally, these concepts were developed to meet the requirements of handling sensitive government information with categories such as sensitive, secret, and top secret. The burden of handling this task can be placed on either administration or the system itself.

Generally, two designs are used:

- **Single-state systems**: This type of system is designed and implemented to handle one category of information. The burden of management falls on the administrator, who must develop the policy and procedures to manage the system. The administrator must also determine who has access and what type of access the users have. These systems are dedicated to one mode of operation, so they are sometimes referred to as *dedicated systems*.
- **Multistate systems**: These systems depend not on the administrator but on the system itself. More than one person can log in to a multistate system and access various types of data, depending on the level of clearance. As you would probably expect, these systems can be expensive. The XTS-400 that runs the Secure Trusted Operating Program (STOP) OS from BAE Systems is an example of a multistate system. A multistate system can operate as a compartmentalized system. This means that Mike can log in to the system with a secret clearance and access secret-level data, whereas Dwayne can log in with top-secret-level clearance and access a different level of data. These systems are compartmentalized and can segment data on a need-to-know basis.

Tip

Security-Enhanced Linux and TrustedBSD are freely available implementations of operating systems with limited multistate capabilities. Security evaluation is a problem for these free MLS implementations because of the expense and time it would take to fully qualify these systems.

Recovery Procedures

Unfortunately, things don't always operate normally; they sometimes go wrong, and system failure can occur. A system failure could potentially compromise a system by corrupting integrity, opening security holes, or causing corruption. Efficient designs have built-in recovery procedures to recover from potential problems. There are two basic types of recovery procedures:

- **Fail safe**: If a failure is detected, the system is protected from compromise by termination of services.
- **Fail soft**: A detected failure terminates the noncritical process. Systems in fail soft mode are still able to provide partial operational capability.

It is important to be able to recover when an issue arises. The best way to ensure recovery is to take a proactive approach and back up all critical files on a regular schedule. The goal of recovery is to recover to a known state. Common issues that require recovery include the following:

- **System reboot**: An unexpected/unscheduled event can cause a system reboot.
- **System restart**: This automatically occurs when a system goes down and forces an immediate reboot.
- **System cold start**: This results from a major failure or component replacement.
- **System compromise**: This can be caused by an attack or a breach of security.

Process Isolation

Process isolation is required to maintain a high level of system trust. For a system to be certified as a multilevel security system, it must support process isolation. Without process isolation, there would be no way to prevent one process from spilling over into another process's memory space, corrupting data, or possibly making the whole system unstable. *Process isolation* is performed by the operating system; its job is to enforce memory boundaries. Separation of processes is an important topic; without it, a system could be designed with a *single point of failure* (*SPOF*) so that one flaw in the design or configuration could cause the entire system to stop operating.

For a system to be secure, the operating system must prevent unauthorized users from accessing areas of the system to which they should not have access, it should be robust, and it should have no single point of failure. Sometimes all this is accomplished through the use of a virtual machine. A virtual machine allows users to believe that they have the use of the entire system, but in reality, processes are completely isolated. To take this concept a step further, some systems that require truly robust security also implement hardware isolation so that the processes are segmented not only logically but also physically.

Note

Java uses a form of virtual machine because it uses a sandbox to contain code and allows it to function only in a controlled manner.

Common Formal Security Models

Security models are used to determine how security will be implemented, what subjects can access the system, and what objects they will have access to. Simply stated, a security model formalizes security policy. Security models of control are typically implemented by enforcing integrity, confidentiality, or other controls. Keep in mind that each of these models lays out broad guidelines and is not specific in nature. It is up to the developer to decide how these models will be used and integrated into specific designs (see Figure 4.7).

The sections that follow discuss the different security models of control in greater detail. The first three models discussed are considered lower-level models.

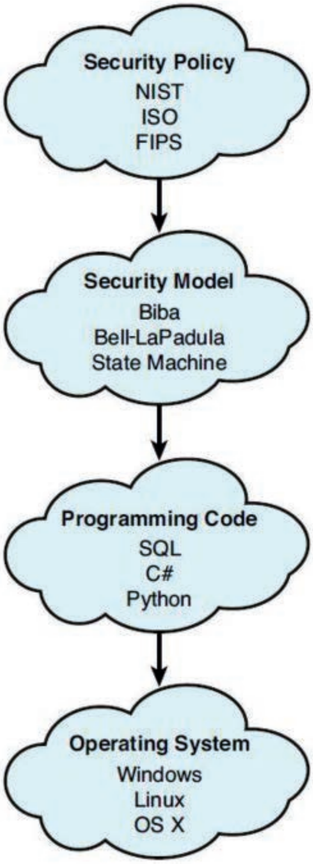


FIGURE 4.7 **Security Model Fundamental Concepts Used in the Design of an OS**

State Machine Model

The *state machine model* is based on a finite state machine (see Figure 4.8). State machines are used to model complex systems and deal with acceptors, recognizers, state variables, and transaction functions. A state machine defines the behavior of a finite number of states, the transitions between those states, and actions that can occur.

The most common representation of a state machine is through a state machine table. For example, as Table 4.3 illustrates, if the state machine is at the current state B and condition 2, the next state would be C and condition 3 as we progress through the options.

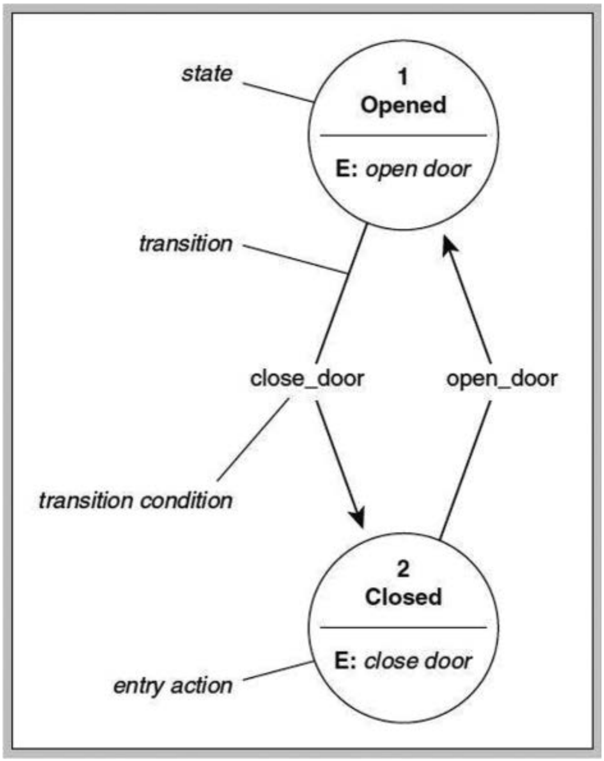


FIGURE 4.8 **Finite State Model**

TABLE 4.3 **State Machine Table**

State Transaction	State A	State B	State C
Condition 1	…	…	…
Condition 2	…	Current state	…
Condition 3	…	…	…

A state machine model monitors the status of the system to prevent it from slipping into an insecure state. Systems that support the state machine model must have all their possible states examined to verify that all processes are controlled in accordance with the system security policy. The state machine concept serves as the basis of many security models. The model is valued for knowing in what state the system will reside. For example, if the system boots up in a secure state, and every transaction that occurs is secure, it must always be in a secure state and will not fail open. (To *fail open* means that all traffic or actions are allowed rather than denied.)

Information Flow Model

The *information flow model* is an extension of the state machine concept and serves as the basis of design for both the Biba and Bell-LaPadula models, which are discussed later in this chapter. The information flow model consists of objects, state transitions, and lattice (flow policy) states. The goal with this model is to prevent unauthorized, insecure information flow in any direction. This model and others can make use of *guards*, which allow the exchange of data between various systems.

Noninterference Model

The *noninterference model*, defined by Goguen and Meseguer, was designed to make sure that objects and subjects of different levels don't interfere with objects and subjects of other levels. The model uses inputs and outputs of either low or high sensitivity. Each data access attempt is independent of all others, and data cannot cross security boundaries.

Confidentiality

Although the models described so far serve as a basis for many security models developed later, one major concern with those earlier models is confidentiality. Government entities such as the DoD are concerned about the confidentiality of information. The DoD divides information into categories to ease the burden of managing who has access to various levels of information. The DoD information classifications are sensitive but unclassified (SBU), confidential, secret, and top secret. The Bell-LaPadula model was one of the first models to address the confidentiality needs of the DoD.

Bell-LaPadula Model

The *Bell-LaPadula state machine model* enforces confidentiality. This model uses mandatory access control to enforce the DoD multilevel security policy. For subjects to access information, they must have a clear need to know and must meet or exceed the information's classification level.

The Bell-LaPadula model is defined by the following properties:

- **Simple security (ss) property**: This property states that a subject at one level of confidentiality is not allowed to read information at a higher level of confidentiality. This is sometimes referred to as "no read up." Figure 4.9 provides an example.

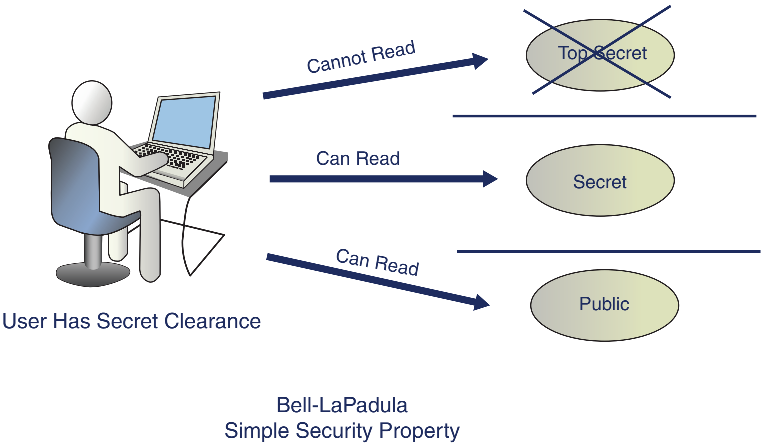


FIGURE 4.9 **Bell-LaPadula Simple Security Model**

- **Star (*) security property**: This property states that a subject at one level of confidentiality is not allowed to write information to a lower level of confidentiality. This is also known as "no write down." Figure 4.10 provides an example.

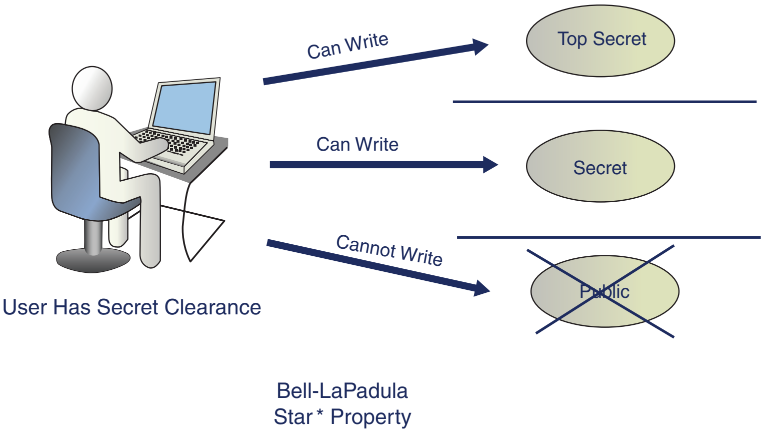


FIGURE 4.10 **Bell-LaPadula Star Property**

- **Strong star property**: This property states that a subject cannot read or write to an object of higher or lower sensitivity. Figure 4.11 provides an example.

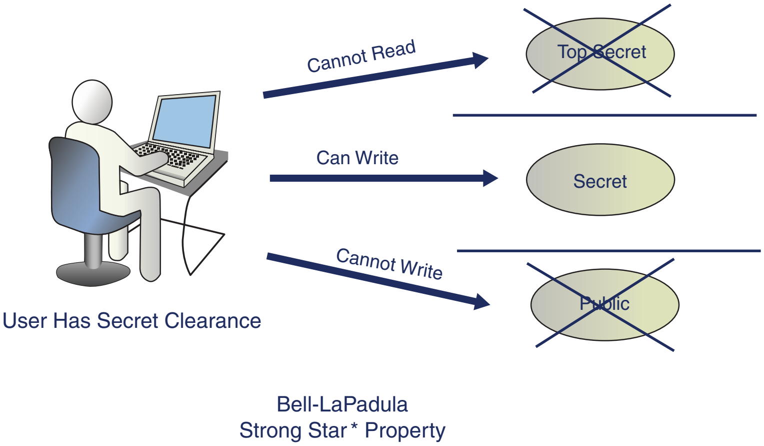


FIGURE 4.11 **Bell-LaPadula Strong Star Property**

ExamAlert

Review the Bell-LaPadula simple security and star security models closely; they are easy to confuse with Biba's two defining properties.

Tip

A fourth but rarely implemented property of the Bell-LaPadula model called the *discretionary security property* allows users to grant access to other users at the same clearance level by means of an access matrix.

Although the Bell-LaPadula model goes a long way in defining the operation of secure systems, the model is not perfect. It does not address security issues such as covert channels. It was designed in an era when mainframes were the dominant platform. It was designed for multilevel security and takes only confidentiality into account.

Tip

It is important to know that the Bell-LaPadula model deals with confidentiality. This means that reading information at a higher level than is allowed endangers confidentiality.

Integrity

Integrity is a good thing. It is one of the basic elements of the security triad, along with confidentiality and availability. Integrity plays an important role in security because it can be used to verify that unauthorized users are not modifying data, authorized users don't make unauthorized changes, and databases balance and data remains internally and externally consistent. Whereas governmental entities are typically very concerned with confidentiality, other organizations might be more focused on the integrity of information. In general, integrity has four goals:

- Prevent data modification by unauthorized parties
- Prevent unauthorized data modification by authorized parties
- Reflect the real world
- Maintain internal and external consistency

> **Note**
>
> Some sources list only three goals of security by combining the third and fourth goals into one: maintain internal and external consistency and ensure that the data reflects the real world.

Two security models that address secure systems integrity include Biba and Clark-Wilson models, which are covered in the following sections. The Biba model addresses only the first integrity goal, and the Clark-Wilson model addresses all four goals.

Biba Model

The *Biba model* was the first model developed to address integrity concerns. Originally published in 1977, this lattice-based model has the following defining properties:

- **Simple integrity property**: This property states that a subject at one level of integrity is not permitted to read an object of lower integrity.
- **Star (*) integrity property**: This property states that an object at one level of integrity is not permitted to write to an object of higher integrity.
- **Invocation property**: This property prohibits a subject at one level of integrity from invoking a subject at a higher level of integrity.

Tip

The star property in both the Biba and Bell-LaPadula models deals with writes. One easy way to remember these rules is to think, "It's written in the stars!"

The Biba model addresses only the first goal of integrity: protecting the system from access by unauthorized users. Other types of concerns such as confidentiality are not examined. This model also assumes that internal threats are being protected by good coding practices, and it therefore focuses on external threats.

Tip

To remember the purpose of the Biba model, you can think that the *i* in *Biba* stands for integrity.

Tibetan Monks and the Biba Model

When learning about the CISSP exam Security Architecture and Engineering domain in the classroom, students are eager for examples related to the material on security models. I typically use the well-known story of Tibetan monks.

After a long journey on your search for Shangri-La and true security awareness, you arrive at a Tibetan monastery. You discover that the monks there are huge fans of the Biba model and, like you, have studied for the CISSP exam. As such, they have defined certain rules that you, the commoner, must abide by:

- A Tibetan monk may write a prayer book that can be read by commoners but not one to be read by a high priest.
- A Tibetan monk may read a book written by the high priest but may not read down to a pamphlet written by a commoner.

Consider this story when you are trying to conceptualize the Biba model, and it might make the task a little easier. A final tip is to look at the star (*) property for both the Bell-LaPadula model and the Biba model and notice how both star properties deal with writes. If this property is applied to Bell-LaPadula, a confidentiality model, the result is *no write down*. If the star property is applied to the Biba model, an integrity model, the result is *no write up*. Just by knowing one, you can easily solve the other.

Tip

Remember that the Biba model deals with integrity and, as such, writing to an object of a higher level might endanger the integrity of the system.

Clark-Wilson Model

The *Clark-Wilson model*, which was created in 1987, differs from previous models because it was developed to be used for commercial activities. This model addresses all four goals of integrity. The Clark-Wilson model dictates that the separation of duties must be enforced, subjects must access data through an application, and auditing is required. Some terms associated with this model include the following:

- User
- Transformation procedure
- Unconstrained data item
- Constrained data item
- Integrity verification procedure

The Clark-Wilson model features an access control triple, where subjects must access programs before accessing objects (subject–program–object). The access control triple is composed of the user, a transformational procedure, and the constrained data item. It was designed to protect integrity and prevent fraud. Authorized users cannot change data in an inappropriate way. The Clark-Wilson model checks three attributes: tampered, logged, and consistent (TLC).

The Clark-Wilson model differs from the Biba model in that subjects are restricted. This means that a subject at one level of access can read one set of data, whereas a subject at another level has access to a different set of data. The Clark-Wilson model controls the way in which subjects access objects so that the internal consistency of the system can be ensured, and data can be manipulated only in ways that protect consistency. Integrity verification procedures (IVPs) ensure that a data item is in a valid state. Data cannot be tampered with while being changed, and the integrity of the data must be consistent. The Clark-Wilson model requires all changes to be logged.

The Clark-Wilson model is made up of transformation procedures (TPs). Constrained data items (CDIs) are data for which integrity must be preserved. Items not covered under the model are considered unconstrained data items (UDIs).

Tip

Remember that the Clark-Wilson model requires that users be authorized to access and modify data, and it deals with three key terms: tampered, logged, and consistent (TLC).

Take-Grant Model

The *Take-Grant model* is another confidentiality-based model that supports four basic operations: take, grant, create, and revoke. This model allows subjects with the take right to remove take rights from other subjects. Subjects possessing the grant right can grant this right to other subjects. The create and revoke operations work in the same manner: Someone with the create right can give the create right to others, and those with the revoke right can remove that right from others.

Brewer and Nash Model

The *Brewer and Nash model* is similar to the Bell-LaPadula model and is also sometimes referred to as the *Chinese Wall model*. It was developed to prevent conflict of interest (COI) problems. The Brewer and Nash model is context oriented in that it prevents a worker consulting for one firm from accessing data belonging to another, thereby preventing any COI. For example, imagine that your security firm does security work for many large firms. If one of your employees could access information about all the firms that your company has worked for, that person might be able to use this data in an unauthorized way.

Other Models

A security model defines and describes what protection mechanisms are to be used and what these controls are designed to achieve. The previous sections cover some of the most heavily tested models, but you should have a basic understanding of a few more security models, including the following:

- **Graham-Denning model**: This model uses a formal set of eight protection rules for which each object has an owner and a controller. These rules define what you can create, delete, read, grant, or transfer.

- **Harrison-Ruzzo-Ullman model**: This model is similar to the Graham-Denning model and details how subjects and objects can be created, deleted, accessed, or changed.

- **Lipner model**: This model combines elements of the Bell-LaPadula and Biba models to guard both confidentiality and integrity.

- **Lattice model**: This model is associated with MAC. Controls are applied to objects, and the model uses security levels that are represented by a lattice structure; this structure governs information flow. Subjects of the lattice model are allowed to access an object only if the security level of the subject is equal to or greater than that of the object. Overall access limits are set by having a least upper bound and a greatest lower bound for each security level.

ExamAlert

Spend some time reviewing all the models discussed in this section. Make sure you know which models are integrity based, which are confidentiality based, and the properties of each; you will need to know this information for the CISSP exam.

Tip

Although the security models described in this section are the ones the CISSP exam is most likely to focus on, there are many other models, such as the Sutherland, Boebert and Kain, Karger, Gong, and Jueneman models. Even though many security professionals may have never heard of these models, those who develop systems most likely learned of them in college.

Product Security Evaluation Models

A set of evaluation standards is needed when evaluating the security capabilities of information systems. A number of documents and guidelines have been developed to help evaluate and establish system assurance. These items are important to a CISSP candidate because they provide a level of trust and assurance that these systems will operate in a given and predictable manner. A trusted system has undergone testing and been validated to a specific standard. Assurance means freedom from doubt and a level of confidence that a system will perform as required every time it is used.

Think of product evaluation models as being similar to EPA gas mileage ratings, which give buyers and sellers a way to evaluate different automotive brands and models. In the world of product security, developers can use product evaluation systems when preparing to sell a system. A buyer can use the same evaluation models when preparing to make a purchase, as they provide a way to measure a system's effectiveness and benchmark its abilities. The following sections describe documents and guidelines that facilitate these needs.

The Rainbow Series

The Rainbow Series is so named because each book in the series has a label of a different color. This 6-foot-tall stack of books was developed by the National Computer Security Center (NCSC), an organization that is part of the National Security Agency (NSA). These guidelines were developed for the Trusted Product Evaluation Program (TPEP), which tests commercial products against a comprehensive set of security-related criteria. The first of these books, released in 1983, is known as *Trusted Computer System Evaluation Criteria* (*TCSEC*), or the Orange Book. Many similar guides were also known by the color of the cover instead of their name, such as the Red Book. While the Orange Book is no longer commercially used, understanding TCSEC will help you understand how product security evaluation models have evolved into what we use today.

Note

Rainbow Series guidelines have all been replaced with Common Criteria, described later in this chapter.

The Orange Book: Trusted Computer System Evaluation Criteria

The Orange Book was developed to evaluate standalone systems. Its basis of measurement is confidentiality, so it is similar to the Bell-LaPadula model.

Note

Canada has its own version of the Orange Book, known as *The Canadian Trusted Computer Product Evaluation Criteria* (*CTCPEC*). It too has been replaced by Common Criteria.

Although the Orange Book is no longer considered current, it was one of the first product security standards. Table 4.4 lists the Orange Book levels.

TABLE 4.4 **Orange Book Levels**

Level	Items to Remember
A1	Built, installed, and delivered in a secure manner
B1	Security labels (MAC)
B2	Security labels and verification of no covert channels (MAC)
B3	Security labels, verification of no covert channels, and must stay secure during startup (MAC)
C1	Weak protection mechanisms (DAC)
C2	Strict login procedures (DAC)
D1	Failed or was not tested

The Red Book: Trusted Network Interpretation

The Red Book's official name is the *Trusted Network Interpretation* (*TNI*). The purpose of the TNI is to examine security for network and network components. Whereas the Orange Book addresses only confidentiality, the Red Book examines integrity and availability. It also is tasked with examining the operation of networked devices. The Red Book addresses three areas of reviews:

- **Denial of service (DoS) prevention**: Management and continuity of operations
- **Compromise protection**: Data and traffic confidentiality and selective routing
- **Communications integrity**: Authentication, integrity, and nonrepudiation

Information Technology Security Evaluation Criteria (ITSEC)

ITSEC is a European standard developed in the 1980s to evaluate confidentiality, integrity, and availability of an entire system. ITSEC is unique in that it was the first standard to unify markets and bring all of Europe under one set of guidelines. ITSEC designates the target system as the target of evaluation (TOE). The evaluation is actually divided into two parts: One part evaluates functionality, and the other evaluates assurance.

ITSEC speaks of 10 functionality (F) classes and 7 assurance (E) classes. Assurance classes rate the effectiveness and correctness of a system. Table 4.5 shows these ratings and how they correspond to the TCSEC ratings.

TABLE 4.5 **ITSEC Functionality Ratings and Comparison to TCSEC**

F Class Rating	E Class Rating	TCSEC Rating
NA	E0	D
F1	E1	C1
F2	E2	C2
F3	E3	B1
F4	E4	B2
F5	E5	B3
F5	E6	A1

F Class Rating	E Class Rating	TCSEC Rating
F6	—	TOEs with high integrity requirements
F7	—	TOEs with high availability requirements
F8	—	TOEs with high integrity requirements during data communications
F9	—	TOEs with high confidentiality requirements during data communications
F10	—	Networks with high confidentiality and integrity requirements

Common Criteria

With all the standards we have discussed to this point, it is easy to see how someone might have a hard time determining which one is the right choice. The International Organization for Standardization (ISO) had this thought as well, and it decided that instead of the various standards and ratings that existed, there should be a single global standard. Figure 4.12 illustrates the development of Common Criteria.

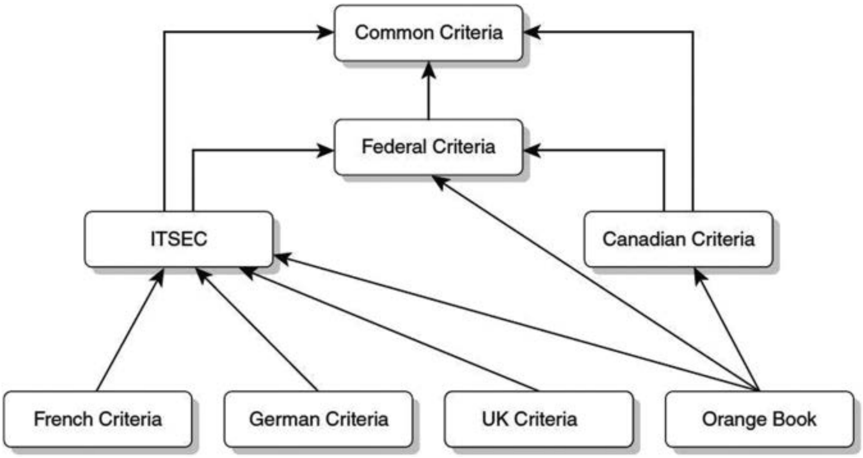


FIGURE 4.12 Common Criteria Development

In 1997, the ISO released *Common Criteria* (ISO 15408), which is an amalgamated version of TCSEC, ITSEC, and CTCPEC. Common Criteria is designed around TCB entities, which include physical and logical controls, startup and recovery, reference mediation, and privileged states. Common Criteria categorize assurance into one of seven increasingly strict levels of assurance, referred to as *evaluation assurance levels* (*EALs*):

- **EAL 1**: Functionality tested
- **EAL 2**: Structurally tested
- **EAL 3**: Methodically checked and tested
- **EAL 4**: Methodically designed, tested, and reviewed
- **EAL 5**: Semi-formally designed and tested
- **EAL 6**: Semi-formally verified, designed, and tested
- **EAL 7**: Formally verified, designed, and tested

EALs provide a specific level of confidence in the security functions of the system being analyzed.

ExamAlert

If you are looking for an example of a high-level EAL 6 operating system, look no further than Integrity 178B by Green Hills software. This secure OS is used in jet fighters and other critical devices.

Like ITSEC, Common Criteria defines two types of security requirements: *functional* and *assurance*. Functional requirements define what a product or system does. They also define the security capabilities of a product. The assurance requirements and specifications to be used as the basis for evaluation are known as the *security target* (*ST*). A protection profile defines the system and its controls. The protection profile is divided into five sections:

- Rationale
- Evaluation assurance requirements
- Descriptive elements
- Functional requirements
- Development assurance requirements

A security target consists of seven sections:

- Introduction
- Conformance Claims
- Security Problem Definition

- Security Objectives
- Extended Components Definition
- Security Requirements
- TOE Security Specifications

A Common Criteria certification contains either a protection profile (PP) or a security target (ST).

Assurance requirements define how well a product is built. Assurance requirements inspire confidence in the product and show the correctness of its implementation.

> **ExamAlert**
>
> Common Criteria's seven levels of assurance and two security requirements are required knowledge for the CISSP exam.

System Validation

No system or architecture will ever be completely secure; there will always be a certain level of risk. Security professionals must understand this risk and be comfortable with it, mitigate it, or offset it through a third party. All the documentation and guidelines already discussed dealt with ways to measure and assess risk. These can be a big help in ensuring that the implemented systems meet your requirements. However, before you begin to use the systems, you must complete the two additional steps of certification and accreditation.

U.S. federal agencies are required by law to have their IT systems and infrastructures certified and accredited. Although you shouldn't expect to see in-depth certification and accreditation questions on the CISSP exam, it is worth knowing if you plan to interact with any agencies that require their use. These methodologies look at much more than a standard penetration test; they are more like an audit. They must validate that the systems are implemented, configured, and operating as expected and meet all security policies and procedures.

Certification and Accreditation

Certification is the process of validating that implemented systems are configured and operating as expected. It also validates that the systems are connected to and communicate with other systems in a secure and controlled manner and that they handle data in a secure and approved manner. The certification process is a technical evaluation of the system that can be carried out by independent security teams or by the existing staff. Its goal is to uncover any vulnerabilities or weaknesses in the implementation.

The results of the certification process are reported to the organization's management for mediation and approval. If management agrees with the findings of the certification, the report is formally approved. The formal approval of the certification is the *accreditation process*. Management usually issues accreditation as a formal, written approval that the certified system is approved for use as specified in the certification documentation. If changes are made to the system or in the environment in which the system is used, a recertification and accreditation process must be repeated. The entire process is periodically repeated at intervals, depending on the industry and the regulations the organization must comply with. For example, Section 404 of Sarbanes-Oxley requires an annual evaluation of internal systems that deal with financial controls and reporting systems.

ExamAlert

For the CISSP exam, you might want to remember that certification is seen as the technical aspect of validation, whereas accreditation is management's approval.

Note

Nothing lasts forever, including certification. The certification process should be repeated when systems change, when items are modified, or on a periodic basis.

Vulnerabilities of Security Architectures

Like most other chapters of this book, this one also reviews potential threats and vulnerabilities. Any time a security professional makes the case for stronger security, there will be those who ask why funds should be spent that way. It's important to point out not only the benefits of good security but also the potential risks of not implementing good practices and procedures.

We live in a world of risk. As security professionals, we need to be aware of the threats to security and understand how the various protection mechanisms discussed throughout this chapter can be used to raise the level of security.

Buffer Overflows

Buffer overflows occur because of poor coding techniques. A *buffer* is a temporary storage area that has been coded to hold a certain amount of data. If additional data is fed to the buffer, it can spill over or overflow to adjacent buffers. This can corrupt those buffers and cause the application to crash or possibly allow an attacker to execute his own code that he has loaded onto the stack. Ideally, programs should be written with error checking—such as to check that you cannot type 32 characters into a 24-character buffer; however, this type of error checking does not always occur. Error checking is really nothing more than making sure that buffers receive the correct type and amount of information required. Here is an example of a buffer overflow:

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
int abc()
{
 char buffer[8];
 strcpy(buffer, "AAAAAAAAAA";
 return 0;
}
```

OS vendors are also working to make buffer overflow attacks harder by using techniques such as data execution prevention (DEP) and address space layout randomization (ASLR). DEP marks some areas of memory as either executable or non-executable. DEP can help avert some attacks by preventing the writing of malicious commands designed to be stored in memory. ASLR randomly rearranges address space positions of data. Think of the shell game, where a small ball is placed under one of three shells and is then moved around. To win the game, you must guess which shell the ball is under. Most modern operating systems, such as Android, Windows, and FreeBSD, make use of ASLR.

Other defenses for buffer overflows include code reviews, using safe programming languages, and applying patches and updates in a timely manner. Finally, because all data should be suspect by default, data being input, processed, or output should be checked to make sure it matches the correct parameters.

Backdoors

Backdoors are potential threats to the security of systems and software. Programmers use *backdoors*, which are also sometimes referred to as *maintenance hooks*, during development to allow easy access to a piece of software. Often these backdoors are undocumented. A backdoor can be used when software is developed in sections and developers want a means of accessing certain parts of the program without having to run through all the code. If backdoors are not removed before the release of the software, they can allow an attacker to bypass security mechanisms and access the program.

State Attacks

A state attack is a form of attack that typically targets timing. The objective is to exploit the delay between the time of check (TOC) and the time of use (TOU). These attacks are sometimes called *asynchronous attacks* or *race conditions* because the attacker races to make a change to the object after it has been checked but before the system uses it.

For example, if a program creates a date file to hold the amount a customer owes, and the attacker can race to replace this value before the program reads it, he can successfully manipulate the program. In reality, it can be difficult to exploit a race condition because a hacker might have to attempt to exploit the race condition many times before succeeding.

Covert Channels

Covert channels provide a means of moving information in a manner that was not intended. Covert channels are a favorite of attackers because they know that you cannot deny what you must permit. The term was originally used in TCSEC documentation to refer to ways of transferring information from a higher classification to a lower classification. Covert channel attacks can be broadly separated into two types:

- **Covert timing channel attacks**: Timing attacks are difficult to detect. They function by altering a component or by modifying resource timing.
- **Covert storage channel attacks**: These attacks use one process to write data to a storage area and another process to read the data.

Here is an example of how covert channel attacks happen in real life. Your organization has decided to allow ping (Internet Control Message Protocol [ICMP]) traffic into and out of your network. Based on this knowledge, an attacker has planted the Loki program on your network. Loki uses the payload portion of a ping packet to move data into and out of your network. Therefore, the network administrator sees nothing but normal ping traffic and is not alerted, even though the attacker is busy stealing company secrets. Sadly, many programs can perform this type of attack.

ExamAlert

The CISSP exam expects you to understand the two types of covert channel attacks.

Incremental Attacks

The goal of an incremental attack is to make changes slowly over time. By making small changes over long periods, an attacker hopes to remain undetected. Two primary incremental attacks are *data diddling*, which is possible if the attacker has access to the system and can make small incremental changes to data or files, and *salami attack*, which is similar to data diddling but involves making small changes to financial accounts or records, often referred to as "cooking the books."

Emanations

Anyone who has seen movies such as *Enemy of the State* or *The Conversation* knows something about surveillance technologies and conspiracy theories. If you have ever thought that only fringe elements are worried about such things, guess again. This might sound like science fiction, but the U.S. government was concerned enough about the possibility of emanation of stray electrical signals from electronic devices that the Department of Defense started a program to study emanation leakage.

Research actually began in the 1950s, and this research eventually led to the TEMPEST technology. The fear was that attackers might try to sniff the stray electrical signals that emanate from electronic devices. Devices built to TEMPEST standards, such as cathode ray tube (CRT) monitors, have had TEMPEST-grade copper mesh, known as a *Faraday cage*, embedded in the case to prevent signal leakage. This costly technology is found only in very high-security environments.

TEMPEST is now considered somewhat dated; newer technologies, such as white noise and control zones, are now used to control emanation security. *White noise* involves using special devices that send out a stream of frequencies that makes it impossible for an attacker to distinguish the real information. *Control zones* are facilities whose walls, floors, and ceilings are designed to block electrical signals from leaving the zone.

Another term associated with this category of technology is *Van Eck phreaking*. This is the name given to eavesdropping on the contents of a CRT through emanation leakage. Although this technique sounds far-fetched, Cambridge University successfully demonstrated the technique against an LCD monitor in 2004.

ExamAlert

For the CISSP exam, you need to know the technologies and techniques implemented to prevent intruders from capturing and decoding information emanated through the airwaves. TEMPEST, white noise, and control zones are the three primary controls.

Web-Based Vulnerabilities

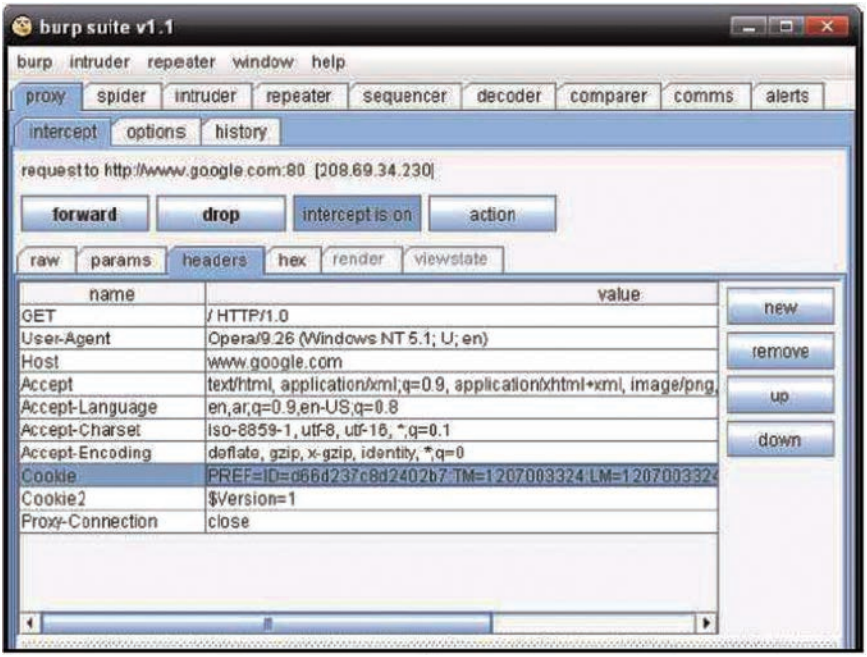
Vulnerabilities in web-based systems involve application flaws or weaknesses in design. Exploits can be launched from a client or server. For example, an input validation attack occurs when client-side input is not properly validated. Application developers should never assume that users will input the correct data. A user bent on malicious activity will attempt to stretch a protocol or an application in an attempt to find possible vulnerabilities. Parameter problems are best solved by implementing pre-validation and post-validation controls. Pre-validation is implemented in the client but can be bypassed by using proxies and other injection techniques. Post-validation is performed to ensure that a program's output is correct. Other security issues directly related to a lack of input validation include the following:

- **Cross-site scripting (XSS)**: An attack that exploits trust so that an attacker uses a web application to send malicious code to a web server or an application server.
- **Cross-site request forgery (CSRF)**: An attack that involves third-party redirection of static content so that unauthorized commands are transmitted from a user that the website trusts.
- **Direct OS commands**: The unauthorized execution of OS commands.
- **Directory traversal attack**: A technique that allows an attacker to move from one directory to another.

- **Unicode encoding**: A technique used to bypass security filters. One famous example used the Unicode string "%c0%af..%c0%af..".
- **URL encoding**: Used by an attacker to hide or execute an invalid application command via an HTTP request (for example, www.knowthetrade.com%2fmalicious.js%22%3e%3c%2fscript%3e).

> **Tip**
>
> XSS and CSRF are sometimes confused, so just keep in mind that one key difference is that XSS executes code in a trusted context.

One of the things that makes a programmer's life difficult is that there is no such thing as trusted input. All input is potentially bad and must be verified. While the buffer overflow is the classic example of poor input validation, these attacks have become much more complex: Attackers have learned to insert malicious code in the buffer instead of just throwing "garbage" (that is, typing random gibberish) at an application to cause a buffer to overflow—which is just messy. There are also many tools available to launch these attacks; Figure 4.13 shows one example.


burp suite v1.1
burp intruder repeater window help
proxy spider intruder repeater sequencer decoder comparer comms alerts
intercept options history
forward
drop
intercept is on
action
raw params headers hex render viewstate
new
remove
up
down

request to http://www.google.com:80 [208.69.34.230]

name	value
GET	/ HTTP/1.0
User-Agent	Opera/9.26 (Windows NT 5.1; U; en)
Host	www.google.com
Accept	text/html, application/xml;q=0.9, application/xhtml+xml, image/png,
Accept-Language	en,ar;q=0.9,en-US;q=0.8
Accept-Charset	iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding	deflate, gzip, x-gzip, identity, *;q=0
Cookie	PREF=ID=d66d237c8d2402b7:TM=1207003324:LM=120700332
Cookie2	$Version=1
Proxy-Connection	close

FIGURE 4.13 The Burp Proxy Attack Tool

Attackers may also use the following techniques to exploit poor input validation:

- XML injection
- LDAP injection
- SQL injection

All of these are the same type of attack, but they target different platforms.

Databases are another common target of malformed input. An attacker can attempt to insert database or SQL commands to disrupt the normal operation of a database. This could cause the database to become unstable and leak information. This type of attack is known as *SQL injection*. The attacker searches for web pages in which to insert SQL commands. Attackers use logic such as ' (a single quote) to test the database for vulnerabilities. Responses such as the one shown in the following code give the attacker the feedback needed to know that the database is vulnerable to attack:

```
Microsoft OLE DB Provider for ODBC Drivers error '80040e07'
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting
the nvarchar value 'sa login' to a column of data type int.
/index.asp, line 5
```

Although knowledge of the syntax and response used for a database attack is not required for the CISSP exam, it is useful to know this information as you attempt to secure your infrastructure.

> **Caution**
>
> SQL injection attacks are among the top attack vectors and are responsible for a large number of attacks. CISSP candidates should understand the threat these attacks pose.

Injection attacks, such as SQL, LDAP, and others, can occur in many different programs and applications and take advantage of a common problem: No separation exists between the application code and the input data, which makes it possible for attackers to run their code on the victim's system. Injection attacks require the following:

- **Footprinting**: It is necessary to determine what technology the web application is running.
- **Identifying**: User input points must be identified.

- **Testing**: User input that is susceptible to the attack must be tested.
- **Exploiting**: Extra bits of code are placed into the input to execute commands on the victim's computer.

Mobile System Vulnerabilities

Mobile devices have increased in power and now have the ability to handle many tasks that previously only desktops and laptops could perform. More and more employees are bringing their own mobile devices to work and using them on corporate networks. Organizations might have a number of concerns about this arrangement, including the following:

- Eavesdropping on voice calls
- Mobile viruses and malware
- Plaintext storage on mobile devices
- Ease of loss and theft of mobile device
- Camera phones' ability to photograph sensitive information
- Large storage ability, which can lead to data theft or exfiltration
- Software that exposes local device data such as names, email addresses, or phone numbers

Bring your own technology (*BYOT*), also known as *bring your own device* (*BYOD*), requires an organization to build in administrative and technical controls to govern how the devices can be used at work. Some of these basic controls might include the following:

- **Passwords**: One of the most basic and cheapest means of protecting a mobile system is to enforce use of passwords. Also, having the ability to remote wipe a missing or stolen device is recommended for corporate devices.
- **Multifactor authentication (MFA)**: Multiple forms of authentication strengthen passwords. For example, a user might be required to use Okta or Microsoft MFA to approve a login from an unknown location.
- **Session lifetimes**: Limiting session times and cookies can promote security by logging users out of sensitive services after a set amount of idle time.
- **Wireless vulnerabilities**: Wireless networks are often vulnerable to attack. For example, an attacker might be able to set up a rogue wireless access point and launch a man-in-the-middle attack.

- **Unpatched OS, software, or browser**: Mobile devices, like other computing devices, must be patched at regular periodic intervals.
- **Insecure devices**: Jailbroken devices pose a risk for corporate networks as they are likely to be missing patches and other security updates.
- **Mobile device management**: Mobile device management (MDM) and mobile application management (MAM) can be used to secure devices and can allow only managed devices to access company resources.

Cryptography

Cryptography involves transforming plaintext data to unreadable data, or cipher text. Today, cryptographic systems are mandatory to protect email, corporate data, personal information, and electronic transactions.

To give you a good understanding of cryptography, this section reviews how it relates to the foundations of security: privacy, authentication, integrity, and nonrepudiation.

> **Tip**
>
> One easy way to remember the primary goals of cryptography is to think of their initials, which spell PAIN: privacy, authentication, integrity, and nonrepudiation.

Confidentiality, or privacy, is the ability to guarantee that private information stays private. Cryptography provides confidentiality by transforming data. This transformation is called *encryption*. Encryption can protect confidentiality of information in storage or in transit. Just think about a CEO's laptop. If it is lost or stolen, what is really worth more: the laptop or information regarding next year's hot new product line? Information assets can be worth much more than the equipment on which they are stored. Hard disk encryption offers an easy way to protect information in the event that equipment is lost, stolen, or accessed by unauthorized individuals.

Authentication has several roles. First, authentication is usually associated with message encryption. Authentication provides a way to ensure that data or programs have not been modified and really come from the source that you believe them to have come from. Authentication is also used to confirm a user's identity and is part of the identification and authentication process. The most common implementation of identification and authentication is with a username and password. Most passwords are encrypted, but they do not have to be. Without encryption, the authentication process is very weak. FTP and Telnet are examples of weak authentication. With these protocols, usernames and passwords are passed in unencrypted (that is, in plaintext), and anyone with access to the communication stream can intercept and capture these passwords. Virtual private networks (VPNs) also use authentication, but instead of using a plaintext username and password, they normally use digital certificates and digital signatures to more accurately identify the user and to protect the authentication process against spoofing.

Integrity is the assurance that information remains unaltered from the point at which it is created until it is received. If you're selling widgets on the Internet for $100 each, you will likely go broke if a criminal can change the posted price to $1 at checkout. Integrity is critical for the exchange of information, be it engaging in e-commerce, maintaining trade secrets, or supplying accurate military communications.

Nonrepudiation is the capability to verify proof of identity. Nonrepudiation is used to ensure that a sender of data is provided with proof of delivery and that the recipient is assured of the sender's identity. Neither party should be able to deny having sent or received the data at a later date. In the days of face-to-face transactions, nonrepudiation was not as hard to prove as it is today. The Internet makes many transactions faceless. You might never see the people that you deal with, and nonrepudiation is all the more critical. Nonrepudiation is achieved through digital signatures, digital certificates, and message authentication codes (MACs).

To help make this section a little easier to digest, review the following basic terms that are used throughout the rest of this chapter:

- **Plaintext**: Text that is directly readable. Sometimes also called cleartext.
- **Encryption**: The transformation of plaintext into ciphertext.
- **Ciphertext**: Text that has been rendered unreadable by encryption.
- **Cryptographic algorithm**: A set of mathematical procedures used to encrypt and decrypt data in a cryptographic system. For example, a simple transposition cypher such as Caesar's cipher simply shifts characters forward or backward three characters in the alphabet.
- **Cryptographic key**: A piece of information, also called a crypto variable, that controls how a cryptographic algorithm functions. It can be used to control the transformation of plaintext to ciphertext or ciphertext to plaintext. For example, an algorithm that shifts characters might use the key "+3" to shift characters forward by three positions. The word "cat" would be encrypted as "fdw" using this algorithm and key.

- **Key management**: The generation, distribution, storage, and disposition of cryptographic keys. Key management is an important piece of the cryptographic process. Any portion of the key management process that is not handled correctly creates an opportunity to compromise the cryptographic system.
- **Digital rights management (DRM)**: A process that involves using tools, standards, and systems to protect intellectual property and copyrighted materials from misuse or theft. DRM is composed of data protection and data governance. Encryption technologies are used to provide data protection, and trust and policy management allow data governance so information can be distributed and used by authorized entities.
- **Steganography**: The process of hiding a piece of information inside another message. Images, audio, and video are three example of messages that can be used to hide information.
- **Symmetric cryptography**: Cryptography that provides for confidentiality by using a single key, a shared key, or the same key for both encryption and decryption.
- **Asymmetric cryptography**: Cryptography that uses a private and public key pair for encryption and decryption. Both keys have dual functionality: What one key encrypts, the other key decrypts. Asymmetric cryptography provides for confidentiality, authentication, and nonrepudiation.
- **Cryptanalysis**: The art and science of breaking a cryptography system or obtaining plaintext from ciphertext without a cryptographic key. Governments, the military, enterprises, and malicious hackers use cryptanalysis to find weaknesses and crack cryptographic systems.
- **Message digest or hash**: A fixed-length hex string used to uniquely identify a variable amount of data.
- **Digital signature**: A hash value that is encrypted with a sender's private key and used for authentication and integrity.

When symmetric encryption is used to convert plaintext into ciphertext, the transformation can be accomplished by using two types of ciphers:

- **Block ciphers**: Ciphers that separate the message into blocks for encryption and decryption
- **Stream ciphers**: Ciphers that divide the message into bits for encryption and decryption

Algorithms

An *algorithm* is a set of rules used to encrypt and decrypt data. It's a set of instructions that is used with a cryptographic key to encrypt plaintext data. Encrypting plaintext data with different keys or with dissimilar algorithms produces different ciphertext.

Not all cryptosystems are of the same strength. The strength of a cryptosystem relies on the strength of an algorithm because a flawed algorithm can be broken. However, the strength of encryption also depends on the size and complexity of the key. For example, imagine that you're contemplating buying a combination lock. One lock has 3 digits, whereas the other has 4. Which would you choose? Consider that there are 1,000 possible combinations for the 3-digit lock, but there are 10,000 possible combinations for the 4-digit lock. As you can see, just a 1-digit increase can create a significant difference. The more possible keys or combinations there are, the longer it takes an attacker to guess the right key.

The size of the key—whether it is 4 possible numbers, 7 possible numbers, or even 64 possible numbers—is known as the *key space*. In the world of cryptography, key spaces are defined by the number of bits. So, a 64-bit key has a key space of 2 to the power of 64, or 18,446,744,073,709,551,616.

Keys must remain secret. Although a 7-digit combination lock can provide great security, it will do you little good if everyone knows the combination is your phone number.

Note

Data Encryption Standard (DES) uses a 64-bit key, with every 8th bit being a parity bit. 3DES (also called Triple DES), which uses three different keys and has a key strength of 168 bits, was the last official version of DES. All versions of DES have been retired.

The final consideration in the choice of a cryptosystem is the value of the data. Highly valued data requires more protection than data that has little value. Therefore, more valuable information needs stronger algorithms, larger keys, and more frequent key exchange to protect against attacks.

Cryptographic systems might make use of a *nonce*, which is a number generated as randomly as possible and used once. These *pseudorandom* numbers are different each time one is generated. An *initialization vector* (*IV*) is an example of a nonce. An IV can be added to a key and used to force creation of unique ciphertext even when encrypting the same message with the same cipher and the same key.

Modern cryptographic systems use two types of algorithms for encrypting and decrypting data:

- **Symmetric algorithms**: Use the same key to encrypt and decrypt data
- **Asymmetric algorithms**: Use different keys: one for encryption and the other for decryption

Table 4.6 highlights some of the key advantages and disadvantages of symmetric and asymmetric algorithms.

TABLE 4.6 **Symmetric and Asymmetric Algorithms**

Encryption Type	Advantages	Disadvantages
Symmetric	Faster than asymmetric	Key distribution Provides only confidentiality
Asymmetric	Easy key exchange can provide confidentiality, authentication, and nonrepudiation	Slower than symmetric Requires larger keys

ExamAlert

Make sure you know the differences between symmetric and asymmetric encryption for the CISSP exam.

Cipher Types and Methods

Symmetric encryption methods include block and stream ciphers. *Block ciphers* operate on blocks or fixed-size chunks of data. The Caesar cipher mentioned earlier in this chapter is an example of a block cipher. Most modern encryption algorithms implement some type of block cipher, and 64-bit blocks are a commonly used size. Block ciphers are widely used in software products. During the encryption and decryption process, the message is divided into blocks of bits. These blocks are then put through Boolean mathematical functions, resulting in the following:

- **Confusion**: Occurs from substitution-type operations that create a complicated relationship between the plaintext and the key so that an attacker can't alter the ciphertext to determine the key.

- **Diffusion**: Occurs from transposition-type operations that shift pieces of the plaintext multiple times. The result is that changes are spread throughout the ciphertext.

A *substitution box* (*s-box*) performs a series of substitutions, transpositions, and exclusive-or (XOR) operations to obscure the relationship between the plaintext and the ciphertext. When properly implemented, s-boxes are designed to defeat cryptanalysis. An s-box takes a number of input bits (*m*) and transforms them into some number of output bits (*n*). S-boxes are implemented as a type of lookup table and used with symmetric encryption systems such as DES.

A *stream cipher* encrypts a stream of data 1 bit at a time. To accomplish this, a one-time pad is created from the encryption engine. This one-time pad is a key stream, and it is XORed with the plaintext data stream (1 bit at a time) to create ciphertext. Stream ciphers differ from each other in the engine they use to create the one-time pad; the engine receives the symmetric key as input to cause the creation of a unique key stream. The XOR operation is a Boolean math function that says when two bits are combined, if either one of them is a value of one, a one will result, and if both of the bits are the same, a zero will result. Table 4.7 provides a list of commonly used Boolean operators.

TABLE 4.7 **Boolean Operators**

Inputs	AND	OR	NAND	NOR	XOR
0 0	0	0	1	1	0
0 1	0	1	1	0	1
1 0	0	1	1	0	1
1 1	1	1	0	0	0

Stream ciphers operate at a higher speed than block ciphers and, in theory, are well suited for hardware implementation.

Symmetric Encryption

In *symmetric encryption*, a single shared secret key is used for both encryption and the decryption, as shown in Figure 4.14. The key is referred to as a *dual-use key* because it is used to lock and unlock data. Symmetric encryption is the oldest form of encryption; scytale and Caesar's cipher are examples of it (see Chapter 5, "Communications and Network Security"). Symmetric encryption provides confidentiality by keeping individuals who do not have the key from knowing the true contents of the message.

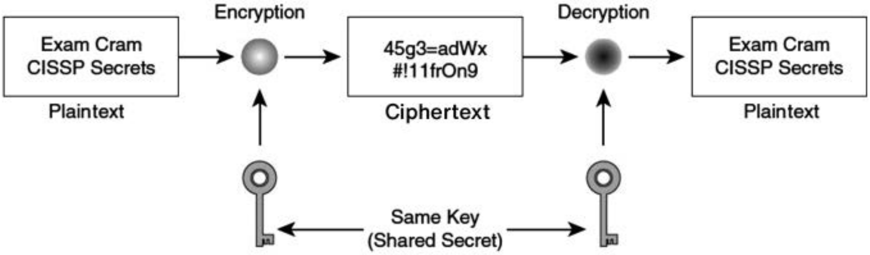


FIGURE 4.14 **Symmetric Encryption**

The simple diagram in Figure 4.14 shows the symmetric encryption process. Plaintext is encrypted with the single shared key, resulting in ciphertext; the ciphertext is then transmitted to the message's recipient, who reverses the process to decrypt the message. Symmetric encryption and decryption are fast, and symmetric encryption is very hard to break if a large key is used. However, it has three significant disadvantages:

- Distribution of the symmetric key
- Key management
- Confidentiality only

Distribution of the symmetric key is the most serious deficiency with symmetric encryption. For symmetric encryption to be effective, there must be a secure method to transfer keys. In our modern world, there needs to be some type of out-of-band transmission. Just think about it: If Bob wants to send Alice a secret message but is afraid that Eavesdropper Eve can monitor their communication, how can he send the message? If the key is sent in plaintext, Eve can intercept it. Bob could deliver the key in person, mail it, or even send a courier. All these methods are highly impractical in our world of e-commerce and electronic communication.

In addition to the problem of key exchange, there is also a key management problem. If, for example, you had 10 people who all needed to communicate with each other in complete confidentiality, you would require *45 keys* for them. The following formula is used to calculate the number of keys needed in symmetric encryption:

$$N(N - 1)/2$$

In this example, the calculation is as follows:

$$10(10 - 1)/2 = 45 \text{ keys}$$

Table 4.8 shows how the number of keys climbs as the number of users increases.

TABLE 4.8 **Symmetric Encryption Users and Keys**

Number of Users	Number of Keys
5	10
10	45
100	4,950
1,000	499,500

The third and final problem with symmetric encryption is that it provides for confidentiality only. The ultimate goal of cryptography is to supply confidentiality, integrity, authenticity, and nonrepudiation.

Some examples of symmetric algorithms include the following:

- **Data Encryption Standard (DES)**: DES was once the most commonly used symmetric algorithm. It has been officially retired by NIST. Even the latest version of DES, 3DES, was retired in 2018 and was replaced by the new FIP 197 standard AES.
- **Blowfish**: Blowfish is a general-purpose symmetric algorithm intended as a replacement for DES. Blowfish has a variable block size and a key size of 32 bits to 448 bits.
- **Twofish**: Twofish is a block cipher that operates on 128-bit blocks of data and is capable of using cryptographic keys up to 256 bits in length.
- **International Data Encryption Algorithm (IDEA)**: IDEA is a block cipher that uses a 128-bit key to encrypt 64-bit blocks of plaintext. It is patented but free for noncommercial use, and it is used by PGP.
- **Rijndael**: This is a block cipher adopted as the Advanced Encryption Standard (AES) by the U.S. government to replace DES. Although Rijndael supports multiple block sizes, AES has a fixed block size of 128 bits. There are three approved key lengths—128, 192, and 256—with block sizes of 10, 12, and 14.
- **Rivest Cipher 4 (RC4)**: RC4 is a stream-based cipher. Stream ciphers treat the data as a stream of bits.
- **Rivest Cipher 5 (RC5)**: RC5 is a fast block cipher. It is different from other symmetric algorithms in that it supports a variable block size, a variable key size, and a variable number of rounds. Allowable choices for

the block size are 32, 64, and 128 bits. The number of rounds can range from 0 to 255, and the key can range up to 2,040 bits.

- **Secure and Fast Encryption Routine (SAFER)**: SAFER is a block-based cipher that processes data in blocks of 64 and 128 bits.
- **MARS**: MARS is a candidate for AES that was developed by IBM. It is a block cipher that has a 128-bit block size and a key length between 128 and 448 bits.
- **Carlisle Adams/Stafford Tavares (CAST)**: CAST is a 128- or 256-bit block cipher that was a candidate for AES.
- **Camellia**: Camellia is a symmetric key block cipher with a block size of 128 bits and key sizes of 128, 192, and 256 bits. Developed by Mitsubishi Electric and NTT of Japan, Camellia is comparable to AES.
- **Skipjack**: Skipjack, promoted by the NSA, uses an 80-bit key, supports the same four modes of operation as DES, and operates on 64-bit blocks of text. Skipjack faced public opposition because it was developed so that the government could maintain information enabling legal authorities (with a search warrant or approval of the court) to reconstruct a Skipjack access key and decrypt private communications between affected parties.

ExamAlert

Be sure to take your time to review the various encryption types, block sizes, and key lengths; you can expect to see these items on the CISSP exam. You will be expected to know some of the algorithms that are discussed in detail in the following section. Others may simply be used as distractors on the exam.

To provide authentication from cryptography, you must turn to asymmetric encryption. However, before we discuss asymmetric encryption, the sections that follow complete the discussion of DES and a couple other popular symmetric encryption methods.

Data Encryption Standard (DES)

DES grew out of an early 1970s project originally developed by IBM. IBM and NIST modified IBM's original encryption standard, known as Lucifer, to use a 56-bit key. This revised standard was endorsed by the NSA, named DES, and published in 1977. It was released as an American National Standards Institute (ANSI) standard in 1981.

DES uses a 64-bit block to process 64 bits of plaintext at a time and outputs 64-bit blocks of ciphertext. As mentioned earlier, DES uses a 64-bit key (with every 8th bit being ignored) and has the following modes of operation:

- Electronic Codebook (ECB) mode
- Cipher Block Chaining (CBC) mode
- Cipher Feedback (CFB) mode
- Output Feedback (OFB) mode
- Counter (CTR) mode

ExamAlert

These modes of operation can be applied to any symmetric key block cipher, such as DES, 3DES, or AES. You need to know them for the CISSP exam.

The written ANSI standard reports the DES key to be 64 bits, but 8 bits are actually used for parity to ensure the integrity of the remaining 56 bits. Therefore, in terms of encryption strength, the key is really only 56 bits long. Each 64-bit plaintext block is separated into two 32-bit blocks and then processed by this 56-bit key. The processing submits the plaintext to 16 rounds of transpositions and substitutions.

ExamAlert

Keep in mind that while DES operates on 64-bit blocks, the key has an effective length of only 56 bits.

Electronic Codebook (ECB) Mode

ECB is the native encryption mode of DES. As with all other modes, if the last block is not full, padding is added to make the plaintext a full block. Although ECB produces the highest throughput, it is also the easiest form of DES encryption to break. If used with large amounts of data, it can be easily attacked because identical plaintext, when encrypted with the same key, will always produce the same ciphertext. ECB mode is appropriate only when used on small amounts of data. Figure 4.15 illustrates ECB.

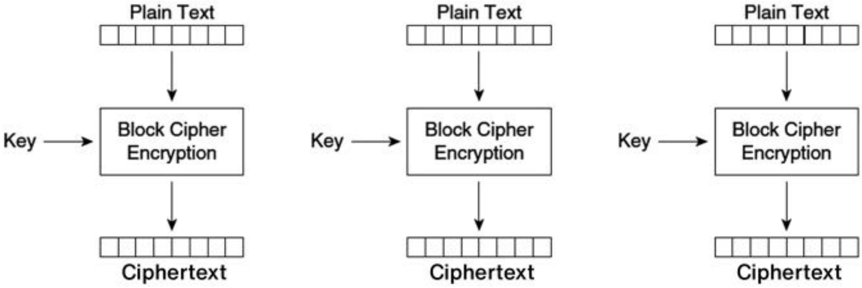


FIGURE 4.15 **DES ECB Encryption**

Tip

When using ECB, a given block of plaintext encrypted with a given key will always give the same ciphertext. ECB is the weakest form of DES.

Cipher Block Chaining (CBC) Mode

The CBC mode of DES, which is widely used, is similar to ECB. CBC processes 64-bit blocks of data but inserts some of the ciphertext created from each block into the next block. In this process, called *chaining*, each block is dependent on the previous block, creating a chain; chaining is accomplished by using the XOR operation.

The CBC mode of DES makes the ciphertext more secure and less susceptible to cracking. CBC mode is subject to a slight risk of propagating transmission errors upon reception. Any error experienced will be propagated into the decryption of the subsequent block of receipt. This can make it impossible to decrypt that block and the following blocks as well.

Cipher Feedback (CFB) Mode

CFB is implemented using a small block size (of 1 bit to 1 byte) so that streaming data can be encrypted without waiting for 64 bits to accrue. The resulting effect is that CFB behaves as a stream cipher. It is similar to CBC in that previously generated ciphertext is added to subsequent blocks. And, as with CBC, errors and corruption during transmission can propagate through the decryption process on the receiving side.

Output Feedback (OFB) Mode

Like CFB mode, OFB mode emulates a stream cipher. Unlike CFB mode, however, OFB mode feeds the plaintext of the data stream back into the next block to be encrypted. Therefore, transmission errors do not propagate throughout the decryption process. An initialization vector is used to create the seed value for the first encrypted block. DES XORs the plaintext with a seed value to be applied with subsequent data.

There is a derivative mode of OFB known as counter mode. *Counter mode*, as described later in this chapter, implements DES as a stream cipher and produces a ciphertext that does not repeat for long periods. Figure 4.16 illustrates DES OFB encryption.

Tip

Although DES remained secure for many years, in 1998 the Electronic Frontier Foundation (EFF) was able to crack DES by brute force in about 23 hours. When DES was officially retired, it was recommended that Triple DES (3DES) be used to ensure security. Triple DES has since been replaced by AES.

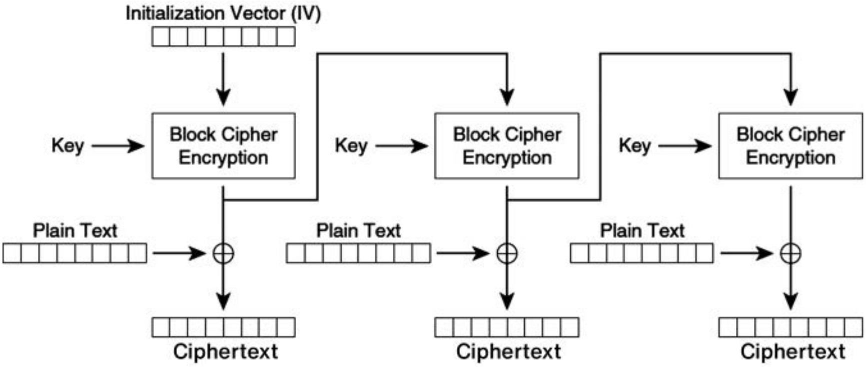


FIGURE 4.16 DES OFB Encryption

Counter (CTR) Mode

Like CFB and OFB modes, counter mode also implements a block cipher into a stream cipher and adds a counter to the process. The counter is a function that produces a sequence that will not repeat for a long time. The counter value gets combined with an initialization vector to produce the input into the symmetric key block cipher. This value is then encrypted through the block cipher using the symmetric key. Counter mode is designed for operation on a multiprocessor machine where blocks can be encrypted in parallel, as shown in Figure 4.17.

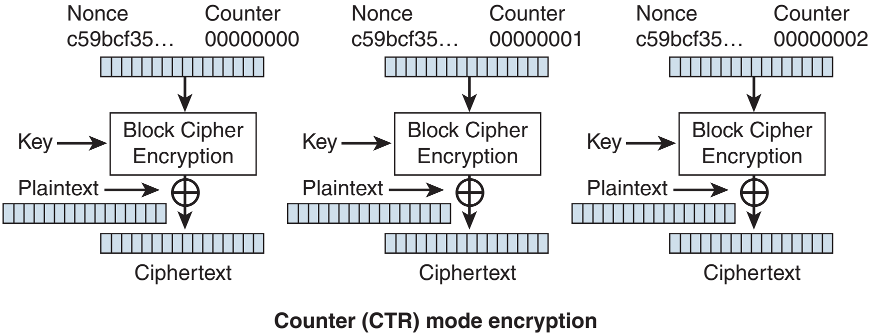


FIGURE 4.17 **Counter Mode Encryption**

Triple DES (3DES)

Before we get to the details of 3DES, let's look at why 3DES was even invented. DES was adopted with a five-year certification, which means it needed to be recertified every five years. While DES initially passed its recertifications without any problems, NIST saw that DES was beginning to outlive its usefulness and began looking for candidates to replace it. DES had become the victim of increased computing power. As Moore's law predicts, the number of transistors per square inch doubles every 18 to 24 months, and so does processing power. As a result, an encryption standard that originally required years to break through brute force was becoming dramatically easier to attack. The final demise of DES came in 1998, when the EFF was able to crack DES by brute force in about 23 hours. The actual attack used distributed systems involving more than 100,000 computers. Although DES had been resistant to cracking for many years, the EFF project demonstrated the need for stronger algorithms.

Although AES was to be the long-term replacement, the government had not chosen a cipher to put behind it. A temporary solution was needed to fill the gap before AES could be deployed. Some thought that Double DES might be used. After all, Double DES could have a 112-bit key! However, cryptanalysis proved that Double DES was no more secure than DES; it required the same work factor to crack as DES. Double DES is also susceptible to meet in the middle https://www.hypr.com/meet-in-the-middle-mitm-attack/.

It turned out that 3DES provided a geometric increase in performance. Therefore, to extend the usefulness of the DES encryption standard, 3DES was used as a stopgap solution. 3DES can make use of two or three keys to encrypt data, depending on how it is implemented; therefore, it has an effective key length of either 112 bits or 168 bits. 3DES performs 48 rounds of transpositions and substitutions. Although it is much more secure, it is approximately three times as slow as 56-bit DES. 3DES can be implemented in several ways:

- **DES EEE2**: DES EEE2 uses two keys. The first key is reused during the third round of encryption. The encryption process is performed three times (encrypt, encrypt, encrypt).
- **DES EDE2**: DES EDE2 uses two keys. Again, the first key is reused during the third round of encryption. Unlike DES EEE2, DES EDE2 encrypts, decrypts, and then encrypts.
- **DES EEE3**: DES EEE3 uses three keys and performs the encryption process three times, each time encrypting. Sometimes, you might see the specifics of these ciphers mathematically summarized. For example, when discussing DES-EEE3 using $E(K,P)$, where E refers to the encryption of plaintext P with key K, the process is summarized as $E(K3,E(K2,E(K1,P)))$.
- **DES EDE3**: DES EDE3 uses three keys but operates by encrypting, decrypting, and then encrypting the data. Figure 4.18 illustrates EDE3.

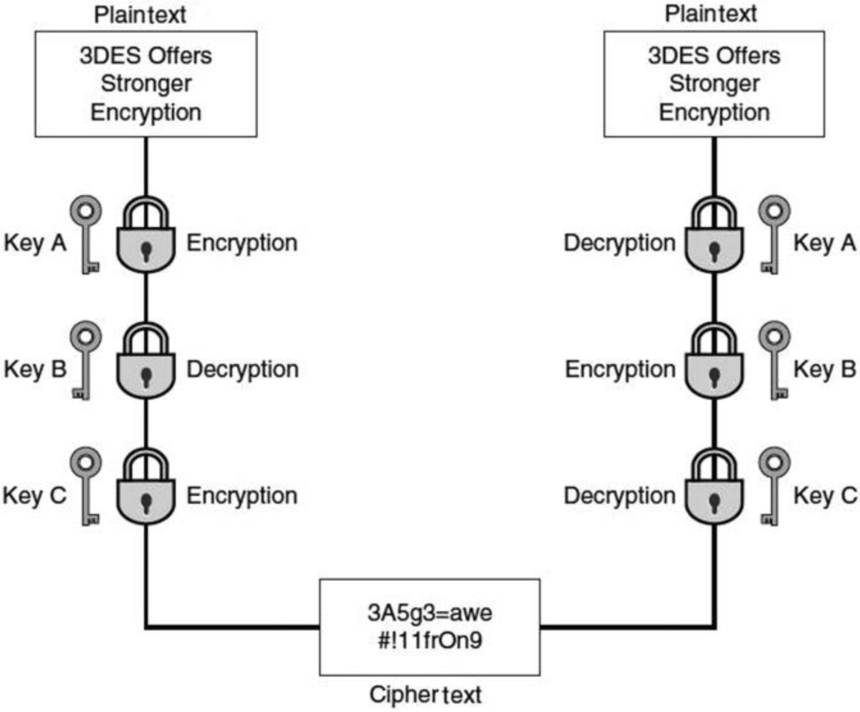


FIGURE 4.18 3DES EDE3

Advanced Encryption Standard (AES)

In 2002, NIST decided on the replacement for DES, to be known as AES. Several algorithms were examined, and *Rijndael* (which sounds like "rain doll") was chosen. Its name derives from the names of its two developers: Vincent Rijmen and Joan Daemen. Rijndael is considered a fast, simple, robust encryption mechanism.

AES is likely the most important symmetric encryption standard today. It is widely used and commonly found in wireless access points and other products. In addition, Rijndael is known to stand up well to various types of attacks. The Rijndael algorithm uses three layers of transformations to encrypt/decrypt blocks of message text:

- Linear mix transform
- Nonlinear transform
- Key addition transform

It also uses parallel series of rounds of four steps each:

1. **Byte sub**: Each byte is replaced by an s-box substitution.
2. **Shift row**: Bytes are arranged in a rectangular matrix and shifted.
3. **Mix column**: Matrix multiplication is performed based on the arranged rectangle.
4. **Add round key**: Each byte of the state is combined with the round key.

On the last round, the fourth step is bypassed and the first is repeated.

Rijndael is an iterated block cipher, and as developed, it supports variable key and block lengths of 128, 192, or 256 bits:

- If both the key size and block size are 128 bits, there are 10 rounds.
- If both the key size and block size are 192 bits, there are 12 rounds.
- If both the key size and block size are 256 bits, there are 14 rounds.

As specified in the standard for AES, Rijndael is now fixed at a block size of 128, but it can still deploy multiple key lengths.

International Data Encryption Algorithm (IDEA)

IDEA is a 64-bit block cipher that uses a 128-bit key. Although it has been patented by a Swiss company, it is freely available for noncommercial use. It is considered a secure encryption standard, and there have been no known attacks against it. It operates in four distinct modes, much like DES. At one time, it was thought that IDEA would replace DES, but patent fees prevented that from happening.

Rivest Cipher Algorithms

Rivest cipher is a general term for a family of ciphers designed by Ron Rivest, including RC2, RC4, RC5, and RC6. Ron Rivest is one of the creators of RSA. RC1 was never released, and RC3 was broken by cryptanalysis before its release.

RC2 is an early algorithm in the series. It features a variable-key-size, 64-bit block cipher that can be used as a drop-in substitute for DES.

RC4 is a fast stream cipher that is faster than block mode ciphers, and it was widely used. It was especially suitable for low-power devices. The 40-bit version is used in Wired Equivalent Privacy (WEP). Although only 40-bit keys (together with a 24-bit IV, creating 64-bit WEP) were specified by the 802.11 standard, many vendors tried to strengthen the encryption through a de facto deployment of a 104-bit key (with the 24-bit IV, making 128-bit WEP).

RC5 is a block-based cipher in which the number of rounds can range from 0 to 255, and the key can range from 0 bits to 2,048 bits. RC6 is similar; it uses a variable key size and key rounds. RC6 added two features (integer multiplication and four 4-bit working registers) not found in RC5.

Asymmetric Encryption

Asymmetric encryption is unlike symmetric encryption in that it uses two unique keys, as shown in Figure 4.19. What one key encrypts the other key must decrypt. One of the greatest benefits of asymmetric encryption is that it overcomes one of the big barriers of symmetric encryption: key distribution.

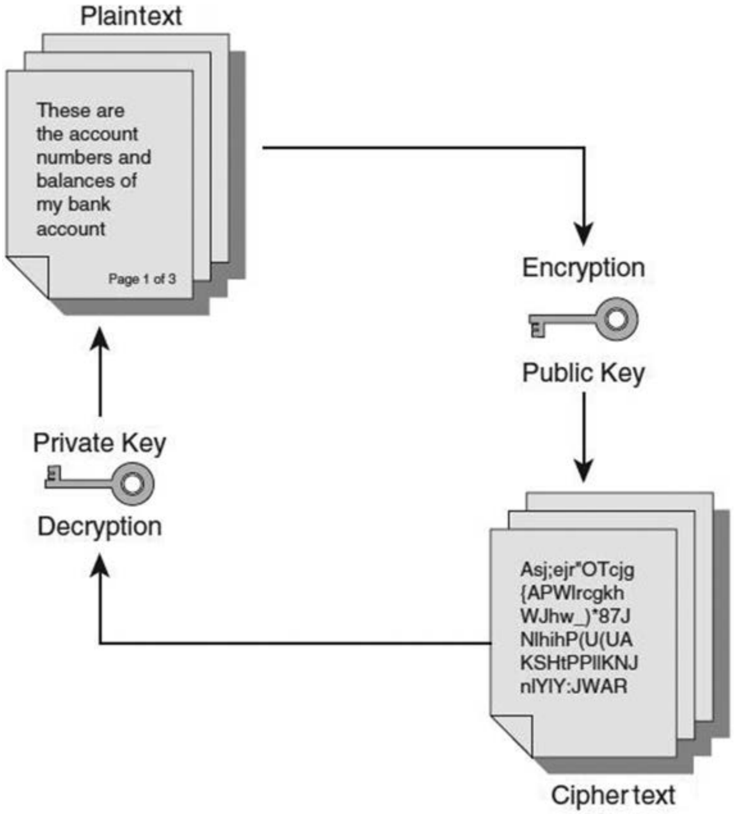


FIGURE 4.19 **Asymmetric Encryption**

Here's how asymmetric encryption functions: Imagine that you want to send a client a message. You use your client's public key to encrypt the message. When your client receives the message, he uses his private key to decrypt it. The important concepts here are that if the message is encrypted with the public key, only the matching private key will decrypt it. The private key, by definition, is generally kept secret, whereas the public key can be given to anyone. If this is properly designed, it should not be possible for someone to easily deduce a key pair's private key from the public key.

Cryptographic systems can also make use of *zero knowledge proof*. This concept allows you to prove your knowledge without revealing the fact to a third party. For example, if someone encrypts data with the private key, that data can be decrypted with the public key. This would permit a perfect check of authenticity. Asymmetric encryption provided the mechanism for accomplishing this concept. It is possible for the holder of a private key to prove she holds that key without ever disclosing the contents to anyone. Dr. W. Diffie and

Dr. M. E. Hellman (discussed shortly) used this concept to permit the creation of a trusted session key while communicating across an untrusted communication path. And—presto!—key distribution was solved.

Public key cryptography is made possible by the use of one-way functions. A one-way function, known as a *trapdoor*, is a mathematical calculation that is easy to compute in one direction but nearly impossible to compute in the other. Depending on the type of asymmetric encryption used, this calculation involves one of the following:

- Manipulating discrete logarithms
- Factoring large composite numbers into their original prime factors

As an example of a trapdoor function, consider an implementation that uses factoring. If you are given two large prime numbers such as 387 and 283, it is easy to multiply them together and get 109,521. However, if you are given only the product 109,521, it will take a while to find the factors.

As you can see, anyone who knows the trapdoor can easily perform the function in both directions, but anyone lacking the trapdoor can perform the function in only one direction. Trapdoor functions are used in the forward direction when someone is using the public key function; the forward direction is used for encryption, verification of digital signatures, and receipt of symmetric keys. Trapdoor functions are used in the inverse direction when someone is using the private key function; the inverse direction is used for decryption, generation of digital signatures, and transmission of symmetric keys.

When public key encryption is properly implemented, anyone with a private key can generate its public pair, but no one with a public key can easily derive its private pair. We have Diffie and Hellman to thank for helping develop public key encryption; they released the first key-exchange protocol in 1976.

Diffie-Hellman

Diffie-Hellman was the first public key-exchange algorithm. It was developed only for key exchange and not for data encryption or digital signatures. The Diffie-Hellman protocol allows two users to exchange a secret key over an insecure medium without any prior secrets.

Although in-depth knowledge of Diffie-Hellman's operation is not necessary for the CISSP exam, its operation is classic and worth review for anyone interested in the working of cryptographic systems. Diffie-Hellman has two system parameters: p and g. Both parameters are public and can be used by all the system's users. Parameter p is a prime number, and parameter g, which is usually called a *generator*, is an integer less than p that has the following property: For every number n between 1 and $p - 1$ inclusive, there is a power k of g such that $g^k = n \bmod p$. For example, when given the following public parameters:

p = Prime number

g = Generator

these values are used to generate the function $y = g^x \bmod p$. With this function, Alice and Bob can securely exchange a previously unshared secret (symmetric) key as follows:

Alice can use a private value *a*, which only she holds, to calculate

$$y^a = g^a \bmod p$$

Bob can use a private value b, which only he holds, to calculate

$$y^b = g^b \bmod p$$

Alice can now send y^a (as Alice's nonce, or A-nonce) to Bob, and Bob can send y^b (as Bob's nonce, or B-nonce) to Alice. Again, Alice can again use her private value A on the B-nonce. Her result will be $(y^b)^a$, or

$$g^{ba} \bmod p$$

Similarly, with his private value, *b*, Bob can calculate $(y^a)^b$ from the received A-nonce:

$$g^{ab} \bmod p$$

But guess what: Mathematically, $g^{ba} \bmod p$ and $g^{ab} \bmod p$ are equivalent. So, in fact, Bob and Alice have just, securely, exchanged a new secret key.

Diffie-Hellman is vulnerable to man-in-the-middle attacks because the key exchange does not authenticate the participants. To prove authenticity, digital signatures and digital certificates—by accepting someone's public key in advance, sometimes within a PKI—should be used. Diffie-Hellman is used in conjunction with several authentication methods, including the Internet Key Exchange (IKE) component of IPsec.

The following are some important facts you should know about Diffie-Hellman:

- It was the first asymmetric algorithm.
- It provides key-exchange services.

- It is considered a key agreement protocol.
- It operates by means of discrete logarithms.

RSA

RSA was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT. The cipher's name is based on their initials. Although RSA is much slower than symmetric encryption cryptosystems, it offers symmetric key exchange and is considered very secure. RSA is based on factoring prime numbers, but to be secure, it has to use prime numbers whose product is much larger than 129 digits. Decimal numbers less than 130 digits have been factored using a number field sieve algorithm. You do not need to know the inner workings of RSA public and private key generation for the CISSP exam, but the information in this section will be useful for you as a security professional.

Typically, the plaintext is broken into equal-length blocks, each with fewer than *n* digits, and each block is encrypted and decrypted. Cryptanalysts or anyone attempting to crack RSA would be left with the difficult challenge of factoring a large integer into its two factors. Cracking the key would require an extraordinary amount of computer processing power and time. RSA supports a key size up to 2,048 bits.

The RSA algorithm has become the de facto standard for industrial-strength encryption, especially since the patent expired in 2000. It has been built into many protocols, firmware, and software products, such as Microsoft Edge, Google Chrome, and Mozilla Firefox.

Note

LUC is an alternative to RSA, although it is not widely used. It was invented in 1991 and uses Lucas functions.

Note

XTR is a public key cryptosystem developed by Arjen Lenstra and Eric Verheul that is also based on finite fields and discrete logs, and it is seen as a generic superset function for all discrete log functions.

El Gamal

El Gamal is an extension of the Diffie-Hellman key exchange. It can be used for digital signatures, key exchange, and encryption. El Gamal consists of three discrete components: a key generator, an encryption algorithm, and a decryption algorithm. It was released in 1985, and its security rests in part on the difficulty of solving the discrete logarithm problem.

Elliptical Curve Cryptosystem (ECC)

ECC is considered more secure than previous asymmetric algorithms because elliptic curve systems are harder to crack than those based on discrete log problems. Elliptic curves are usually defined over finite fields such as real and rational numbers and implemented analogously to the discrete logarithm problem. An elliptic curve is defined by the following equation:

$$y^2 = x^3 + ax + b$$

along with a single point O, the point at infinity.

The space of the elliptic curve has the following properties:

- Addition is the counterpart of modular multiplication.
- Multiplication is the counterpart of modular exponentiation.

Thus, given two points, P and R, on an elliptic curve where $P = KR$, finding K is known as the *elliptic curve discrete logarithm problem*. ECC is fast. According to RFC 4492, a 163-bit key used in ECC has similar cryptographic strength to a 1,024-bit key used in the RSA algorithm. It can therefore be implemented in smaller, less-powerful devices such as smartphones, tablets, smart cards, and other handheld devices.

Merkle-Hellman Knapsack

Merkle-Hellman Knapsack (Knapsack) is an asymmetric algorithm based on fixed weights. Although this system was popular for a while, it was broken in 1982.

Review of Symmetric and Asymmetric Cryptographic Systems

To help ensure your success on the CISSP exam, Table 4.9 compares symmetric and asymmetric cryptographic systems.

TABLE 4.9 **Symmetric and Asymmetric Systems Attributes and Features**

Symmetric	Asymmetric
Confidentiality	Confidentiality, integrity, authentication, and nonrepudiation
One single shared key	Two keys: public and private
Requires out-of-band exchange	Useful for in-band exchange
Not scalable, too many keys needed	Scalable, works for e-commerce
Small key size and fast	Larger key size required and slower to process
Useful for bulk encryption	Digital signatures, digital envelopes, digital certificates, and small amounts of data

ExamAlert

Before attempting the CISSP exam, it is prudent that you know which categories each of the asymmetric algorithms discussed fit into. Take some time to review the differences:

- **Functions by using a discrete logarithm in a finite field:** Diffie-Hellman; El Gamal
- **Functions by using the product of large prime numbers**: RSA
- **Functions by means of fixed weights**: Merkle-Hellman Knapsack
- **Functions by means of elliptic curve**: Elliptic curve cryptosystem

Hybrid Encryption

Up to this point in the chapter, we have discussed symmetric and asymmetric ciphers individually, and as noted in Table 4.9, each has advantages and disadvantages. Although symmetric encryption is fast, key distribution is a problem. Asymmetric encryption offers easy key distribution but is not suited for large amounts of data. Hybrid encryption uses the advantages of each approach and combines them into a truly powerful system: The public key cryptosystem is used as a key encapsulation scheme, and the private key cryptosystem is used as a data encapsulation scheme.

Hybrid encryption system works as follows. If Michael wants to send a message to his editor, Betsy, the following would occur (see Figure 4.20):

1. Michael generates a random private key for the data encapsulation scheme. We can call this the *session key*.
2. Michael encrypts the message with the data encapsulation scheme using the session key that was generated in step 1.

3. Michael encrypts the session key using Betsy's public key.
4. Michael sends both the encrypted message and the encrypted key to Betsy.
5. Betsy uses her private key to decrypt the session key and then uses the session key to decrypt the message.

Nearly all modern cryptosystems are built to work this way because they provide the speed of secret key cryptosystems and the "key-exchange-ability" of public key cryptosystems. Hybrid cryptographic systems include IPsec, PGP, SSH, SET, SSL, WPA2-Enterprise, and TLS. (These systems are discussed in detail later in this chapter.)

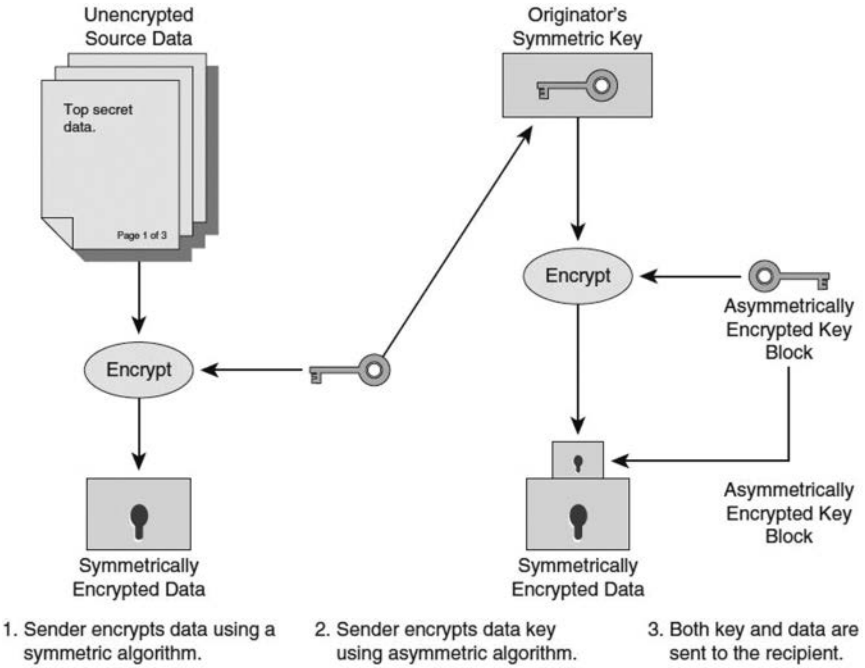


FIGURE 4.20 **Hybrid Encryption**

Public Key Infrastructure and Key Management

Dealing with brick-and-mortar businesses gives us plenty of opportunity to develop trust with a vendor. We can see the store, talk to the employees, and get a good look at how the vendor does business. Internet transactions are far less transparent. We can't see who we are dealing with, don't know what type of operation they really run, and might not be sure we can trust them. *Public key infrastructure* (*PKI*) was made to address these concerns and bring trust, integrity, and security to electronic transactions.

PKI is a framework that consists of hardware, software, and policies that exist to manage, create, store, and distribute keys and digital certificates. The components of this framework include the following:

- The certificate authority (CA)
- The registration authority (RA)
- The certificate revocation list (CRL)
- Digital certificates
- A certificate distribution system

Certificate Authorities

A good analogy for a CA is the Department of Motor Vehicles (DMV), a state entity that is responsible for issuing driver's licenses, which are the known standard for physical identification. If you cash a check, go to a night club, or catch a plane, your driver's license is one document that is widely accepted at these locations to prove your identity. CAs are like DMVs: They vouch for your identity in a digital world. VeriSign, Thawte, and Entrust are some of the companies that perform public CA services.

A CA doesn't have to be an external third party; many companies decide to tackle these responsibilities by themselves. Regardless of who performs them, the following steps are necessary:

1. The CA verifies the request for certificate with the help of the RA.
2. The individual's identification is validated.
3. A certificate is created by the CA, which certifies that the person matches the public key that is being offered.

Registration Authorities

The RA is like a messenger: It's positioned between the client and the CA. Although the RA cannot generate a certificate, it can accept requests, verify a person's identity, and pass along the information to the CA for certificate generation.

RAs play a key role when certificate services expand to cover large geographic areas. One central CA can delegate its responsibilities to regional RAs around the world.

ExamAlert

Expect to see CISSP exam questions that deal with the workings of PKI. It's important to understand that the RA cannot issue certificates.

Certificate Revocation Lists

Just like driver's licenses, digital certificates might not always remain valid. (I had a great aunt who drove with an expired license for years. In her case, she was afraid that at 95 years old, she might not pass the eye exam.) In corporate life, certificates might become invalid because someone leaves the company, information might change, or a private key might become compromised. For these reasons, the CRL must be maintained.

The CRL is maintained by the CA, which signs the list to maintain its accuracy. Whenever problems with digital certificates are reported, those certificates are considered invalid, and the CA has the serial number added to the CRL. Anyone requesting a digital certificate can check the CRL to verify the certificate's integrity. The replacement for CRLs is the Online Certificate Status Protocol (OCSP); it has a client/server design that scales better than a CRL. When a user requests access to a server, OCSP sends a request for certificate status information. The server sends back a response of current, expired, or unknown. Regardless of which method is used, problems with certificates are nothing new; to read about the problem Dell had in 2015, see www.infoworld.com/article/3008422/security/what-you-need-to-know-about-dells-root-certificate-security-debacle.html.

Digital Certificates

Digital certificates are at the heart of a PKI system. A digital certificate serves two roles:

- It ensures the integrity of the public key and makes sure the key remains unchanged and in a valid state.
- It validates that the public key is tied to the stated owner and that all associated information is true and correct.

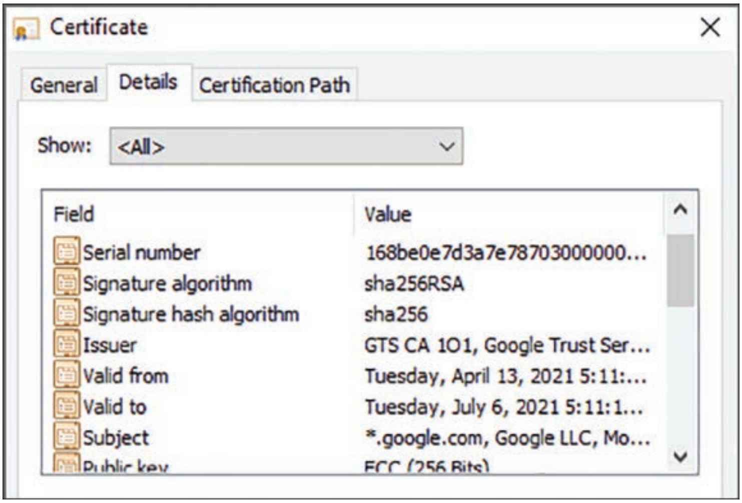
The information needed to accomplish these goals is added to the digital certificate. Digital certificates are formatted to the X.509 standard, whose most current version is Version 3. One of the key developments in Version 3 is the addition of extensions. Version 3 includes the flexibility to support other topologies. It can operate as a web of trust, much like PGP. An X.509 certificate includes the following elements, and examples showing some of these elements are provided in Figure 4.21:

- Version
- Serial number
- Algorithm ID
- Issuer
- Validity
  - Not before (a specified date)
  - Not after (a specified date)
- Subject
- Subject public key information
  - Public key algorithm
  - Subject public key
- Issuer—unique identifier (optional)
- Subject—unique identifier (optional)
- Extensions (optional)

Digital certificates play a vital role in the chain of trust. Public key encryption works well when you are dealing with people you know because it's easy for you to send each other a public key. But what about communicating with people you don't know?

Note

Digital certificates are used to prove your identity when performing electronic transactions.



Show: <All>

Field	Value
Serial number	168be0e7d3a7e78703000000...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	GTS CA 1O1, Google Trust Ser...
Valid from	Tuesday, April 13, 2021 5:11:...
Valid to	Tuesday, July 6, 2021 5:11:1...
Subject	*.google.com, Google LLC, Mo...
Public key	ECC (256 Bits)

FIGURE 4.21 **X.509 Certificate**

Although you might want to use an external certificate authority, doing so is not mandatory. You could decide to have your own organization act as a certificate authority. Regardless of whether you have a third party handle certificate duties or you perform them yourself, digital certificates typically contain the following critical pieces of information:

- Identification information including username, serial number, and validity dates of the certificates
- The public key of the certificate holder
- The digital signature of the signature authority, which piece is critical because it certifies and validates the integrity of the entire package

The Client's Role in PKI

It might seem that up to this point, all the work has fallen on the shoulders of the CAs; this is not entirely true, however. Clients are responsible for requesting digital certificates and for maintaining the security of their private keys. Loss or compromise of a private key would be devastating; it would mean that communications were no longer secure. If you are dealing with credit card numbers or other pieces of user identity, this type of loss of security could lead to identity theft.

Protecting a private key is an important issue because it's easier for an attacker to target the key than to try to crack the certificate service. Organizations should concern themselves with seven key management issues:

- Generation
- Distribution
- Installation
- Storage
- Key change
- Key control
- Key disposal

Key recovery and control is an important issue that must be addressed. One basic recovery and control method is the M of N control method of access. This method is designed to ensure that no one person can have total control; it is closely related to dual control. Therefore, if N number of administrators have the ability to perform a process, M number of those administrators must authenticate for access to occur. *M of N control* should require physical presence for access. Here is an example: Suppose that a typical M of N control method requires that four people have access to the archive server and at least two of them must be present to accomplish access. In this situation, M = 2 and N = 4. This would ensure that no one person could compromise the security system or gain access.

Note

Many organizations use hardware security modules (HSMs) to securely store and securely retrieve these escrowed keys. HSM systems protect keys and can detect and prevent tampering by destroying the key material if unauthorized access is detected.

Integrity and Authentication

One of the things cryptography offers to its users is the capability to verify integrity and authentication. Integrity assures a recipient that the information remained unchanged and is in its true original form. Authentication provides the capability to ensure that messages are sent from who you believed sent them and that messages are received by the intended recipient. To help ensure your success on the CISSP exam, review the integrity methods listed in Table 4.10.

TABLE 4.10 **Integrity Verification**

Method	Description
Parity	Simple error detection code for networking
Hashing	Integrity
Digital signature	Integrity, authentication, and nonrepudiation
Hashed MAC	Integrity and data origin authentication
CBC MAC	Integrity and data origin authentication
Checksum	Redundancy check, weak integrity

Hashing and Message Digests

Hashing algorithms function by taking a variable amount of data and compressing it into a fixed-length value referred to as a *hash value*. Hashing provides a fingerprint or message digest of the data. Strong hashing algorithms are hard to break and will not produce the same hash value for two or more messages. Hashing can be used to meet the goals of integrity and/or nonrepudiation, depending on how the algorithms are used. Hashes can help verify that information has remained unchanged. Figure 4.22 provides an overview of the hashing process.

Hashing algorithms are not intended to be reversed to reproduce the data. The purpose of the message digest is to verify the integrity of data and messages. In a well-designed message digest, if there is even a slight change in an input string, the output hash value should change drastically. This is known as the *avalanche effect*. For example, the version of SolarWinds that is vulnerable to Sunburst has the MD5 hash value b91ce2fa41029f6955bff20079468448. This means if you were to match this hash to the version of SolarWinds, the version you are running would leave you exposed to the Sunburst malware. Another value would indicate that the version you have may not be vulnerable.

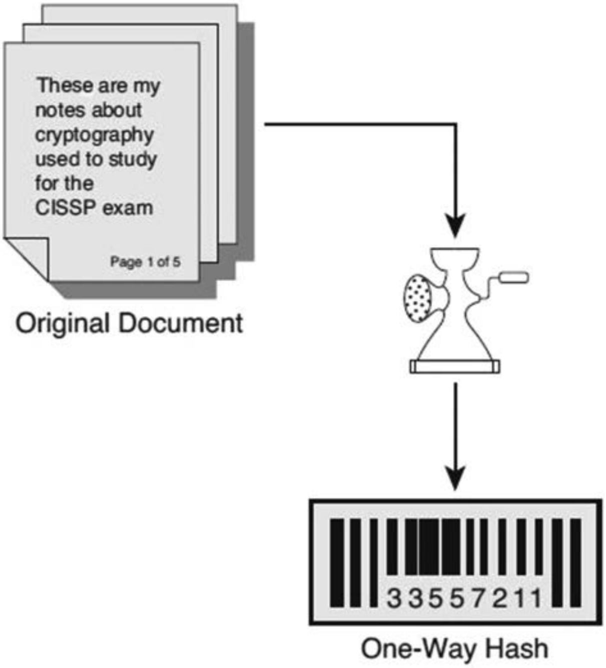

These are my notes about cryptography used to study for the CISSP exam
Page 1 of 5
Original Document
33557211
One-Way Hash

FIGURE 4.22 **Hashing**

Programs such as Tripwire, MD5sum, and Windows System File Verification rely on hashing. Some common hashing algorithms include the following:

- Message-Digest algorithm series
- Secure Hash Algorithm (SHA)
- HAVAL
- RIPEMD
- Whirlpool
- Tiger

Note

While there are many hashing algorithms, two of the most common are SHA and MD series.

The biggest problem for hashing is the possibility of collisions. Collisions result when two or more different inputs create the same output. Collisions can be reduced by moving to an algorithm that produces a larger hash.

Note

When considering hash values, remember that close does not count! If the hashes being compared differ in any way—even by just a single bit—the data being digested is not the same.

MD Series

All of the MD algorithms were developed by Ron Rivest. They have progressed through a series of versions over the years as technology has advanced. The original was MD2, which was optimized for 8-bit computers and is somewhat outdated. It has also fallen out of favor because MD2 has been found to suffer from collisions. MD4 was the next algorithm to be developed. The message is processed in 512-bit blocks plus a 64-bit binary representation of the original length of the message, which is concatenated to the message. As with MD2, MD4 was found to be vulnerable to possible attacks. This is why MD5 was developed; it could be considered MD4 with additional safety mechanisms. MD5 processes a variable-size input and produces a fixed 128-bit output. As with MD4, it processes the data in blocks of 512 bits.

Tip

Collisions occur when two different messages are passed through a hash and produce the same message digest value. This is undesirable because it can mask the fact that someone might have changed the contents of a file or message. MD5 and SHA-0 have been shown to be vulnerable to forced collisions.

SHA-1/2

SHA-1 is a version of *Secure Hashing Algorithm* (*SHA*) that is similar to MD5. It is considered the successor to MD5 and produces a 160-bit message digest. SHA-1 processes messages in 512-bit blocks and adds padding, if needed, to get the data to add up to the right number of bits. Out of the 160 bits, SHA-1 has only 111-bit effectiveness. SHA-1 is one of a series of SHA algorithms including SHA-0, SHA-1, and SHA-2. SHA-0 is no longer considered secure, and SHA-1 is no longer recommended. SHA-2 is actually a family of functions and is a safe replacement for SHA-1. The SHA-2 family includes SHA-224, SHA-256, SHA-386, and SHA-512.

SHA-3

SHA-3 is the newest family of hashing algorithms and was designed to replace SHA-1 and SHA-2.

HAVAL

HAVAL is another one-way hashing algorithm that is similar to MD5. Unlike MD5, HAVAL is not tied to a fixed message-digest value. HAVAL-3-128 makes three passes and produces a 128-bit fingerprint; HAVAL-4-256 makes four passes and produces a 256-bit fingerprint.

Message Authentication Code (MAC)

A MAC is like a poor man's version of a digital signature and is somewhat similar to a digital signature except that it uses symmetric encryption. MACs are created and verified with the same secret (symmetric) key. Four types of MACs exist: unconditionally secure, hash function based, stream cipher based, and block cipher based.

HMAC

Hashed-Based Message Authentication Code (*HMAC*) was designed to be immune to multi-collision attacks. This immunity was added by including a shared secret key. In simple terms, HMAC functions by using a hashing algorithm such as MD5 or SHA-1 and altering the initial state of the file to be processed by adding a password. Even if someone can intercept and modify the data, it's of little use if that person does not possess the secret key. There is no easy way for the person to re-create the hashed value without it. For HMAC to be used successfully, the recipient would have to have acquired a copy of the symmetric key through some secure out-of-band mechanism.

CBC-MAC

A cipher block chaining MAC uses the CBC mode of a symmetric algorithm such as DES to create a MAC. CBC-MAC differs from HMAC in that CBC-MAC uses one algorithm, whereas HMAC uses two (a hashing algorithm and a symmetric block cipher). The last block of the message is used as the MAC authentication portion and is appended to the actual message.

CMAC

Cipher-Based Message Authentication (CMAC) addresses some of the security deficiencies of CBC-MAC. CMAC has more complex logic and uses mathematical functions that make use of AES for increased security. You can use CMAC to verify both the integrity and authenticity of a message.

Digital Signatures

Digital signatures, which are based on public key cryptography, are used to verify the authenticity and integrity of a message. Digital signatures are created by passing a message's contents through a hashing algorithm and encrypting it with a sender's private key. When the message is received, the recipient decrypts the encrypted hash and then recalculates the received message's hash. These values should match to ensure the validity of the message and to prove that the message was sent by the party believed to have sent it (because only that party has access to the private key). Let's break this process out step by step with an example to help detail the operation:

1. Bill produces a message digest by passing a message through a hashing algorithm.
2. The message digest is encrypted using Bill's private key.
3. The message is forwarded to the recipient, Alice.
4. Alice creates a message digest from the message with the same hashing algorithm that Bill used. Alice then decrypts Bill's signature digest by using his public key.
5. Finally, Alice compares the two message digests—the one originally created by Bill and the other that she created. If the two values match, Alice can rest assured that the message is unaltered.

Figure 4.23 illustrates this process and demonstrates how the hashing function ensures integrity and the signing of the hash value provides authentication and nonrepudiation.

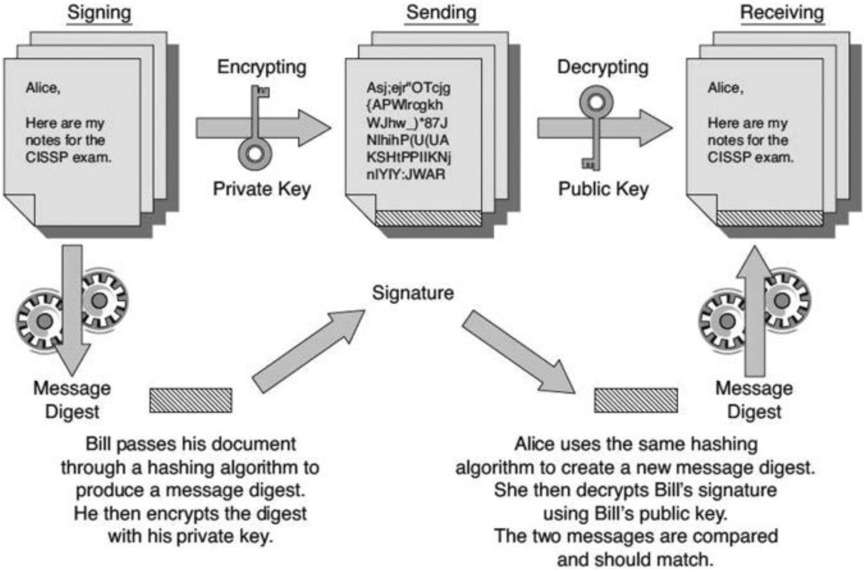

Signing
Sending
Receiving
Alice,
Here are my notes for the CISSP exam.
Encrypting
Private Key
Asj;ejr*OTcjg {APWlrogkh WJhw_)*87J NlhihP(U(UA KSHtPPIIKNj nIYIY:JWAR
Decrypting
Public Key
Alice,
Here are my notes for the CISSP exam.
Signature
Message Digest
Message Digest
Bill passes his document through a hashing algorithm to produce a message digest. He then encrypts the digest with his private key.
Alice uses the same hashing algorithm to create a new message digest. She then decrypts Bill's signature using Bill's public key. The two messages are compared and should match.

FIGURE 4.23 Digital Signatures

DSA

Things are much easier when we have standards, and that is what Digital Signature Algorithm (DSA) was designed for. The DSA standards were proposed by NIST in 1991 to standardize Digital Signature Standards (DSS). DSA involves key generation, signature generation, and signature verification. It uses SHA-1 in conjunction with public key encryption to create a 160-bit hash. Signing speeds are equivalent to RSA signing, but signature verification is much slower. The DSA digital signature is a pair of large numbers represented as binary digits.

Cryptographic System Review

As a recap and to help ensure your success on the CISSP exam, review the well-known cryptographic systems in Table 4.11.

TABLE 4.11 **Algorithms and Their Functions**

Category	Algorithm
Symmetric	DES, 3DES, Blowfish, Twofish, IDEA, CAST, SAFER, Skipjack, and RC (series)
Asymmetric	RSA, ECC, Diffie-Hellman, Knapsack, LUC, and El Gamal
Hashing	MD (series), SHA (series), HAVAL, Tiger, Whirlpool, and RIPEMD
Digital signature	DSA

Cryptographic Attacks

Attacks on cryptographic systems are not new. Whenever someone has information to hide, there is usually someone who would like to reveal it. *Cryptanalysis* is the analysis of cryptography, as can be seen in the parts of the word: *crypt* = secret or hidden and *analysis* = loosen or dissolve. The ultimate goal of cryptanalysis is to determine the key value, and these types of activities occur every day at organizations like the NSA and at locations where hackers and security specialists are working. Depending on which key is cracked, an attacker could gain access to confidential information or could pretend to be someone else and attempt some sort of masquerade attack.

Because cryptography can be a powerful tool and the ability to break many algorithms is limited, the Coordinating Committee for Multilateral Export Controls (CoCom) was established to deal with the control of cryptographic systems. CoCom disbanded in 1994 and was replaced by the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. The Wassenaar Arrangement had wide support, bringing together more than 30 countries to control the export of cryptography.

Methods the U.S. Government Can Use to Defeat Encryption

The U.S. government must deal with many individuals and organizations that use encryption, such as terrorists and organized crime. Documents made public by whistleblower Edward Snowden have disclosed some of the cryptanalysis techniques that the NSA uses to break cryptographic systems. These techniques include exerting control over setting of international encryption standards, using supercomputers to brute-force algorithms, and collaboration with technology companies and Internet service providers to insert backdoors or trapdoors into commercial encryption software. The NSA has even been rumored to work with major antivirus companies to develop software that will not be detected by antivirus software. You can read more about these techniques at www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html.

One issue to consider before launching a cryptographic attack is what is known about the algorithm. Is it public or private? Auguste Kerckhoffs is credited with creating, in the nineteenth century, *Kerckhoffs's principle*, which states that a cryptographic system should not require secrecy; everything should be public except the key. An example of this debate can be seen in the development and crack of *Content Scrambling System* (*CSS*). This method of encryption was developed by the DVD Copy Control Association (DVD CCA). Because the algorithm was proprietary, it was not made public. CSS was designed to allow only authorized DVD players to decode scrambled content stored on the original DVD discs. This was until Jon Lech Johansen and others got together and cracked CSS and posted a utility called DeCSS to the Internet in 1999. So, whereas some argue that algorithms should be secret, others continue to believe that open standards and systems allow for more robust, secure systems.

With a review of some of the basics completed, let's now review some common attack techniques that might target a cryptographic system:

- **Known plaintext attack**: This type of attack requires the attacker to have the plaintext and ciphertext of one or more messages. Encrypted file archives such as zip are prone to this type of attack.
- **Ciphertext-only attack**: This type of attack requires the attacker to obtain several encrypted messages that have been encrypted using the same encryption algorithm. The attacker does not have the associated plaintext but attempts to crack the code by looking for patterns and using statistical analysis.
- **Chosen ciphertext**: If an attacker can decrypt portions of a ciphertext message, the decrypted portion can then be used to discover the key.
- **Chosen plaintext**: An attacker can have plaintext messages encrypted and then can analyze the ciphertext output.
- **Differential cryptanalysis**: This type of attack, which is generally used to target block ciphers, works by looking for the difference between related bits of plaintext that are encrypted, and the difference between their resultant ciphertexts.
- **Linear cryptanalysis**: Along with differential cryptanalysis, this is one of the two most widely used attacks on block ciphers. Linear cryptanalysis uses functions to identify the highest probability that a specific key was used during the encryption process. The key pairs are then studied to derive information about the key used to create them.

- **Birthday attack**: This type of attack gets its name from the birthday paradox, which states that within a group of people, the chances that two or more will share birthdays is unexpectedly high. This same logic is applied to calculate collisions in hash functions. A message digest can be susceptible to birthday attacks if the output of the hash function is not large enough to avoid collisions.
- **Key clustering**: This vulnerability can occur when two different keys produce the same ciphertext from the same message. This can sometimes be the result of having a small key space or might be a characteristic of some cryptosystems. Key clustering is a real problem as it means that two or more different keys could also decrypt the secure content. A strong cryptosystem should have a low frequency of key clustering occurrences. If it doesn't, this is yet another way that a cryptosystem might be targeted for attack.
- **Replay attack**: This method of attack occurs when the attacker can intercept cryptographic keys and reuse them later to either encrypt or decrypt messages.
- **Man-in-the middle attack**: This type of attack is carried out when attackers place themselves in the communications path between two users. From this position, the attackers may be able to intercept and modify communications.
- **Side-channel attack**: This type of attack is based on side-channel information, such as timing, sound, or electromagnetic leaks.

> ExamAlert
>
> When comparing cryptographic algorithms, it is important to keep in mind that the larger the work factor, the stronger the cryptosystem. Cryptographers develop systems with high work factors to withstand attacks, not to be foolproof. All systems can be cracked with enough time and determination. Sometimes attackers simply look for vulnerabilities that have yet to be publicly discovered. These are known as *zero-day vulnerabilities*.

- **Rubber hose attack**: When all else fails, this method might be used to extract a key value or other information. This type of attack might include threats, violence, extortion, or blackmail because humans are a bigger weakness than cryptosystems.

When attempting a cryptographic attack, the work factor must be considered. The *work factor* can be measured as the time and effort needed to perform a brute-force attack against an encryption system. The following are some examples of successful attacks against cryptosystems that have occurred in the recent past:

- **BEAST**: BEAST exploits weakness in the CBC usage in TLS 1.0. Violated same-origin constraints.
- **CRIME and BREACH**: CRIME targeted compression over TLS, and BREACH was an instance of CRIME used over HTTP.
- **Cryptolocker**: This ransomware had the ability to encrypt local and network files using RSA encryption.
- **DROWN**: DROWN exploited the cipher of the then-still-supported SSL 2.
- **FREAK**: FREAK exploited the cipher to carry out a man-in-the-middle attack and force the usage of weak keys.
- **Meltdown**: Meltdown targeted hardware and Intel x86 processors to attempt a race condition and side-channel attack. It would allow a rogue process to read all memory, regardless of authorization.
- **POODLE**: This cipher attack affected all block ciphers in SSL 3.0 and led to a migration from SSL to TLS. A POODLE variant also affected TLS 1.0 to 1.2.
- **Spectre**: Spectre targeted hardware and microprocessors with branch prediction. It is an example of a side-channel and timing attack.

Site and Facility Security Controls

Keep in mind that good security requires multiple layers of defense, both logical and physical. Site and facility security controls are vital parts of strong facility security. They are covered in detail in Chapter 6, “Identity and Access Management,” and Chapter 8, “Security Operations,” but this section presents some common controls that are used for physical security:

- **Physical access controls**: These controls include gates, fences, doors, guards, and locks. Fencing can be made from a range of components, such as steel, wood, brick, or concrete, but must be the correct design for the level of protection needed. Guards can also be used in multiple roles to monitor, greet, sign in, and escort visitors. Locks come in many types, sizes, and shapes; they are both some of the oldest theft-deterrent mechanisms and the most commonly used deterrents.

- **Controls in server rooms and data centers**: Controls in these areas can include time restrictions on access, controls that specify who can enter specific areas, and where servers and data centers are placed. A well-placed data center should have limited accessibility and typically no more than two doors. A first-floor interior room is a good location for a data center. The ceilings should extend all the way up past the drop ceiling, access to the room should be controlled, and doors should be solid core with hinges to the inside.
- **Evidence storage controls**: If you maintain a security operations center or deal with computer forensics, you might need to keep an evidence storage area. Typically, such storage is located in a secure area, with a locked secure cabinet or safe and a log to record activity related to chain of custody.
- **Restricted access and work area security**: The goal of a security design should be to make it as hard as possible for unauthorized personnel to gain access to sensitive resources.
- **HVAC and environmental controls**: Heat can be damaging to computer equipment, and most data centers are kept around 70°F. Security management should know who is in charge of the HVAC system, and the system must be controlled to protect the organization and its occupants from chemical and biological threats. Electrical power, like HVAC, is a resource that most of us take for granted. Even areas that have dependable power can be subject to outages, line noise, or electromagnetic interference (EMI). Businesses must be prepared to deal with all these factors. Uninterruptible power supplies (UPSs) are typically used to help with these issues.
- **Fire prevention, detection, and suppression controls**: A big part of prevention is making sure people are trained and know how to prevent potential fire hazards. Policy must define how employees will be trained to deal with fires. Companies should make sure they have appropriate and functioning fire-detection equipment so that employees can be alerted to possible danger. Just being alerted to a fire is not enough. Employees need to know what to do and how to handle different types of fires.

Note

Physical security is covered in greater depth in Chapters 6 and 8.

Exam Prep Questions

1. Which of the following best describes a superscalar processor?

❍ **A.** A superscalar processor can execute only one instruction at a time.

❍ **B.** A superscalar processor has two large caches that are used as input and output buffers.

❍ **C.** A superscalar processor can execute multiple instructions at the same time.

❍ **D.** A superscalar processor has two large caches that are used as output buffers.

2. Which of the following are developed by programmers and used to allow the bypassing of normal processes during development but are left in the software when it ships to the customer?

❍ **A.** Backdoors

❍ **B.** Traps

❍ **C.** Buffer overflows

❍ **D.** Covert channels

3. Which of the following attacks occurs when an attacker can intercept session keys and reuse them at a later date?

❍ **A.** Known plaintext attack

❍ **B.** Ciphertext-only attack

❍ **C.** Man-in-the-middle attack

❍ **D.** Replay attack

4. Which of the following is a disadvantage of symmetric encryption?

❍ **A.** Key size

❍ **B.** Speed

❍ **C.** Key management

❍ **D.** Key strength

5. Which of the following is *not* an example of a symmetric algorithm?

❍ **A.** DES

❍ **B.** RC5

❍ **C.** AES

❍ **D.** RSA

6. Which of the following was the first model based on confidentiality that was developed?

   ○ **A.** Bell-LaPadula

   ○ **B.** Biba

   ○ **C.** Clark-Wilson

   ○ **D.** Take-Grant

7. Which of the following models is integrity based and was developed for commercial applications?

   ○ **A.** Information flow model

   ○ **B.** Clark-Wilson model

   ○ **C.** Bell-LaPadula model

   ○ **D.** Brewer and Nash model

8. Which of the following does the Biba model address?

   ○ **A.** Focuses on internal threats

   ○ **B.** Focuses on external threats

   ○ **C.** Addresses confidentiality

   ○ **D.** Addresses availability

9. Which model is also known as the Chinese Wall model?

   ○ **A.** Biba model

   ○ **B.** Take-Grant model

   ○ **C.** Harrison-Ruzzo-Ullman model

   ○ **D.** Brewer and Nash model

10. Which hashing algorithm produces 160-bit output?

   ○ **A.** MD2

   ○ **B.** MD4

   ○ **C.** SHA-1

   ○ **D.** El Gamal

11. What is the result of the * property in the Bell-LaPadula model?

   ○ **A.** No read up

   ○ **B.** No write up

   ○ **C.** No read down

   ○ **D.** No write down

12. What is the result of the simple integrity property of the Biba model?

○ **A.** No read up

○ **B.** No write up

○ **C.** No read down

○ **D.** No write down

13. Which of the following can be used to connect different MAC systems together?

○ **A.** Labels

○ **B.** Reference monitor

○ **C.** Controls

○ **D.** Guards

14. Which of the following security modes of operation best describes a user's valid need to know all data?

○ **A.** Dedicated

○ **B.** System high

○ **C.** Compartmented

○ **D.** Multilevel

15. Which of the following security models makes use of the TLC concept?

○ **A.** Biba model

○ **B.** Clark-Wilson model

○ **C.** Bell-LaPadula model

○ **D.** Brewer and Nash model

16. Which of the following DES modes is considered the most vulnerable to attack?

○ **A.** CBC

○ **B.** ECB

○ **C.** CFB

○ **D.** OFB

17. Which of the following is the key size DES uses?

○ **A.** 56 bits

○ **B.** 64 bits

○ **C.** 96 bits

○ **D.** 128 bits

18. Which implementation of Triple DES uses the same key for the first and third iterations?

❍ **A.** DES-EEE3

❍ **B.** HAVAL

❍ **C.** DES-EEE2

❍ **D.** DES-X

19. Which of the following algorithms is used for key distribution and not encryption or digital signatures?

❍ **A.** El Gamal

❍ **B.** HAVAL

❍ **C.** Diffie-Hellman

❍ **D.** ECC

20. You are working with the file integrity program Tripwire and have been asked to review some recent issues with a cryptographic program. What is it called when two different keys generate the same ciphertext for the same message?

❍ **A.** Hashing

❍ **B.** Collision

❍ **C.** Key clustering

❍ **D.** Output verification

Answers to Exam Prep Questions

1. **C.** A superscalar processor can execute multiple instructions at the same time. Answer A describes a scalar processor; it can execute only one instruction at a time. Answer B does not describe a superscalar processor because it does not have two large caches that are used as input and output buffers. Answer D is incorrect because a superscalar processor does not have two large caches that are used as output buffers.
2. **A.** Programmers use backdoors, also referred to as *maintenance hooks*, during development to get easy access into a piece of software. Answer B is incorrect because a trap is a message used by Simple Network Management Protocol (SNMP) to report a serious condition to a management station. Answer C is incorrect because a buffer overflow occurs due to poor programming. Answer D is incorrect because a covert channel is a means of moving information in a manner that was not intended.
3. **D.** A reply attack occurs when the attacker can intercept session keys and reuse them at a later date. Answer A is incorrect because a known plaintext attack requires the attacker to have the plaintext and ciphertext of one or more messages. Answer B is incorrect because a ciphertext-only attack requires the attacker to obtain several messages encrypted using the same encryption algorithm. Answer C is incorrect because a man-in-the-middle attack is carried out when attackers place themselves in the communications path between two users.
4. **C.** Key management is a primary disadvantage of symmetric encryption. Answers A, B, and D are incorrect because encryption speed, key size, and key strength are not disadvantages of symmetric encryption.
5. **D.** RSA is an asymmetric algorithm. Answers A, B, and C are incorrect because DES, RC5, and AES are examples of symmetric algorithms.
6. **A.** Bell-LaPadula was the first model developed that is based on confidentiality. Answers B, C, and D are incorrect: The Biba and Clark-Wilson models both deal with integrity, whereas the Take-Grant model is based on four basic operations.
7. **B.** The Clark-Wilson model was developed for commercial activities. This model dictates that the separation of duties must be enforced, subjects must access data through an application, and auditing is required. Answers A, C, and D are incorrect. The information flow model addresses the flow of information and can be used to protect integrity or confidentiality. The Bell-LaPadula model is an integrity model, and the Brewer and Nash model was developed to prevent conflicts of interest.
8. **B.** The Biba model assumes that internal threats are being protected by good coding practices and, therefore, focuses on external threats. Answers A, C, and D are incorrect. The Biba model addresses only integrity and not availability or confidentiality.
9. **D.** The Brewer and Nash model is also known as the Chinese Wall model and was specifically developed to prevent conflicts of interest. Answers A, B, and C are incorrect because they do not fit the description. The Biba model is integrity-based, the Take-Grant model is based on four modes, and the Harrison-Ruzzo-Ullman model defines how access rights can be changed, created, or deleted.

10. **C.** SHA-1 produces a 160-bit message digest. Answers A, B, and D are incorrect because MD2 and MD4 both create a 128-bit message digest, and El Gamal is not a hashing algorithm.

11. **D.** The * property enforces “no write down” and is used to prevent someone with high clearance from writing data to a lower classification. Answers A, B, and C do not properly describe the Bell-LaPadula model’s star property.

12. **C.** The purpose of the simple integrity property of the Biba model is to prevent someone from reading an object of lower integrity. This helps protect the integrity of sensitive information.

13. **D.** A guard is used to connect various MAC systems together and allow for communication between these systems. Answer A is incorrect because labels are associated with MAC systems but are not used to connect them together. Answer B is incorrect because the reference monitor is associated with the TCB. Answer C is incorrect because the term *controls* here is simply a distractor.

14. **A.** Of the four modes listed, only the dedicated mode supports a valid need to know for all information on the system. Therefore, answers B, C, and D are incorrect.

15. **B.** The Clark-Wilson model was designed to support integrity and is focused on TLC, which stands for tampered, logged, and consistent. Answers A, C, and D are incorrect; the Biba, Bell-LaPadula, and Brewer and Nash models are not associated with TLC.

16. **B.** Electronic Code Book mode is susceptible to known plaintext attacks because the same plaintext always produces the same ciphertext. Answers A, C, and D are incorrect. Because CBC, CFB, and OFB all use some form of feedback, which helps randomize the encrypted data, they do not suffer from this deficiency and are considered more secure.

17. **A.** Each 64-bit plaintext block is separated into two 32-bit blocks and then processed by the 56-bit key. The total key size is 64 bits, but 8 bits are used for parity, thereby making 64, 96, and 128 bits incorrect.

18. **C.** DES-EEE2 performs the first and third encryption passes using the same key. Answers A, B, and D are incorrect: DES-EEE3 uses three different keys for encryption; HAVAL is used for hashing, and DES does not use it; and DES-X is a variant of DES with only a 56-bit key size, and it was designed for DES, not 3DES.

19. **C.** Diffie-Hellman is used for key distribution but not encryption or digital signatures. Answer A is incorrect because El Gamal is used for digital signatures, data encryption, and key exchange. Answer B is incorrect because HAVAL is used for hashing. Answer D is incorrect because ECC is used for digital signatures, data encryption, and key exchange.

20. **C.** Key clustering is said to occur when two different keys produce the same ciphertext for the same message. A good algorithm, using different keys on the same plaintext, should generate a different ciphertext. Answers A, B, and D are incorrect: Hashing is used for integrity verification; a collision occurs when two different messages are hashed and output the same message digest; and output verification is simply a distractor.

Need to Know More?

Microcode: https://www.techopedia.com/definition/8332/microcode

Trust and assurance: www.cs.clemson.edu/course/cpsc420/material/Assurance/Assurance%20and%20Trust.pdf

TPM binding and sealing: https://docs.microsoft.com/it-it/windows/iot-core/secure-your-device/tpm

Covert-timing-channel attacks: http://crypto.stanford.edu/~dabo/papers/ssl-timing.pdf

Digital rights management: https://digitalguardian.com/blog/what-digital-rights-management

HVAC and cybersecurity: https://www.propmodo.com/the-cyber-security-threats-lurking-in-your-hvac-system/

Restricted and work area security: https://info-savvy.com/cissp-restricted-and-work-area-security-bk1d3t11st6/

The Bell-LaPadula model: csrc.nist.gov/publications/secpubs/rainbow/std001.txt

ISO 17799: https://www.iso.org/standard/39612.html

Vulnerabilities in embedded devices: http://www.cse.psu.edu/~pdm12/cse597g-f15/readings/cse597g-embedded_systems.pdf

Five common vulnerabilities in industrial control systems: https://www.lanner-america.com/blog/5-common-vulnerabilities-industrial-control-systems/

Symmetric encryption: https://www.thesslstore.com/blog/symmetric-encryption-101-definition-how-it-works-when-its-used/

Ten types of vulnerabilities in web-based systems: https://www.terraats.com/2019/03/12/10-types-of-security-vulnerabilities-for-web-applications/

Site and facility security control checklist: http://www.mekabay.com/infosecmgmt/facilities_checklist.pdf

The BIBA security model: http://nathanbalon.com/projects/cis576/sBiba_Security.pdf

CHAPTER 5

Communications and Network Security

Terms you'll need to understand:

- Address Resolution Protocol (ARP)
- Domain Name System (DNS)
- Firewall
- Network Address Translation (NAT)
- IP Security (IPsec)
- Open Systems Interconnection (OSI) model
- Transmission Control Protocol/Internet Protocol (TCP/IP)
- Local area network (LAN)
- Wide area network (WAN)
- Cloud computing

Topics you'll need to master:

- Secure network design
- The differences between LAN and WAN topologies
- The OSI model and its layers
- The four layers of the TCP/IP stack
- Convergence protocols

Introduction

The CISSP exam Communication and Network Security domain addresses communications and network security. This is one of the larger domains, and you can expect about 13% of the exam questions to be on this topic. After all, this area covers many of the core concepts a security professional is required to know. Mastery of this domain requires you to fully understand networking, TCP/IP, LAN, WAN, telecommunications equipment, wireless networking, and related security controls. Being adept in network security requires that you understand the techniques used for preventing network-based attacks.

If you have spent some time working in network security, you might need only a quick review of the material in this chapter. If your work has led you to concentrate in other areas, you will want to spend adequate time on this chapter, reviewing the material to make sure you have the essential knowledge needed for the exam.

Secure Network Design

To be fully prepared for the CISSP exam, you need to understand the data communication process and how it relates to network security. Also, knowledge of remote access, use of firewalls, network equipment, and network protocols is required. Securing a network requires defense in depth—building layers of control. For example, before ransomware can be executed by an end host, it must be passed by a firewall, screened by an email server, verified as nonmalicious by antivirus software, and scanned by an intrusion detection system (IDS). The idea is that the failure of any one device should not lead to compromise of the system, and layers of defense can help protect assets.

Before you can begin to build layers of defense, you need to understand the basic building blocks of a network and network models and standards such as the Open Systems Interconnection (OSI) and TCP/IP network standards.

Network Models and Standards

Network models and standards play an important role in the telecommunications industry. These standards and protocols set up rules of operation. Protocols describe how requests, messages, and other signals are formatted and transmitted over the network. The network can only function as long as all computers are consistent in following the same set of rules for communication.

TCP/UDP and TCP/IP are two examples of network standards. These standards have helped build the Internet and the worldwide data networks we have today. The goal of any set of network standards is to provide the following:

- Interoperability
- Availability
- Flexibility
- Maintainability

Many groups have been working toward meeting this challenge, including the following organizations:

- International Organization for Standardization (ISO)
- Institute of Electrical and Electronics Engineers (IEEE)
- Internet Engineering Task Force (IETF)
- International Telecommunication Union–Telecommunications Standardization Sector (ITU-T)

The next section discusses the OSI model in detail.

OSI Model

The International Standards Organization developed the Open Systems Interconnection (OSI) model in 1984. This model features a specific hierarchy in which each layer encapsulates the output of each adjacent layer. It is described in ISO 7498. Today, the OSI model is widely used as a guide in describing the operations of a networking environment. It was once considered the universal communications standard and now serves as a teaching model for all other protocols.

The OSI model is designed so that network communication is passed down the stack, from layer to layer. Information to be transmitted is put into the application layer and ends at the physical layer. Then it is transmitted over some medium (wire, coaxial, optical, or wireless) toward the target device, and then it travels back up the stack to the application. From the bottom of the stack, the seven layers of the OSI model are the physical, data link, network, transport, session, presentation, and application layers (see Figure 5.1). People often remember this order by using one of the many acronyms that have been thought up over the years. My favorite one is “Please Do Not Throw Sausage Pizza Away”:

- Please (physical—Layer 1)
- Do (data link—Layer 2)
- Not (network—Layer 3)
- Throw (transport—Layer 4)
- Sausage (session—Layer 5)
- Pizza (presentation—Layer 6)
- Away (application—Layer 7)

To help you understand how the OSI model works, the following sections start at the bottom of the stack, Layer 1, and work up to Layer 7.

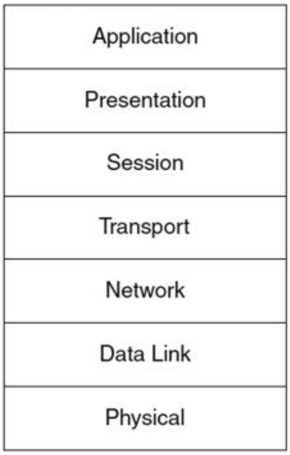


FIGURE 5.1 **OSI Model**

ExamAlert

CISSP candidates need to know the seven layers of the OSI model: physical (Layer 1), data link, network, transport, session, presentation, and application layer (Layer 7).

Physical Layer

Layer 1, the *physical layer*, accepts data that has been formatted as a frame from the data link layer and converts it to an electrical signal. Physical layer components include the following:

- Copper cabling
- Fiber cabling
- Wireless system components
- Wall jacks and connectors
- Ethernet hubs and repeaters

At Layer 1, bit-level communication takes place. The bits have no defined meaning on the wire, but the physical layer defines how long each bit lasts and how it is transmitted and received. Standards and specifications at the physical layer include the following:

- High-Speed Serial Interface (HSSI)
- V.24 and V.35
- EIA/TIA-232 and EIA/TIA-449 (where *EIA/TIA* stands for Electronic Industries Alliance/Telecommunications Industry Association)
- X.21

Data Link Layer

Layer 2, the *data link layer*, focuses on traffic within a single LAN. The data link layer is responsible for receiving data from the physical layer. The data link layer formats and organizes data. Components of this layer include the following:

- Bridges
- Switches
- Network interface cards (NICs)
- Media Access Control (MAC) addresses

The data link layer organizes data into *frames*, which are logical structures in which data can be placed. The data link layer is responsible for stripping off the header of the data frame, leaving a data packet, which passes up to the network layer. Some of the protocols found at the data link layer include the following:

- Layer 2 Forwarding (L2F)
- Layer 2 Tunneling Protocol (L2TP)
- Fiber Distributed Data Interface (FDDI)
- Integrated Services Digital Network (ISDN)
- Serial Line Internet Protocol (SLIP)
- Point-to-Point Protocol (PPP)

Network Layer

Layer 3 is the *network layer*. Whereas the bottom two layers of the OSI model are associated with hardware, the network layer is tied to software. This layer is concerned with how data moves from network A to network B, ensuring that frames from the data link layer reach the correct network. The network layer is the home of Internet Protocol (IP), which determines the best route from the source to the target network. Network layer protocols include the following:

- Internet Protocol (IPv4, IPv6, and IPsec)
- Internetwork Packet Exchange (IPX)
- Internet Control Message Protocol (ICMP)
- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGP)
- Internet Group Management Protocol (IGMP)

Transport Layer

Layer 4 is the *transport layer*. Whereas the network layer routes information to its destination, the transport layer ensures completeness by handling end-to-end error recovery and flow control and establishes a logical connection between two devices. Transport layer protocols include the following:

- **Transmission Control Protocol (TCP)**: This connection-oriented protocol provides reliable communication using handshaking, acknowledgments, error detection, and session teardown.

- **User Datagram Protocol (UDP)**: This connectionless protocol offers speed and low overhead as its primary advantages. Applications that use UDP must provide their own forms of error recovery because the protocol does not have this feature built in.

Session Layer

The purpose of Layer 5, the *session layer*, is to allow two applications on different computers to establish and coordinate a session. A *session* is simply a connection between two computers. When a data transfer is complete, the session layer is responsible for tearing down the session. Session layer protocols include the following:

- Remote Procedure Call (RPC)
- Structured Query Language (SQL)
- Secure Sockets Layer (SSL)
- Network File System (NFS)

Presentation Layer

Layer 6, the *presentation layer*, performs a job similar to that of a waiter in a restaurant: Its main purpose is to deliver and present data to the application layer. In performing its job, the data must be formatted in such a way that the application layer can understand and interpret the data. The presentation layer is skilled in translation, and its duties include encrypting data, changing or converting the character set, and handling format conversion. Some standards and protocols found at the presentation layer include the following:

- American Standard Code for Information Interchange (ASCII)
- Extended Binary Coded Decimal Interchange Code (EBCDIC)
- Joint Photographic Experts Group (JPEG)
- Musical Instrument Digital Interface (MIDI)
- Tagged Image File Format (TIFF)

ExamAlert

Where does encryption occur? The presentation layer is the natural home of encryption in the OSI model. Modern systems can implement encryption (for example, with IPv6) at other layers, such as the data link, network, or even application layer.

Note

Encapsulation is the process of adding headers to user data as it is handed from each layer to the next lower layer.

Application Layer

Recognized as the top layer of the OSI model, Layer 7, or the *application layer*, serves as the window for application services; it is the layer that applications talk to. You probably send email or surf the Web without thinking about all the underlying processes that make it possible. Layer 7 is not an application but rather the channel through which applications communicate. Examples of protocols operating at the application layer include the following:

- File Transfer Protocol (FTP)
- Line Print Daemon (LPD)
- Telnet
- Simple Mail Transfer Protocol (SMTP)
- Trivial File Transfer Protocol (TFTP)
- Hypertext Transfer Protocol (HTTP)
- Post Office Protocol Version 3 (POP3)
- Internet Message Access Protocol (IMAP)
- Simple Network Management Protocol (SNMP)
- Electronic Data Interchange (EDI)

OSI Summary

Table 5.1 summarizes each of the seven layers and the equipment and protocols that work at each layer.

TABLE 5.1 **OSI Model and Protocols**

Layer	Equipment	Protocols
Application	Application proxy firewall	FTP, DNS, HTTP, SNMP, RIP
Presentation	—	ASCII, TIFF, JPEG, GIF, MIDI, MPEG
Session	—	NetBIOS, NFS, SQL, RPC, SMB
Transport	Circuit-level proxy firewall	TCP, UDP, SPX, SSL, TLS
Network	Router	IP, ICMP, IGMP, OSPF, IPX
Data link	Switch, bridge	SLIP, PPP, L2F, L2TP, FDDI, ARP, RARP
Physical	Hub	EIA/TIA-232, HSSI, X.21

ExamAlert

For the CISSP exam, you need to know where various protocols operate in the OSI model. Make sure you can specify the placement of well-known protocols at each of the seven layers: physical, data link, network, transport, session, presentation, and application layer.

Note

In real life, not all protocols fit cleanly into the OSI layered model. Although SSL is typically shown at the transport layer, it actually provides functionality between Layer 4 (transport) and Layer 5 (session). SSL sits between these layers to provide security services to many modern Internet applications.

Encapsulation/De-encapsulation

Encapsulation is a key concept in networking. Encapsulation is the process of adding headers to the data as it is passed down the stack. Consider the following example:

1. A message is created at the application layer.
2. The message, or protocol data unit (PDU), is passed to the presentation layer, where information and a checksum, known as a *header*, are added.
3. The information is passed down to the session layer, and the process is repeated. This continues until the data reaches the data link layer.

4. At the data link layer, a header and trailer are added. Now the data is said to be a *frame*. When Ethernet is used for this process, the trailer is a cyclic redundancy check (CRC).
5. The frame is passed to the physical layer and converted to signals appropriate for the transmission medium.

The *de-encapsulation* process starts when a message reaches the recipient. The headers at each layer are stripped off as the data moves back up the stack. The only layer that physically communicates is the physical layer. Processes running at higher layers, say Layer 7, communicate logically as if they were directly connected at Layer 1, even though they are not. Figure 5.2 shows an example of this communication.

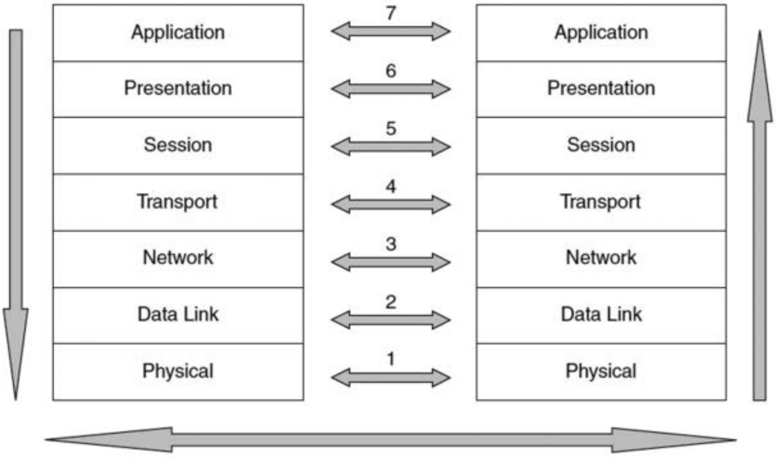


FIGURE 5.2 **OSI Communication**

Note

PDU is just one of the terms used in networking. Don't be surprised to also see such terms as *frame*, *packet*, and *datagram* to refer to the same concept.

TCP/IP

TCP/IP is the foundation of the Internet as we know it today. Its roots can be traced back to standards adopted by the U.S. government's Department of Defense (DoD) in 1982. The *TCP/IP model* is similar to the OSI model, but it consists of only four layers: the network access layer, the Internet layer, the host-to-host (transport) layer, and the application layer.

It is of critical importance to remember that the TCP/IP model was originally developed as a flexible, fault-tolerant network. Security was not a driving concern. The network was designed to specifications that could withstand a nuclear strike destroying key routing nodes. The designers of this original network never envisioned the Internet we use today. Therefore, many of the original TCP/IP protocols seem dated and insecure now. Protocols like FTP, Telnet, and Routing Information Protocol (RIP) suffer from security problems. For example, Telnet's security was designed to mask the screen display of passwords the user typed because the designers didn't want shoulder surfers stealing passwords; however, the passwords themselves are then sent in plaintext on the wire. Little concern was given to the fact that an untrusted party might have access to the wire and be able to sniff the plaintext password. FTP is also a plaintext protocol; it uses both ports TCP/20 and TCP/21 for data and control. Many of the security mechanisms used in IPv4, such as IPsec, are add-ons to the original protocol suite.

Network Access Layer

The network access layer loosely corresponds to Layers 1 and 2 of the OSI model. Some literature separates this single layer into two and refers to them as the *physical access* and *data link* layers. Whether viewed as one layer or two, this portion of the TCP/IP network model is responsible for the physical delivery of IP packets via frames.

Ethernet is the most commonly used LAN frame type. Ethernet uses carrier-sense multiple access with collision detection (CSMA/CD). Ethernet frames are addressed with MAC addresses that identify the source and destination devices. A MAC address is 6 bytes long and is intended to be unique to the NIC in which it is burned. The first 3 bytes, known as the organizationally unique identifier (OUI), are unique to the manufacturer. For example, Cisco owns OUI 00:00:0C, so any NIC with a MAC address that begins with 00:00:0C is a Cisco NIC. Cisco can assign this portion of the address until all possible values have been exhausted, at which point a new OUI is needed. Occasionally, though, vendors repeat addresses as they cycle through series.

Sometimes vendors also provide features in the NIC driver to change the MAC address to a unique locally administered address. Third-party programs are available that allow attackers to spoof MAC addresses. Network layer security standards include the following:

- **802.1AE (MACsec)**: This security standard is designed to provide confidentiality, integrity, and data origin authentication. MACsec frame formats are similar to the Ethernet frame but include security tags, message authentication codes (ICV), secure connectivity associations, and default cipher suites (such as Galois/Counter Mode or the Advanced Encryption Standard cipher with a 128-bit key).

- **802.1AR**: This standard ensures the identity of the trusted network components, using unique per-device identifiers along with cryptography to bind a specific device to a unique identifier.

Note

Address Resolution Protocol (ARP) can be discussed at either the TCP/IP model network layer or Internet layer. The ARP table and NICs are at TCP/IP Layer 1, whereas logical addresses are at Layer 2. The ARP process takes a Layer 2 logical address and resolves it to an unknown Layer 1 physical address.

Internet Layer

The Internet layer maps to OSI Layer 3. Two primary protocol groups found at this layer are routable protocols (such as IP) and routing protocols (such as OSPF and Internet Gateway Routing Protocol [IGRP]). The Internet layer also contains ICMP, the interface to ARP, and IGMP:

- ICMP is usually noted for its support of ping but can also be used for services such as IP support, error, and diagnostic protocols. ICMP can handle problems such as delivering error messages.
- IGMP is used for multicast messages.
- ARP is used to resolve known IP addresses to unknown MAC addresses.

Internet Protocol (IP)

IP is a routable protocol whose job is to make the best effort at delivery. An IPv4 header is normally 20 bytes long but can be as long as 60 bytes with options added. Currently, most organizations use IPv4. IPv6 is the planned replacement. It offers better security and increases support for IP addresses from the current 32 bits of IPv4 to 128 bits. IPv4 uses a logical address scheme for IP addresses. Whereas a MAC address is considered a physical address, an IP address is considered a logical address.

Although in-depth knowledge of the header is not needed for the CISSP exam, complete details can be found in Request for Comments (RFC) 791. Examination of the structure of IP packets might not be the most exciting part of security work, but having a basic understanding is extremely helpful in recognizing the many attacks based on manipulation of these packets. For example, in a teardrop attack, the Total Length and Fragmentation fields are modified so that fragments are incorrectly overlapped. Fragmentation and source routing are two potential security issues with IPv4.

If IP needs to transmit a datagram larger than the network access layer allows, the datagram must be divided into smaller packets. Not all network topologies are capable of handling the same datagram size; therefore, *fragmentation* is an important function of IP. And as IP packets pass through routers, the needs of the upcoming network access layer may change again. IP is responsible for reading the acceptable size for the network access layer. If the existing datagram is too large, IP performs fragmentation and divides the datagram into two or more packets. Each fragmented packet is labeled with the following bits:

- **Length**: The length specified is the total length of the fragment.
- **Offset**: This bit specifies the distance from the first byte of the original datagram.
- **More**: This bit indicates whether this fragment has more fragments following it or is the last in the series of fragments.

Loose source routing and *strict source routing* are additional options that IP supports. These options allow a pseudo-routing path to be specified between the source and the target. Although this functionality is potentially useful in certain situations, attackers can use it to set up a man-in-the-middle attack.

Note

IP addresses are required because physical addressees are tied to the physical topology used. Some LANs use Ethernet, but other LANs are connected to Asynchronous Transfer Mode (ATM) or token ring networks. Because no common format or structure exists, IP is used to bind these dissimilar networks together.

The newest version of IP is Internet Protocol Version 6 (IPv6). Although the depletion of IPv4 addresses has been a concern for many years, the fact that IPv4 address space has reached exhaustion means we have reached the tipping point of adoption of the IPv6 protocol. IPv6 brings many improvements to modern networks. One of these is that the address space moves from 32 bits to 128 bits. IPv6 does not support broadcast traffic; instead, IPv6 uses a link-local scope as an all-nodes multicast address. IPv6 can use multiple addresses, including a global address and a local-link address. A global (routable) address is used for communication beyond the local network. IPv6 relies on IPv6 routing advertisements to assign the global address. The link-local address is used for local network communication only. IPv6-enabled devices create a link-local address independently. There is no need for an IPv6 router advertisement for the creation of a local-link address.

IPv6 offers built-in support for IPsec so that greater protection exists for data during transmission, and it offers end-to-end data authentication and privacy. With the move to IPv6, Network Address Translation (NAT) is no longer needed. However, with so many IPv4 networks in place, there is a need for transition mechanisms for migrating from IPv4 to IPv6. The following are two such mechanisms:

- **6to4**: This Internet transition mechanism for migrating from IPv4 to IPv6 allows IPv6 packets to be transmitted over an IPv4 network.
- **Teredo**: This transition technology can be used for IPv6-capable hosts that are on the IPv4 Internet and that have no native connection to an IPv6 network.

When IPv6 is fully deployed, one protocol that will no longer be needed is ARP. IPv6 does not support ARP and instead uses Network Discovery Protocol (NDP). DHCP is also not required with IPv6. It can be used but has been replaced with stateless autoconfiguration. Common routing protocols to be used with IPv6 include RIPng, OSPFv3, IS-ISv2, and EIGRPv6. To date, Asia has a higher adoption rate of IPv6 than the United States.

Figure 5.3 illustrates the IPv6 header.

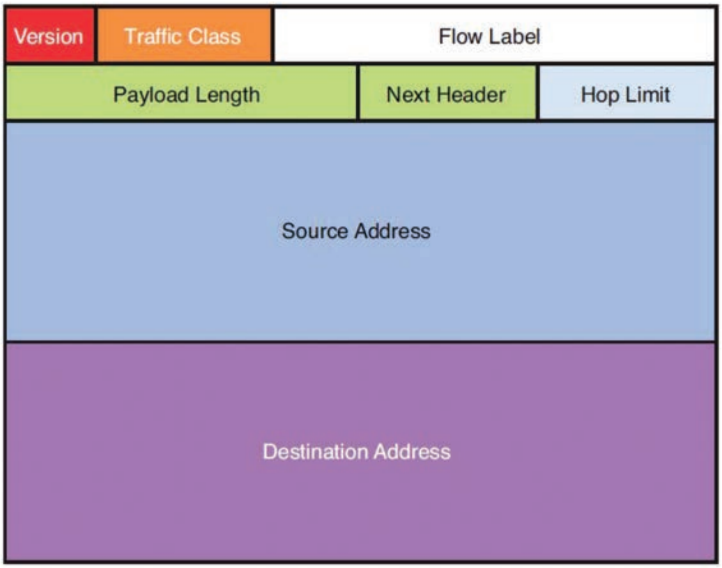


FIGURE 5.3 **IPv6 Header**

Internet Control Message Protocol (ICMP)

One of the protocols residing at the Internet layer is *ICMP*. Its purpose is to provide diagnostic feedback or to report logical errors. Because ICMP resides at the Internet layer, it is a separate protocol and is distinctly different from IP.

All ICMP messages have the same basic format. The first byte of an ICMP header indicates the type of ICMP message. The following byte contains the code for each particular type of ICMP. Table 5.2 lists the eight most common ICMP types. For a complete list of all ICMP parameters, see www.iana.org/assignments/icmp-parameters.

TABLE 5.2 **ICMP Types and Codes**

Type	Code	Function
0/8	0	Echo response/request (ping)
3	0–15	Destination unreachable
4	0	Source quench
5	0–3	Redirect
11	0–1	Time exceeded
12	0	Parameter fault
13/14	0	Timestamp request/response
17/18	0	Subnet mask request/response

One of the most common ICMP types is a ping. Although ICMP can be very helpful, it is also valued by attackers because it can be manipulated and used for a variety of attacks, including pings of death, Smurf attacks, timestamp queries, netmask queries, and redirects.

Address Resolution Protocol (ARP)

ARP is used to resolve addressing between the network access layer and the Internet layer of the TCP/IP model. ARP is a two-step resolution process performed by first sending a broadcast message requesting a target's physical address. If the device with the requested logical address hears the request, it issues a unicast ARP reply containing its MAC address to the original sender. The MAC address is then placed in the requester's ARP cache and used to address subsequent frames. *Reverse ARP* (*RARP*) is used to resolve known physical addresses to unknown IP addresses.

Attackers can manipulate ARP because it is a trusting protocol. Two well-known attacks are ARP poisoning and ARP flooding. ARP poisoning is possible because a host cannot tell the difference between a bogus reply and valid reply, and so it will accept bogus ARP responses as valid. Such attacks can be used to intercept traffic bound for a gateway or can be used to facilitate attacks against targeted hosts. ARP poisoning allows attackers to redirect traffic on a switched network. ARP attacks play a role in a variety of man-in-the middle attacks, spoofing, and session-hijacking attacks.

Caution

Remember that ARP is unauthenticated; therefore, an attacker can send unsolicited ARP replies, poison the ARP table, and spoof another host.

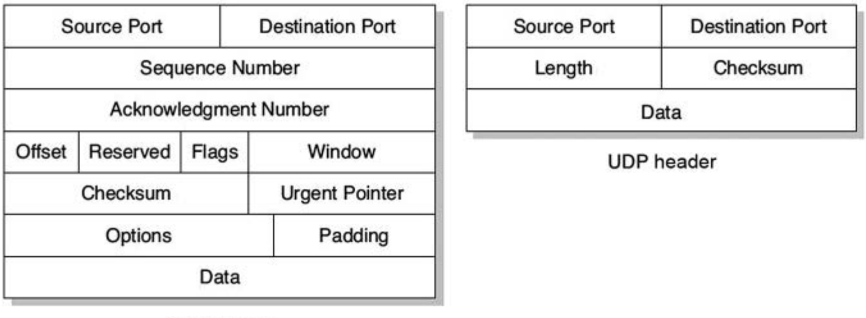
Internet Group Management Protocol (IGMP)

IGMP is a Layer 2 protocol that is responsible for managing IP multicast groups. IP multicasts can send messages or packets to a specified group of hosts or routers. This is different from a broadcast, which all users in a network receive. IGMP transmissions are sent to a group of systems.

Host-to-Host (Transport) Layer

The host-to-host layer is responsible for reliable and efficient communication between endpoints. The endpoints referred to are programs or services. This exchange can be a peer-to-peer exchange, as with an instant messaging application, or it might be a client/server interaction, such as a web browser sending a request to a web server. The host-to-host layer loosely corresponds to OSI Layer 4 but provides end-to-end delivery. The two primary protocols located at the host-to-host layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Figure 5.4 illustrates the packet headers for TCP and UDP.

Each of these protocols has pros and cons, and developers select one or the other depending on what they are trying to accomplish via the network. Generally, trivial and ad hoc exchanges across the network are done in a connectionless manner (using UDP). More persistent network relationships are largely handled with connection-oriented solutions (using TCP), especially when a substantial amount of data is being transferred.



TCP header

UDP header

FIGURE 5.4 **TCP and UDP Headers**

At the host-to-host layer, you will find the capability for error checking and retransmission. This ensures that all connection-oriented messages sent will arrive intact at the receiving end. A checksum or similar mechanism is generally used to ensure message integrity. Retransmission strategies vary; for example, in the case of TCP, data not positively acknowledged by the recipient in a timely way is retransmitted.

Transmission Control Protocol (TCP)

TCP enables two hosts to establish a connection and exchange data reliably. TCP has a nominal 20-byte packet size that contains fields to support flow control and reliable communication and to ensure that missing data is re-sent. At the heart of TCP is a 1-byte Flag field. The most common flags are summarized in Table 5.3. These flags help control the TCP communication.

TABLE 5.3 **TCP Flags**

Flag	Name	Function
URG	Urgent	Urgent data
ACK	Acknowledgment	Acknowledge data
PSH	Push	Push buffered data
RST	Reset	Reset TCP connection
SYN	Synchronize	Start session
FIN	Finish	Close session

Although there are actually eight fields (bits) in the 1 byte reserved for flags, the upper two—the Congestion Window Reduced (CWR) and Explicit Congestion Notification Echo (ECN) flags—were not defined until 2001 and are not widely used.

TCP provides reliable communication by performing formal startup and shutdown handshakes. The TCP three-step handshake occurs before any data is sent. Figure 5.5 illustrates the three-step startup and four-step shutdown.

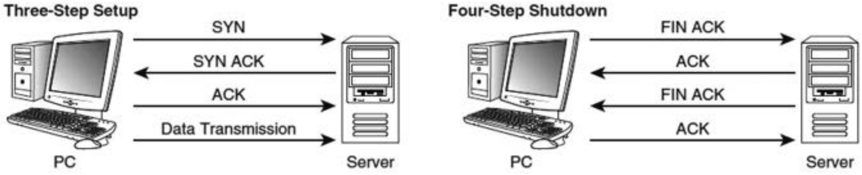


FIGURE 5.5 **TCP Operation**

The flags used to manage three-step startup are SYN and ACK, and RST and FIN are used to tear down a connection. FIN is used during a normal four-step shutdown, whereas RST is used to signal the end of an abnormal session. Between the startup and shutdown, TCP guarantees delivery of data by using sequence and acknowledgment numbers. Vulnerabilities that exist at this layer include the TCP sequence number attack that results in session hijacking and the port-based attack of SYN flooding.

User Datagram Protocol (UDP)

UDP does not perform any handshaking processes. So although this makes it considerably less reliable than TCP, it does offer the benefit of speed. The UDP header is only 8 bytes in length. There are four 2-byte fields in the header, and there are no variations on this; the length is fixed. Figure 5.6 illustrates the operation of UDP.

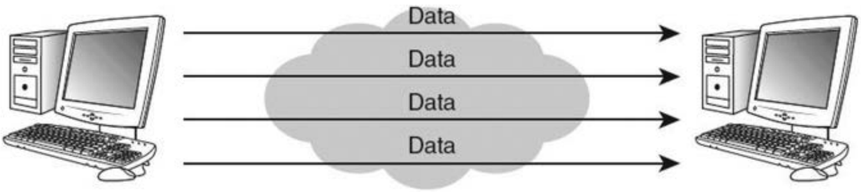


FIGURE 5.6 **UDP Operation**

UDP can be used for services such as IPTV (Internet Protocol Television), video multicast, and voice over IP (VoIP). With VoIP, UDP is primarily used for the voice connection portion of the call, and TCP is used for the setup and call control for the actual call. UDP is ideally suited for such applications that require fast delivery. UDP does not use sequence and acknowledgment numbers.

Comparing and Contrasting UDP and TCP

Table 5.4 illustrates the differences between UDP and TCP.

TABLE 5.4 **UDP and TCP Compared**

Service	UDP	TCP
Speed	✓	—
Low overhead	✓	—
Connectionless	✓	—
Reliable	—	✓
Maintains state	—	✓
Controls congestion	—	✓
Uses flow control	—	✓

Application Layer

The application layer, or process layer, sits at the top of the protocol stack and maps loosely to OSI Layers 6 and 7. This layer is responsible for application support. Applications are typically mapped not by name but by their corresponding port. Ports are placed into TCP and UDP packets so that the correct application can be passed to the required protocols. Although applications can be made to operate on nonstandard ports, the established port numbers serve as the de facto standard. There are 65,535 ports separated into three ranges, as shown in Table 5.5.

TABLE 5.5 **Ports and Ranges**

Range	Usage	Attribute
0–1023	Well known	System services
1024–49151	Registered	Software services
49152–65535	Random	Client programs

Some of the most common well-known applications and their associated ports are as follows:

- **File Transfer Protocol (FTP)**: FTP is a TCP service that operates on ports 20 and 21 and moves files from one computer to another. Port 20 is used for the data stream and transfers the data between the client and the server. Port 21 is the control stream and is used to pass commands between the client and the FTP server. Attacks on FTP commonly target plaintext passwords that can be sniffed. FTP is one of the most commonly targeted services.

- **Telnet**: Telnet is a TCP service that operates on port 23. Telnet enables a client at one site to establish a remote session with a host at another site. The program passes the information typed at the client's keyboard to the host computer system. Telnet can be configured to allow anonymous connections but should be configured to require usernames and passwords. Unfortunately, even then, Telnet sends them in plaintext. A user who is logged in can perform any task allowed by his or her user permissions. Applications like Secure Shell Version 2 (SSHv2) should be used instead of Telnet.
- **Simple Mail Transfer Protocol (SMTP)**: This TCP service operates on port 25. It is designed for the exchange of email between networked systems. Messages sent through SMTP have two parts: an address header and the message text. All types of computers can exchange messages with SMTP. Spoofing, spamming, and open/misconfigured mail relays are several of the vulnerabilities associated with SMTP.
- **Domain Name System (DNS)**: DNS operates on port 53 and performs address translation. DNS converts fully qualified domain names (FQDNs) into numeric IP addresses or IP addresses into FQDNs. This system works in a similar way to a phone directory that enables users to remember domain names (such as examcram2.com) instead of IP addresses (such as 114.112.18.23). On some small networks, *Network Information Service* (*NIS*) can be used in place of DNS to provide name server information and distribute system configuration information. DNS uses UDP for DNS queries and TCP for zone transfers. DNS is subject to poisoning and, if misconfigured, can be solicited to perform a full zone transfer. DNS Security Extensions (DNSSEC) is an alternative to DNS. With DNSSEC, the DNS server provides a signature and digitally signs every response. For DNSSEC to function properly, authentication keys have to be distributed before use. Otherwise, if the client has no means to validate the authentication, DNSSEC is of little use. You can read more about DNSSEC at www.dnssec.net.

Caution

DNSSEC does not provide confidentiality of data, and it does not protect against DDoS attacks.

- **Bootstrap Protocol (BootP)**: BootP is used to download operating parameters to thin clients and is the forerunner to Dynamic Host Configuration Protocol (DHCP). Both protocols are found on UDP ports 67 and 68.
- **Trivial File Transfer Protocol (TFTP)**: TFTP operates on port 69. TFTP uses UDP to cut down on overhead and is intended for very small files. It not only copies files without the session management offered by TCP but requires no authentication, which could pose a big security risk. It is typically used to transfer router configuration files and to configure cable modems for cable companies.
- **Hypertext Transfer Protocol (HTTP)**: HTTP is a TCP service that operates on port 80 and is one of the most well-known protocols at the application layer. An HTTP connection is a *stateless* connection. HTTP uses a request/response model in which a client sends a request and a server sends a response. Attacks that exploit HTTP can target a server, a browser, or scripts that run on the browser.
- **Internet Message Authentication Protocol (IMAP)**: IMAPv4 is an alternative to POP3 that operates on port 143. IMAPv4 offers advantages over POP3, such as enhanced functionality in manipulating a user's inbox, the capability to better manage mail folders, and optimized online performance. With IMAPv4, email is stored on the mail server and can be accessed from any IMAPv4 email client on the network. With POP3, email is downloaded to the mail client, where it is accessed.
- **Simple Network Management Protocol (SNMP)**: SNMP is a UDP service that operates on ports 161 and 162. It was envisioned as an efficient and inexpensive way to monitor and remotely configure networks. SNMP allows agents to gather information, including network statistics, and report back to their management stations. Most large corporations have implemented some type of SNMP management. Some of the security problems that plague Versions 1 and 2 of SNMP are related to the fact that community access strings are passed as plaintext, and the default community strings (public/private) are well known. SNMP Version 3 is the most current form and offers encryption for more robust security.
- **Secure Sockets Layer (SSL)**: SSL operates on port 443 and is a secure protocol used to connect to an untrusted network. SSL uses a two-part process to establish communications and is based on hybrid cryptography. It provides encryption in HTTPS. Attacks against SSL can be launched if a targeted system supports weak ciphers. In such a situation, an attacker might be able to manipulate the system so that encrypted data is downgraded or even deciphered to achieve access to sensitive data.

- **Line Printer Daemon (LPD)**: LPD operates on TCP port 515 and is a network protocol used to spool and deliver print jobs to printers.
- **Lightweight Directory Access Protocol (LDAP)**: LDAP, which operates on TCP, was created as a means to access X.500 directory services. X.500 is a series of computer networking standards covering electronic directory services. LDAP had no data encryption method in Versions 1 and 2, but Version 3 has a much stronger security model built in and supported by TLS.
- **Routing Information Protocol (RIP)**: RIP operates on port 520 and allows routing information to be exchanged between routers on an IP network. Even though RIP is usually listed as part of Layer 3, as are the other routing protocols, it is an application. RIP uses UDP ports to send and receive routing information. The original version of RIP has no security, and bogus RIP updates can be used to launch DoS attacks.
- **Pretty Good Privacy (PGP)**: PGP was developed in 1991 as a free email security application. PGPv5 uses port 11371. PGP was designed to offer military-grade encryption and works well at securing email. Unlike a public key infrastructure (PKI), PGP works by using a web of trust. Users distribute and sign their own public keys. Unlike a PKI certificate authority, this web of trust requires users to determine how much they trust the party they are about to exchange keys with. PGP is a hybrid cryptosystem in that it uses both public and private encryption. PGP can use Triple DES and Twofish for symmetric encryption and RSA for asymmetric encryption.

Although there are hundreds of ports and corresponding applications, in practice only a few hundred are in common use. CISSP exam questions on ports will most likely be focused on common ports like the ones listed in Table 5.6.

TABLE 5.6 **Common Ports**

Port	Service	Protocol
21	FTP	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP	TCP
53	DNS	TCP/UDP
67/68	DHCP	UDP
69	TFTP	UDP
80	HTTP	TCP

Port	Service	Protocol
88	Kerberos	UDP
110	POP3	TCP
111	SUNRPC	TCP/UDP
143	IMAP	TCP
161	SNMP	UDP
162	SNMP trap	UDP
389	LDAP	TCP
443	SSL/TLS	TCP

LANs and Their Components

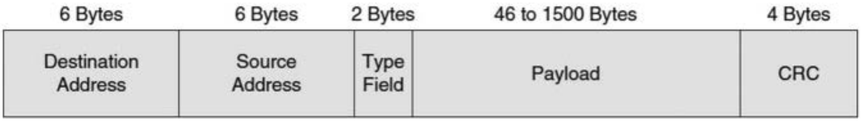
A *local area network* (*LAN*) is a critical component of a modern data network. A LAN comprises two or more computers, a communication protocol, a network topology, and cabling or wireless connectivity. A LAN includes computers or other devices that communicate over a small geographic area, such as a section of a one-story building, a whole floor of a small building, or several buildings on a small campus.

LAN Communication Protocols

More than 80% of all LANs use the Ethernet protocol as a means of communication. The Ethernet specification describes how data can be sent between computers that are in physical proximity to each other. The Digital, Intel, and Xerox (DIX) group first released Ethernet in 1975. Since its introduction, the IEEE Standards Committee has introduced several variations of the Ethernet II protocol, including the following:

- IEEE 802.3
- IEEE 802.3 with Logical Link Control (LLC)
- IEEE 802.3 with Subnetwork Access Protocol (SNAP)

Although the CISSP exam will not delve very far into the specifics of Ethernet, it is helpful to know the size and structure of these frames. Not including the preamble, an Ethernet frame ranges from 64 to 1,518 bytes. An Ethernet frame uses 18 bytes for control information; therefore, the data in an Ethernet frame can be between 46 and 1,500 bytes long. Figure 5.7 illustrates an 802.3 Ethernet frame.



6 Bytes	6 Bytes	2 Bytes	46 to 1500 Bytes	4 Bytes
Destination Address	Source Address	Type Field	Payload	CRC

FIGURE 5.7 **Ethernet Frame**

An older LAN wired networking protocol is token ring, which has all the systems arranged in a circle. A special packet, known as a *token*, travels around the circle. If any device needs to send information, it must capture the token, attach a message to it, and then let it continue to travel around the network.

Network Topologies

The layout of a network is referred to as its *topology*. Before a network can be installed, a topology must be chosen to suit the network's needs and intended use. Common topologies include bus, star, ring, mesh, and fully connected. The sections that follow discuss these topologies in greater detail.

Bus Topology

A bus topology consists of a single cable with multiple computers or devices attached to it. The cable is terminated on each end. In large environments, this is impractical because the medium has physical limitations and is subject to low speeds and complete network outages; one break can bring down an entire network (see Figure 5.8).

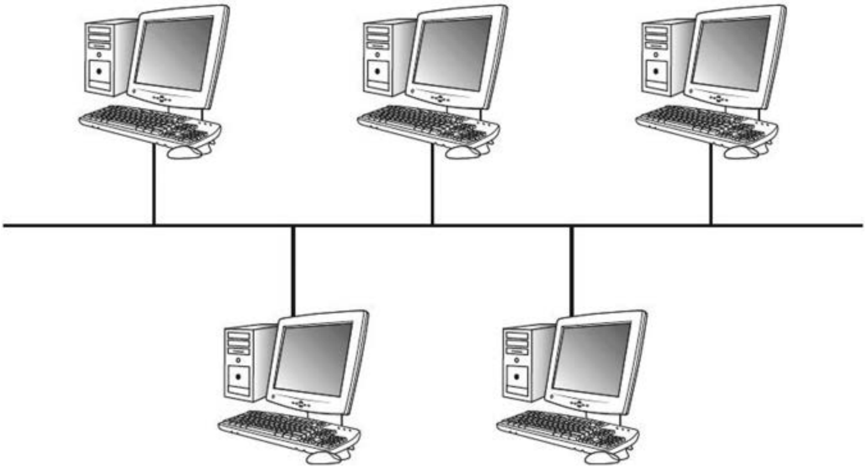


FIGURE 5.8 **Bus Topology**

Star Topology

The star topology, the oldest of the three primary network topologies, was originally used in telephone systems. The star design consists of multiple computers or devices attached to a central switch. Wires radiate outward from the hub in a star-like pattern. Although this scheme uses the most cable, a break normally affects only one computer. This is the most widely used LAN topology (see Figure 5.9).

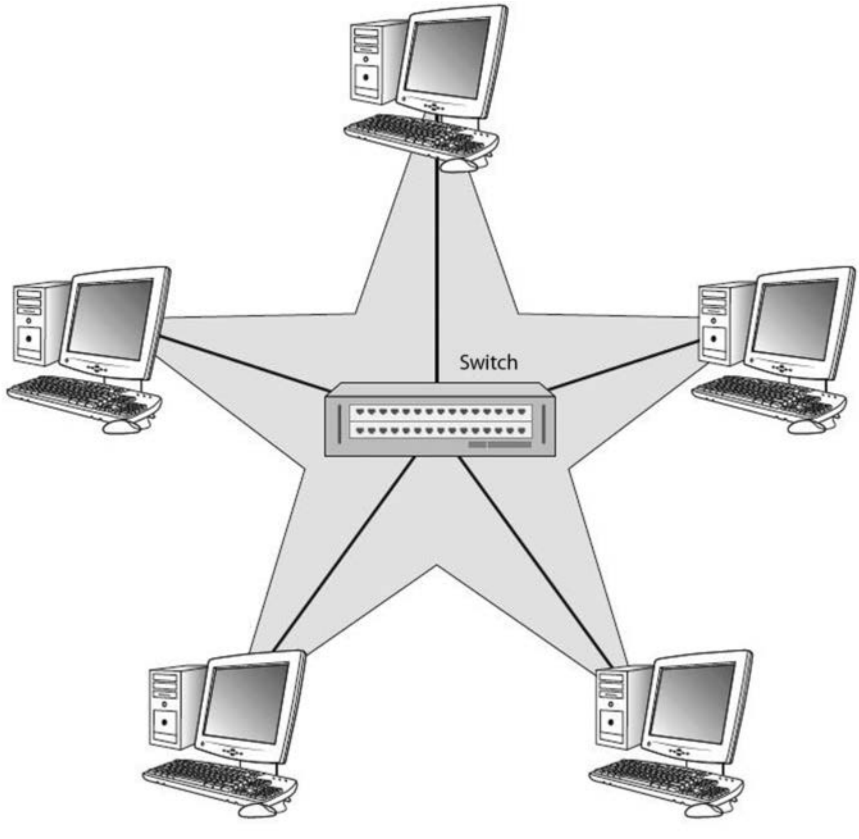


FIGURE 5.9 **Star Topology**

Ring Topology

The ring topology has no endpoints or terminators. It is laid out as a continuous loop of cable to which all networked computers are attached. Token Ring Copper Distributed Data Interface (CDDI) and FDDI networks use a ring topology (see Figure 5.10). Some ring technologies use carrier-sense multiple access with collision avoidance (CSMA/CA). Whereas CSMA/CD is a contention-based technology, CSMA/CA is deterministic.

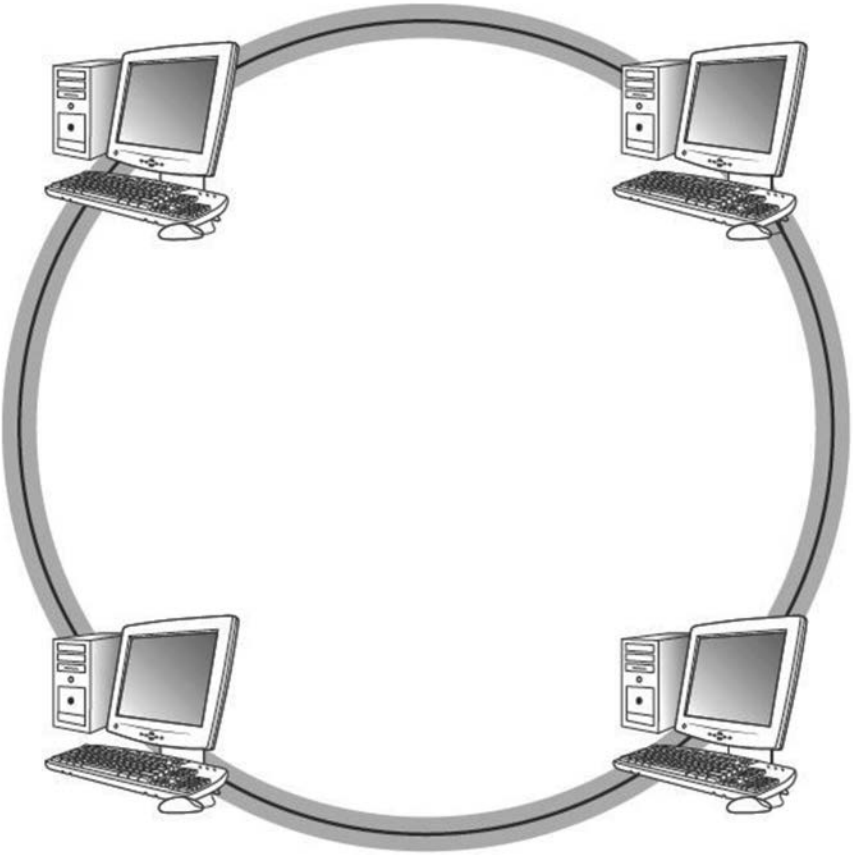


FIGURE 5.10 **Ring Topology**

ExamAlert

For the CISSP exam, you should be sure to understand how CSMA/CD works because it is Ethernet's media access method. Each device has equal priority when accessing and transmitting data on the wire. Ethernet devices must sense the wire before transmitting. If two devices attempt to transmit simultaneously, a collision occurs. When this happens, the devices wait a random period, sense the wire again, and retransmit their frames.

Mesh Topology

In a mesh network topology, each node relays data for the network. Mesh networks can use either flooding or routing to relay communications.

Fully Connected Topology

A fully connected network connects to all nodes. Although such designs offer great redundancy, the number of connections grows quickly, which makes this topology impractical for large networks.

ExamAlert

Modern networks commonly implement combinations of network topologies.

LAN Cabling

Even with a defined topology, it is necessary to determine what type of cable will connect the various devices. Cables act as a medium to carry electrical signals between the networked devices. One of two transmission methods can be used:

- **Baseband**: Baseband transmissions use the entire medium to transport a single channel of communication. Ethernet is an example of a baseband transmission scheme.
- **Broadband**: Broadband can support many channels and frequencies on its backbone. Two good examples of broadband are cable television and Digital Subscriber Line (DSL).

Many types of cables can be used for network communications, including the following:

- **Coaxial cable**: Coax cable consists of a single solid-copper wire core to carry data signals. This wire is insulated with a Teflon or plastic material, called a *dielectric*, which is covered with braided shielding used as the signal ground. The entire cable is then coated with plastic (see Figure 5.11). Common types include RG-6 and RG-59. Connectors are typically either BNC or F-connectors. Although coax was widely used in the early days of networking, its usage has waned.
- **Twisted pair**: If your computer gets its Internet connection through a wire, twisted pair wiring is used to connect the computer to a wall jack located nearby. The most common connector terminating this wiring is the RJ-45. Twisted pair is available in many varieties, including unshielded twisted pair (UTP). UTP is formed of unshielded copper wires twisted around each other and insulated in plastic. Not only is it easy to work with, but it is also generally inexpensive. Shielded twisted

pair (STP) cable comprises individually insulated twisted wire pairs (like UTP), but it has an additional shielding made of a metallic substance, such as foil. This additional shielding offers support against electromagnetic interference (EMI). The primary drawbacks to copper cabling are that it is vulnerable to being tapped, and it emanates electrical energy that could possibly be intercepted. The most common types of twisted pair cabling include Cat3, Cat5, Cat5e, Cat6, Cat6a, and Cat7. Twisted pair wiring standards include T568A and T568B. Figure 5.11 shows the components of twisted pair.

Table 5.7 lists some of the cable types, lengths, and topologies.

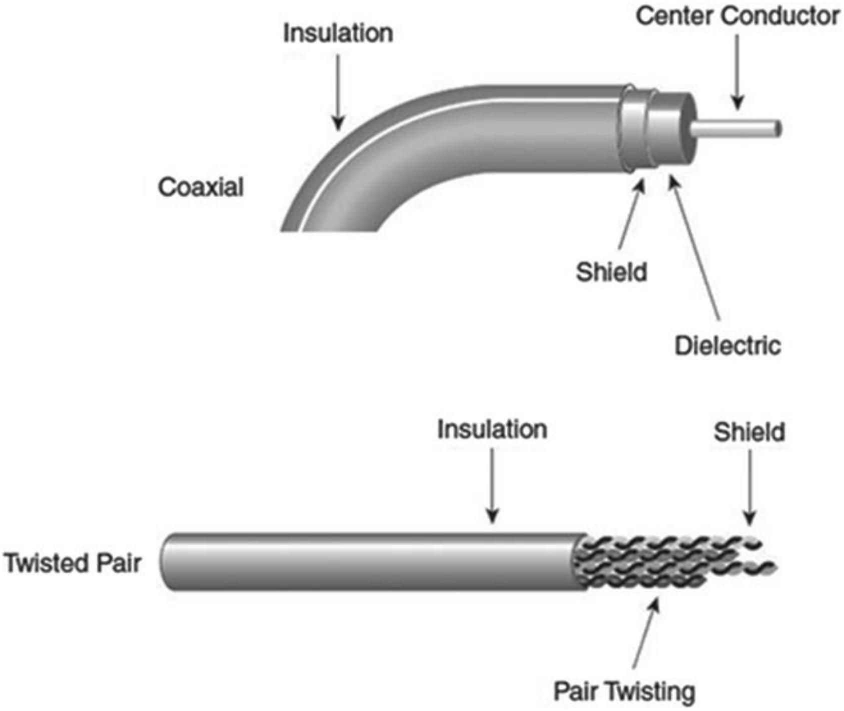


FIGURE 5.11 Coaxial and Twisted Pair

TABLE 5.7 **Cable Specification**

Ethernet Variant	Cable Specifications	Distance Supported	Topology
10BASE-5	50-ohm, thick coaxial (Thicknet)	500 meters	Bus
10BASE-2	50-ohm, RG-58 A/U (Thinnet)	185 meters	Bus
10BASE-T	Cat3 UDP (or better)	100 meters	Star
10BASE-FL	Multimode fiber optic	2,000 meters	Star
100BASE-TX	Cat5 UTP	100 meters	Star
10,000BASE-TX	Cat6/Cat7 UTP	100 meters	Star
100BASE-T4	Cat3 UTP (or better)	100 meters	Star
100BASE-FX multimode fiber optic	Multiple-fiber connections	136 meters	Star
100BASE-FX multimode fiber optic	One-fiber connection	160 meters	Star

ExamAlert

For the CISSP exam, you should know that plenum-grade cable, which is coated with a fire retardant, is designed to be used in plenum spaces, such as in crawl spaces, above false ceilings, and below the raised floors in a building. The special coating is fluoropolymers instead of the polyethylene vinyl chloride used in nonplenum cables. It is designed to not give off toxic gases or smoke as it burns to help ensure the safety of occupants in the event of a fire.

- **Fiber-optic cable**: Whereas twisted pair cable and coax cable rely on copper wire for data transmissions, fiber uses glass. These strands of glass carry light waves encoded to signal the data being transmitted. Common connector types include SC, ST, and LC. Fiber has several advantages, including greater bandwidth, and is somewhat more secure against physical tapping. Basically, two types of fiber cables are in use. They are constructed differently to handle different types of light:
  - **Multimode fiber**: Typically used in LANs and powered by light-emitting diodes (LEDs)
  - **Single-mode fiber**: Typically used in WANs and powered by laser light

Note

Fiber is more secure than copper cable because it does not radiate signals and can be tapped only with the use of specialized equipment.

Network Types

Computer networks can range from small to large. On a very small scale, there are *personal area networks* (*PANs*), which allow a variety of personal and handheld electronic devices to communicate over a short range. The most common type of PAN is a wireless PAN (WPAN). Bluetooth is one technology used in support of WPANs.

Although it is nice to know two computers can communicate locally via a local area network (LAN), most computers need the capability to communicate over a larger geographic region. To communicate between neighboring buildings, a *campus area network* (*CAN*) can be used. For computers that need to communicate on a citywide level, the *metropolitan area network* (*MAN*) was created. A MAN is a network that interconnects a region larger than that covered by a LAN. It can include a city, a geographic region, or another large area.

If you work for a company that owns several buildings located in different states or countries, that network is part of a *wide area network* (*WAN*). A WAN spans a geographic distance that is too large for LANs and MANs. WANs are connected by routers. When two LANs are connected together over a distance, they form a WAN. A *global area network* (*GAN*) connects computers from various countries or localities from around the world.

Network Storage

A *storage area network* (*SAN*) is a network of storage disks and devices. A SAN connects multiple servers to a centralized pool of disk storage. SANs improve system administration by allowing centralized storage instead of requiring management of hundreds of servers, each with its own disks. SANs are similar to network-attached storage (NAS). One of the big differences is that a NAS appears to the client as a file server or standalone system, whereas a SAN appears to the client as a local disk or volume that is available to be formatted and used locally as needed. SANs are growing in use because of increased server virtualization.

SANs can use various types of technologies for connectivity, including the following:

- **Internet Small Computer System Interface (iSCSI)**: iSCSI is a SAN standard used for connecting data storage facilities and allowing remote SCSI devices to communicate. It does not require any special infrastructure and can run over existing IP LAN, MAN, or WAN networks.
- **Fibre Channel over Ethernet (FCoE)**: FCoE, a transport protocol that is similar to iSCSI, can operate at speeds of 10 Gbps and rides on top of the Ethernet protocol. Although it is fast, it has a disadvantage in that it is non-routable.
- **Host bus adapter (HBA) allocation**: A host bus adapter is used to connect a host system to an enterprise storage device. HBAs can be allocated either through soft zoning or persistent binding. Soft zoning is more permissive, whereas persistent binding decreases address space and increases network complexity.
- **LUN masking**: LUN masking is implemented primarily at the HBA level. It is a system that makes LUNs available to some HBAs but not to others. LUN masking implemented at this level is vulnerable to any attack that compromises the local adapter.

Several issues related to SANs include redundancy, replication, snapshots, and duplication. Location redundancy is the concept that data should be accessible from more than one location as a backup. An extra measure of redundancy can be provided by means of a replication service so that data is available even if the main storage backup system fails.

Another issue with SANs is the protection of the data. Secure storage management and replication systems are designed to allow a company to manage and handle all corporate data in a secure manner, with a focus on the confidentiality, integrity, and availability of the information. The replication service allows for the data to be duplicated and secured so that confidentiality and fault tolerance are achieved.

For better fault tolerance, multipath solutions can be used to reduce the risk of data loss or lack of availability. Multipathing involves setting up multiple routes between a server and its drives. Multipathing software maintains a listing of all requests, passes them through the best possible path, and reroutes communication if one of the paths dies.

SAN snapshots provide the capability to temporarily stop writing to physical disk to make a point-in-time backup copy. Snapshot software is typically fast and makes a copy quickly, regardless of the drive size.

De-duplication in SANs is the process of removing redundant data to improve enterprise storage utilization. Redundant data is not copied but is replaced with a pointer to the one unique copy of the data. Only one instance of redundant data is retained on the enterprise storage media, such as disk or tape.

Communication Standards

The baseband and broadband communications discussed earlier in this chapter need to be signaled across the cabling. This signaling can take place using one of three methods:

- **Simplex**: Communication occurs in one direction.
- **Half duplex**: Communication can occur in both directions, but only one system can send information at a time.
- **Full duplex**: Communication occurs in both directions, and both computers can send information at the same time.

Something to consider when choosing cabling is how far you need to propagate the signal. Although each communication approach has specific advantages, there are also some common disadvantages, including attenuation and crosstalk. *Attenuation* is the reduction of signal. As the signal travels farther away from the transmitting device, the signal becomes weaker in intensity and strength. Therefore, all signals need periodic reamplification and regeneration. Figure 5.12 illustrates attenuation. Crosstalk is bleed over from one channel to another.

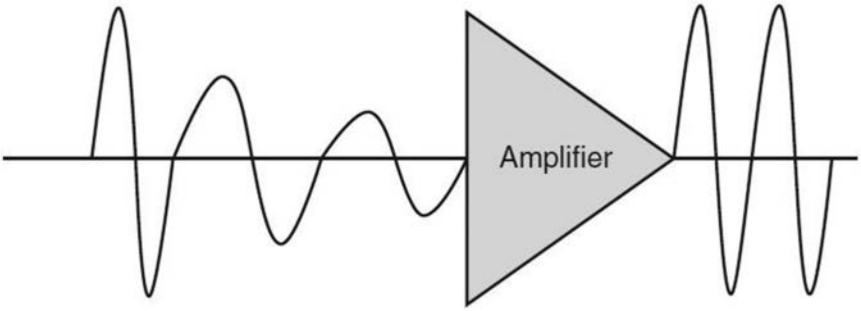


FIGURE 5.12 Attenuation

Your basic choices for signaling are analog or digital transmissions. Both analog and digital signals vary a carrier wave in frequency and amplitude. With analog signals, however, it is harder to eliminate noise and to determine where the signal ends and where noise begins.

Network Equipment

Telecommunications equipment refers to all the hardware used to move data between networked devices, including equipment for LANs and WANs. It is important to know about the various types of network equipment not only from a networking standpoint but also to better implement security solutions and pass the CISSP exam.

Repeaters

Repeaters, concentrators, and amplifiers are used to strengthen the communication signal and overcome the problems with attenuation. These devices all operate at Layer 1 of the OSI model.

Hubs

Hubs are some of the most basic multiport networking devices. A hub allows all the connected devices to communicate with one another. A hub is logically nothing more than a common wire to which all computers have shared access. Hubs operate at Layer 1 of the OSI model. Systems on a hub all share the same broadcast and collision domain.

Hubs have fallen out of favor because of their low maximum throughput. Whenever two or more systems attempt to send packets at the same time on the same hub, there is a collision. As utilization increases, the number of collisions skyrockets, and the overall average throughput decreases.

ExamAlert

For the CISSP exam, don’t spend too much time worrying about repeaters and hubs; just know their basic purpose and that they’ve been replaced by Layer 2 switches.

Bridges

Another somewhat outdated piece of equipment is a wired bridge. Bridges are semi-intelligent pieces of equipment that have the capability to separate collision domains. Bridges examine frames and look up the corresponding MAC addresses. If a device tied to a particular MAC address is determined to be local, the bridge blocks the traffic.

One big problem with bridges is that, by default, they pass broadcast traffic. Too much broadcast traffic can effectively flood the network and cause a broadcast storm. Almost the only bridges seen today are the wireless bridges used in 802.11x networks.

ExamAlert

Exams—including the CISSP exam—are notorious for lagging behind the real world. Although items like bridges are rarely seen in the workplace today, the exam might cover them. It is also important to understand, from a historical perspective, how we got to where we are today and to understand corporate security documentation that describes earlier technologies.

Switches

A switch performs in much the same way as a hub; however, switches are considered intelligent devices. A switch segments traffic by observing the source and destination MAC addresses of each data frame. In the classical sense, switches are OSI Layer 2 devices; modern switches can operate at higher layers and have the capability to work with different headers.

A sample technology that bridges Layer 2 and Layer 3 is known as *Multiprotocol Label Switching* (*MPLS*). MPLS is an OSI Layer 2 protocol. MPLS works with high-speed switches.

Commercial switches also offer *virtual LAN* (*VLAN*) capabilities. Such switches can operate at Layer 3 of the OSI model. A VLAN allows a group of devices on different physical LAN segments to communicate with each other as if they were all on the same logical LAN.

Note

The basic difference between Layer 2 switches and switches that work at higher layers is in the way they deal with addresses and tags.

Switches operate by storing MAC addresses in a lookup table that is located in *random-access memory* (*RAM*). This lookup table, which is also referred to as *content-addressable memory* (*CAM*), contains the information needed to match each MAC address to the corresponding port it is connected to. When the data frame enters the switch, it finds the target MAC address in the lookup table and matches it to the switch port the computer is attached to. The frame is forwarded to only that switch port; therefore, computers on all other ports never see the traffic. Switches offer the following advantages:

- They provide higher throughput than hubs.
- They provide VLAN capabilities.
- They can be configured for full duplex.
- They can be configured to span a port to support intrusion detection systems/intrusion prevention systems (IDSs/IPSs), network feeds, or monitoring.

Note

Microsegmentation allows you to segment networks even further. With microsegmentation, every node can have access to the entire bandwidth available in the transmission channel rather than sharing the bandwidth with others. Microsegmentation enables the creation of dedicated or private segments.

Not all switches are made the same. Switches can process an incoming frame in three ways:

- **Store-and-forward**: After a frame is completely input into the switch, the destination MAC address is analyzed to block or forward the frame.
- **Cut-through**: This faster design is similar to the store-and-forward design, but it examines only the first 6 bytes and then forwards the packet to its rightful owner.
- **Fragment free**: This is a Cisco Systems design that has a lower error rate than the other designs.

Note

Originally, switches were Layer 2 devices; today, switches can be found at Layer 3 of the OSI model and can work up to Layer 7. Higher-layer switches are known as *content switches*, *content-services switches*, or *application switches*.

Mirrored Ports and Network Taps

Monitoring devices have a harder time examining traffic on switched networks than on non-switched networks. To overcome this problem, port mirroring is used. Different vendors use different names for this technology. For example, Cisco Systems offers Switched Port Analyzer (SPAN), and 3Com offers Roving Analysis Port (RAP).

Port mirroring is used to send a copy of network packets from one switch port to a network monitoring connection on another switch port. Therefore, if you are using a managed switch, you can configure port mirroring to easily capture and analyze traffic. Although this works well in corporate environments and in situations where you have control of the managed switch, it is not as useful when a switch is unmanaged or where someone does not have access to the switch. In such cases, network taps can be used. A network tap provides another way to monitor a network and see all traffic, much like a hub. This functionality acts as a point to intercept traffic. For example, a Throwing Star LAN tap is a simple device that allows anyone to easily monitor Ethernet communications (see greatscottgadgets.com/throwingstar/).

VLANs

Virtual LANs (VLANs) are used to segment network traffic to create smaller broadcast domains. VLANs reduce network congestion and increase bandwidth, and they do not need to be isolated to a single switch; a VLAN can span many switches throughout an organization.

You can extend VLANs by using a trunking protocol. A trunking protocol propagates the definition of a VLAN to the entire LAN. Trunking protocols work by encapsulating Ethernet frames. Two common trunking protocols are the 802.1Q standard and Cisco's proprietary Inter-Switch Link (ISL). The 802.1Q standard places information inside an Ethernet frame, whereas ISL wraps an Ethernet frame.

> **Note**
>
> Spanning Tree Protocol (STP), which is another protocol that can be used in a VLAN, is used to prevent networking loops, build active paths, and provide for backup paths in the event that an active path or link fails. The newest version is Rapid Spanning Tree Protocol (RSTP), which is backward compatible with STP and provides significantly faster spanning tree convergence.

Virtual Extensible LAN (VXLAN) is a technology designed to provide the same Ethernet Layer 2 network services as a VLAN but with greater extensibility and flexibility. VXLAN supports the virtualization of a data center network while addressing the needs of multi-tenant data centers by providing the necessary segmentation on a large scale.

Note

VXLAN is an encapsulation protocol that provides mechanisms to aggregate and tunnel multiple Layer 2 subnetworks across a Layer 3 infrastructure.

Trunking security is an important concern in VLANs. A *trunk* is simply a link between two switches that carries the data of more than one VLAN. A security professional should be aware that an attacker who can get access to a trunked connection can potentially jump from one VLAN to another. This is called *VLAN hopping*. It is very important to ensure that trunked connections are secure so that malicious activity cannot occur.

ExamAlert

VLAN hopping is a hacking technique that enables attackers to send packets outside a VLAN. These attacks are generally launched by tagging the traffic with a VLAN ID that is outside the attacker's VLAN.

Routers

Routers reside at Layer 3 of the OSI model. Routers are usually associated with IP, which sends blocks of data that have been formatted into packets. IP is considered a best-effort delivery protocol, and IP packets are examined and processed by routers. Routers can connect networks that have the same or different media types.

A router's primary purpose is to forward IP packets toward their destination through a process known as *routing*. Whereas bridges and switches examine the physical frame, routers focus on the information in the IP header. One important item in the IP header is the IP address. As mentioned earlier, an IP address is a logical address; it is laid out in dotted-decimal notation format. The IPv4 address format is four decimal numbers separated by decimal points. Each of these decimal numbers is 1 byte in length, supporting values from 0 to 255. IPv4 addresses are separated into the following classes:

- **Class A**: A Class A network consists of up to 16,777,214 client devices. The address range can extend from 1 to 126.

- **Class B**: A Class B network consists of up to 65,534 client devices. The address range can extend from 128 to 191.
- **Class C**: A Class C network can have 245 devices. The address range can extend from 192 to 223.
- **Class D**: A Class D network is reserved for multicasting. The address range can extend from 224 to 239.
- **Class E**: A Class E network is reserved for experimental purposes. The addresses range from 240 to 254.

ExamAlert

You may have noticed that the 127.0.0.0 address range is missing from the preceding list. Although officially part of the class A address range, it is used for loopback. The CISSP exam may test you on such details.

Not all the addresses shown can be used on the Internet. Some addresses have been reserved for private use and are considered nonroutable. These private addresses include the following:

- **Class A**: 10.0.0.0
- **Class B**: 172.16.0.0 to 172.31.0.0
- **Class C**: 192.168.0.0 to 192.168.255.0

Routers can be used to improve performance by limiting physical broadcast domains. They act as a limited type of firewall when *access control lists* (*ACLs*) are used for filtering, and they ease network management by segmenting larger networks into smaller subnets. The security of a network's router is paramount. A compromised router can have devastating consequences, especially if it is used as an endpoint for other services, such as IPsec, a VPN, or a firewall.

ExamAlert

Blocking unauthorized traffic via routers and firewalls is sometimes referred to as *bogon filtering*. Bogons are simply IP packets that are spoofed and appear to be from an area of the IP address space that is reserved but not yet allocated or delegated by the Internet Assigned Numbers Authority (IANA) or a delegated Regional Internet Registry (RIR).

Gateways

A *gateway*, sometimes called a *protocol translator*, connects networks that use dissimilar protocols by converting one software protocol into another. A gateway can be software based or can be a standalone hardware device. Gateways function at Layer 7 of the OSI model.

Routing

Routing protocols are a key component of modern networks. Confusion often exists over the terms *routed protocol* and *routing protocol*. Both reside at Layer 3. Routed protocols can be forwarded from one router to another. A good example of a routed protocol is IP. IP acts as the postal service of the Internet. Its job is to organize data into a packet and then address the packet for delivery. IP must place target and source addresses on the packet. This is similar to addressing a package before delivering it to the post office. And as with physical packages in the postal system, postage is required: In the world of IP, the postage is a TTL (Time-to-Live) value, which keeps packets from traversing the network forever and decrements every time a router is passed. If the recipient cannot be found before the TTL reaches 1, the packet is discarded.

A routing protocol sends and receives routing information to and from other routers. A routing protocol can be likened to a large mechanized mail sorting machine. Whereas routed protocols, such as IP, build and address a packet, a routing protocol must decide how to best deliver a packet. In real life, there are many ways to get from point A to point B. Likewise, on the Internet, there are many paths to a target network.

Routing protocols can be placed into several basic categories:

- **Static routing**: *Static*, or fixed, routing algorithms are not actually algorithms. They rely on a simple table developed by a network administrator mapping one network to another. Static routing works best when a network is small and the traffic is predicable. The big problem with static routing is that it cannot react to network changes. As networks grow, management of these tables can become difficult. Although this makes static routing unsuitable for use on the Internet or other large networks, it can be used in special circumstances where normal routing protocols don't function well.

- **Dynamic routing**: *Dynamic routing* uses metrics to determine which path a router should use to send a packet toward its destination. Dynamic routing protocols include RIP, BGP, IGRP, and OSPF. Dynamic routing takes time as all routers must learn about all possible paths. *Convergence* is reached when all routers on a network agree on the state of routing.
- **Default routes**: *Default routes* are similar to static routes. When default routes are used and the router knows no other route to use, the designated route becomes the default path the router uses to transmit packets.

Each time a router receives packets, it must examine them and determine what interface to forward the packets to. Not all routing protocols that routers work with function in the same manner. Dynamic routing protocols can be divided into two broad categories:

- Algorithms based on distance-vector protocols
- Algorithms based on link-state protocols

Distance-vector protocols, which are based on Bellman-Ford algorithms, try to find the best route by determining the shortest path. The shortest path is commonly calculated based on hops. Distance-vector routing is also called *routing by rumor*.

RIP is probably the most common distance-vector protocol currently in use. It is a legacy UDP-based routing protocol that does not use authentication and that determines path based on hop count. RIP has a 15-hop count maximum and uses broadcast routing updates to all devices. Later versions of RIP provide authentication in plaintext. Although RIP works in small networks, it does not operate successfully in large network environments. RIP makes use of *split horizon* and *poison reverse*. Split horizon is a route advertisement that prevents routing loops in distance-vector routing protocols by prohibiting a router from advertising a route back onto the router interface from which it was discovered. Poison reverse allows a gateway node to tell its neighbor gateways that you can't get there from here. It basically means that one of the gateways is no longer connected. Poison reverse sets the number of hops to the unconnected gateway to 16 hops; this number of hops indicates "infinite."

One major shortcoming of distance-vector protocols is that the path with the lowest number of hops might not be the optimal route. The path with the lowest hop count could have considerably less bandwidth than a route with a higher hop count.

Caution

Distance-vector protocols like RIP can be spoofed and are subject to redirection. It is also easy for attackers to sniff RIP updates. RIP routers update each other by sending out complete routing tables every 30 seconds.

Link-state protocols are based on Dijkstra's algorithm. Unlike distance-vector protocols, link-state protocols determine the best path with metrics like delay or bandwidth. When this path is determined, the router informs other routers of its findings. This is how reliable routing tables are developed and routing tables reach convergence. Link-state routing protocols are considered more robust than distance-vector routing protocols. OSPF is probably the most common link-state routing protocol; it is often used as a replacement for RIP.

OSPF is an improved link-state routing protocol that offers authentication. It is an implementation of a link-state-based routing protocol developed in the mid-1980s to overcome the problems associated with RIP. OSPF has several built-in advantages over RIP, including the use of IP multicast to send out router updates, no limitation on hop count (as with RIP), better support for load balancing, and fast convergence.

Routing protocols can be further divided and defined as interior or exterior routing protocols. RIP, OSPF, and IS-IS are three examples of interior routing protocols. Interior routing protocols are used within an organization.

Exterior gateway protocols are used by routers connecting different *autonomous systems* (*ASs*). An example of an exterior routing protocol is BGP, which is the core routing protocol used by the Internet. It is based on TCP and is used to connect autonomous systems.

Note

An early exterior routing protocol was Exterior Gateway Protocol (EGP). This term is sometimes used to describe all exterior routing protocols.

WANs and Their Components

WANs are considerably different from LANs. Organizations usually own their own LANs, but WAN services are typically leased; it's not feasible to have your network guy run a cable from New York to Dallas. WANs are concerned with the long-haul transmission of data and connect remote devices. The Internet is a good example of a WAN. WAN data transmissions typically incur higher costs than LAN transmissions. WAN technologies can be divided into two broad categories: *packet switching* and *circuit switching*.

Packet Switching

Packet-switched networks share bandwidth with other devices. Packet-switched networks divide data into packets and frames. These packets are individually routed among various network nodes at the provider's discretion. They are considered more resilient than circuit-switched networks and work well for on-demand connections with "bursty" traffic. Each packet takes the most expedient route, which means the packets might not arrive in order or at the same time. Packet switching is a form of connectionless networking.

Synchronous Optical Network (SONET)

A large portion of long-haul data communication is done via fiber. *SONET* is one of the leading technologies that makes this possible. SONET uses light to send multiple digital data streams over the same fiber-optic cable.

X.25

X.25 is one of the original packet-switching technologies. Although it is not fast, with speeds up to 56 Kbps, it is reliable and works over analog phone lines.

Frame Relay

Frame Relay is a virtual circuit-switched network. It is a kind of streamlined version of X.25. Frame Relay controls bandwidth use with a *committed information rate* (*CIR*) that specifies the maximum guaranteed bandwidth the customer is promised. The customer can send more data than specified in the CIR if additional bandwidth is available. If there is additional bandwidth, the data passes; otherwise, the data is marked discard eligible (DE) and is discarded.

Frame Relay can use *permanent virtual circuits* (*PVCs*) or *switched virtual circuit* (*SVCs*). A PVC is used to provide a dedicated connection between two locations. An SVC works much like a phone call in that connections are set up on a per-call basis, and a call is disconnected when it is complete. Switched virtual circuits are good when data transmission is sporadic and for teleconferencing and phone calls.

Asynchronous Transfer Mode (ATM)

ATM is a cell-switching-based physical layer protocol. It supports high-bandwidth data needs and works well for time-sensitive applications. Because the switching process occurs in hardware, delays are minimized. ATM uses a fixed cell size of 53 bytes. ATM can be implemented on LANs or WANs.

ATM is being surpassed by newer technologies, such as MPLS, which is described earlier in this chapter. MPLS designers recognized that data didn't need to be converted into 53-byte cells. MPLS packets can be much larger than ATM cells. MPLS can provide traffic engineering, and it enables the creation of VPNs without end-user applications. MPLS can carry many types of traffic, handles addresses via labels, and does not encapsulate header data.

Note

For the CISSP exam, keep in mind that MPLS uses labels to simplify WAN routing and can carry voice and data.

Circuit Switching

Circuit switching comes in either analog or digital configurations. At the heart of circuit switching is multiplexing. *Multiplexing* is a technique used to combine multiple channels of data over a single set of wires or a transmission path. Today the most common form of circuit switching is the plain old telephone service (POTS), but ISDN, T-carrier, and Digital Subscriber Line (DSL) are also options. The sections that follow describe these circuit-switching options in more detail.

Plain Old Telephone Service (POTS)

POTS is a voice-grade analog telephone service used for voice calls and for connecting to the Internet and other locations via modem. Modem speeds can vary from 9600 bps to 56 Kbps. Although POTS is relatively inexpensive and widely available, it offers only low data speeds.

Integrated Services Digital Network (ISDN)

ISDN is a communication protocol that operates similarly to POTS, except that all-digital signaling is used. Although originally planned as a replacement for POTS, ISDN was not hugely successful. ISDN uses separate frequencies called *channels* on a special digital connection. It consists of B channels used for voice, data, video, and fax services and a D channel used for signaling by the service provider and user equipment. Keeping the D signaling data separate makes it harder for attackers to manipulate the service. The D channel operates at a low 16 Kbps; the B channels operate at speeds up to 64 Kbps. By binding the B channels together, ISDN can achieve higher speeds. ISDN is available in two levels: Basic Rate Interface (BRI) at up to 128 Kbps and Primary Rate Interface (PRI) at up to 1.544 Mbps. BRI comprises 2 B channels and 1 D channel, and PRI comprises 23 B channels and 1 D channel.

T-Carrier

T-carrier service is used for leased lines. A leased line, which is locked between two locations, is very secure, and users pay a fixed monthly fee for this service, regardless of use. The most common T-carrier is a T1. A T1 uses time-division multiplexing and consists of 24 digital signal 0 (DS0) channels. Each DS0 channel is capable of transmitting 64 Kbps of data; therefore, a T1 can provide a composite rate of 1.544 Mbps. T3s are the next available choice. A T3 is made up of 672 DS0s and has a composite data rate of 45 Mbps. For those who don't need a full T1 or a full T3, fractional service is available. A fractional T-line is just a portion of the entire carrier. Table 5.8 details common T-carrier specifications and contrasts them with POTS, ISDN, and DSL.

TABLE 5.8 **Circuit-Switching Specifications**

Service	Characteristics	Maximum Speed
POTS dialup service	Switch line; widely used	56 Kbps
ISDN BRI digital	Requires a terminal adapter; can be costly	128 Kbps
ISDN PRI digital	Requires a terminal adapter; can be costly	1.54 Mbps
DSL	Typically asymmetric; downloads faster than uploads	Up to 52 Mbps
T1	Dedicated leased line; 24 bundled phone lines	1.54 Mbps
T3	Dedicated leased line; 28 bundled T1s	44.736 Mbps

Note

T1s are the standard in the United States, and Europe uses an E-carrier system. An E1 carries 30 channels; an E3 is 16 E1s. E1s are dedicated 2.048 Mbps circuits, and E3 are dedicated 34.368 Mbps circuits.

Digital Subscriber Line (DSL)

DSL is another circuit-switching connectivity option. DSL is typically asymmetric, which means that the download speed is much faster than the upload speed. The theory is that you usually download more than you upload.

DSL modems are always connected to the Internet; therefore, you do not have to dial in to make a connection. As long as your computer is powered on, it is connected to the Internet and is ready to transmit and receive data. This is the primary security concern with DSL. An advantage of DSL is that it maintains a more fixed speed than cable modems typically do. Table 5.9 provides details about the different DSL types.

TABLE 5.9 **DSL Types and Speeds**

DSL Type	Data Rate	Mode	Distance
IDSL (ISDN DSL)	160 Kbps	Duplex	18,000 ft., 24 AWG
HDSL (High-Bit-Rate DSL)	1.544 Mbps 2.048 Mbps	Duplex Duplex	12,000 ft., 24 AWG
SDSL (Symmetric DSL)	1.544 Mbps 2.048 Mbps	Duplex Duplex	10,000 ft., 24 AWG
ADSL (Asymmetric DSL)	1.5–9 Mbps 16–640 Kbps	Down Up	9,000–18,000 ft., 24 AWG
VDSL (Very-High-Bit-Rate DSL)	13–52 Mbps 1.5–2.3 Mbps	Down Up	1,000–4,500 ft., 24 AWG

Cable Internet Access

Cable Internet access refers to the delivery of Internet access over the cable television infrastructure. The Internet connection is made through the same coaxial cable that delivers the television signal to your home. The coaxial cable connects to a special cable modem that demultiplexes the TCP/IP traffic. This always-on Internet connection presents a big security issue if no firewall is used. One of the weaknesses of cable Internet access is that there is a shared amount of bandwidth among many users. Cable companies control the maximum data rate of each subscriber by capping the maximum data rate. Some unscrupulous individuals attempt to uncap their line to obtain higher speeds. Uncappers can be caught and prosecuted because cable Internet providers routinely check for this illegal action.

Note

Although uncapping a cable connection might lead only to a disconnection of your service, service providers might push for criminal charges. That's what happened to one Buckeye Cable customer whose home was searched by the FBI; the individual in that case was charged with fifth-degree felonies for tampering with the service connection in violation of law.

Problems with cable modems continue to be discovered. It is possible to hijack some cable modems by simply visiting a vulnerable website (see www.gnucitizen.org/blog/bt-home-flub-pwnin-the-bt-home-hub/).

Another lingering concern is loss of confidentiality. Individuals have worried about the possibility of sniffing attacks. Most cable companies have addressed this issue by implementing the Data Over Cable Service Interface Specification (DOCSIS) standard. The DOCSIS standard specifies encryption and other security mechanisms that prevent sniffing and protect privacy. DOCSIS is currently at Version 3.1.

Other WAN Technologies

When systems communicate with each other remotely, a variety of protocols and standards are needed, including the following:

- **Switched Multimegabit Data Service (SMDS)**: SMDS is a high-speed, packet-switched service used for MANs and WANs.
- **Synchronous Data Link Control (SDLC)**: SDLC was developed by IBM in the 1970s and used to develop HDLC. SDLC is a Layer 2 communication protocol designed for use with mainframes.
- **High-Level Data Link Control (HDLC)**: HDLC uses a frame format to transmit data between network nodes. It supports full-duplex communication and is used with Systems Network Architecture (SNA).
- **High-Speed Serial Interface (HSSI)**: HSSI is a connection standard used to connect routers and switches to high-speed networks.

Cloud Computing

Cloud computing is an Internet-based approach that provides computing and storage capacity as a service, as illustrated in Figure 5.13. Cloud computing can be broken down into several basic models, including the following:

- **Infrastructure-as-a-service (IaaS)**: IaaS is a cloud solution in which you purchase virtual power to execute your software as needed. This is much like running a virtual server on your own equipment, except you are running a virtual server on a virtual disk. This model is similar to a utility company model, where you pay for what you use.

- **Software-as-a-service (SaaS)**: SaaS is designed to provide a complete packaged solution, with software rented out to the user. The service is usually provided through some type of front-end or web portal. Although the end user is free to use the service from anywhere, the company pays a per-use fee.
- **Platform-as-a-service (PaaS)**: PaaS provides a platform for your use. Services provided by this model include all phases of the software development life cycle (SDLC) and can include application program interfaces (APIs), website portals, or gateway software. These solutions tend to be proprietary, which can cause problems if the customer moves away from the provider's platform. Unlike IaaS and SaaS, PaaS includes a development environment. Two technologies used in this area are containers and dockers. A container packages up code and all its dependencies. A container allows software to run quickly and reliably from any computing. A docker is a standalone executable package of software that includes everything needed to run an application. Kubernetes is an open-source system for automating deployment, scaling, and management of containerized applications.

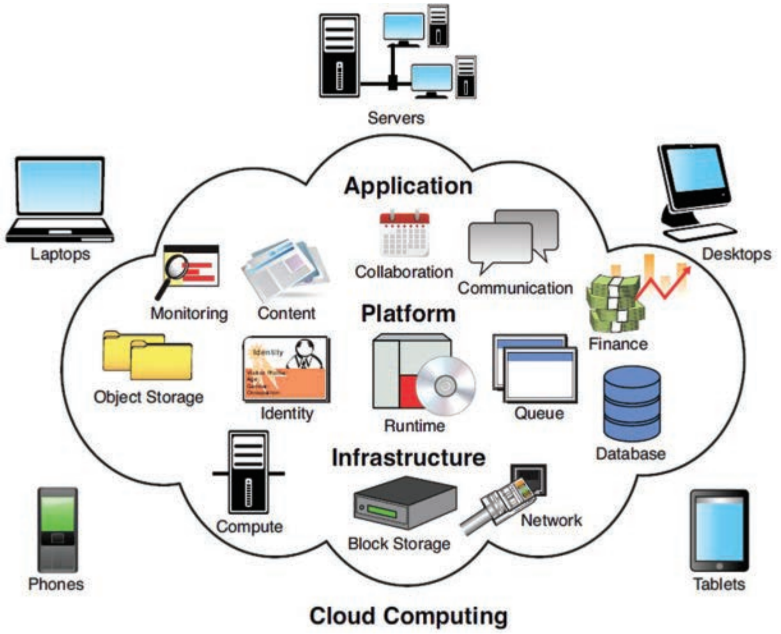


FIGURE 5.13 Cloud Computing

Software-Defined WAN (SD-WAN)

Software-Defined WAN (SD-WAN) is a cost-effective alternative to traditional networking technology. SD-WAN is used for connecting geographically distributed locations and remote users. While software-defined networking (SDN) and SD-WAN seem closely related and serve similar purposes, SDN targets the management of LANs and centralizes management. OpenFlow is one protocol that can be used with SDN to allow for control of switching rules from a central controller. Table 5.10 shows the basic differences between SD-WAN and SDN.

TABLE 5.10 **SDN and SD-WAN Uses and Details**

SDN	SD-WAN
Manages a LAN or service provider's core network	Enables connections between networks and users across geographies
Programmable by the user to deliver bandwidth on demand	Programmable to deliver operational simplification, integrated security, and traffic prioritization
Separates the control plane from the data plane	Separates the control plane from the data plane
Provides a centralized view for automation of network services	Focuses on software-defined application routing capabilities

Securing Email Communications

Secure email solutions are important because email is one of the most widely used Internet applications. Email is susceptible to several threats, including spoofing, spamming, and address forgery. Standard email uses Simple Mail Transfer Protocol (SMTP) TCP port 25 to accept messages from clients and Internet Message Access Protocol (IMAP4) TCP port 143 or Post Office Protocol Version 3 (POP3) TCP port 110 to retrieve email from server-based inboxes.

Sending an email is much like sending a postcard through the postal service: Anyone along the way can easily read the note your mom wrote to you while visiting the Grand Canyon. Fortunately, several applications and protocols are available to help secure email. The following sections describe some of them.

Pretty Good Privacy (PGP)

Phil Zimmermann developed PGP in 1991 by to provide privacy and authentication. Over time, it evolved into an open standard known as OpenPGP, and it can be purchased as a commercial product from Symantec for enterprise known as PGP Whole Disk Encryption.

PGP is unlike PKI in that there is no CA. PGP builds a web of trust that develops as users sign and issue their own keys. Users must determine what level of trust they are willing to place in other parties. The goal was for PGP to become encryption for everyone (as opposed to encryption available only to companies and corporations). Popular programs and providers such as ProtonMail and Hushmail are based on PGP.

Other Email Security Applications

PGP is not the only option for securing email. Other options include the following:

- **Secure Multipurpose Internet Mail Extensions (S/MIME)**: By default, MIME does not provide any protection. To overcome this problem, RSA developed S/MIME. S/MIME has been built in to virtually every email system to encrypt and digitally sign the attachments of protected email messages. S/MIME adds two valuable components to standard email: digital signatures and public key encryption. S/MIME supports X.509v3 digital certificates and RSA encryption.
- **Privacy Enhanced Mail (PEM)**: PEM is an older standard that has not been widely implemented but was developed to provide authentication and confidentiality. PEM public key management is hierarchical. PEM uses MD2/MD5 and RSA for integrity and authentication.
- **Message Security Protocol (MSP)**: MSP is a military version of PEM. Because it was developed by the National Security Agency (NSA), it has not been open to public scrutiny and is not widely used. It is part of the DoD's Defense Messaging System and provides authentication, integrity, and nonrepudiation. The military has its own security network, called SIPRNet.
- **MIME Object Security Services (MOSS)**: MOSS extends the functionality of PEM but is not widely used as it has been eclipsed by S/MIME and PGP. MOSS is the only email standard that gives users an out-of-the-box mechanism for signing the recipient list.

Securing Voice and Wireless Communications

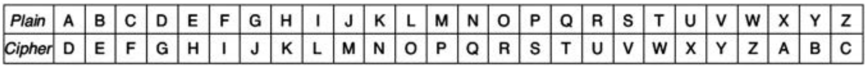
Secure communications have come a long way from the time of the Spartans, Romans, and others who used crude forms of encryption. VoIP and wireless capture more attention and use each year. Some studies report that there are more cell phones in China than there are people in the United States. 5G supports the ability to deploy millions of tiny sensors that can collect all kinds of data across networks around the globe. Li-Fi, which is a wireless communication technology that has been promoted as the key to solving challenges faced by 5G, uses light to transmit data and position between devices and is being promoted as more reliable, virtually interference free, and uniquely more secure than radio technology such as Wi-Fi or cellular.

The following sections look at some of these technologies and the history of secure communications.

Secure Communications History

Throughout time, there has been a need for secure communications. As long as there have been people, there have been secrets. One early system that was used by the ancient Greeks and the Spartans is called *scytale*. This system involved wrapping a strip of papyrus around a rod of fixed diameter on which a message was written. If anyone intercepted the paper, it appeared as a meaningless letters. The recipient could read the message by wrapping the papyrus around a rod of the same diameter.

Even Julius Caesar encrypted messages he sent to his trusted advisors. Caesar's cipher was a simple substitution cipher. In *Caesar's cipher*, there was a plaintext alphabet and a ciphertext alphabet. The alphabets were arranged as shown in Figure 5.14.



Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

FIGURE 5.14 **Caesar's Cipher**

When Caesar was ready to send a message, it was encrypted by moving the text forward according to the key. If the key was 3 characters, for example, then the word "cat" would encrypt to "fdw." You can see how this works by examining Figure 5.14. Just look up each of the message's letters in the top row and write down the corresponding letter from the bottom row. Caesar's cipher is also known as a rotation cipher, and a key of three is called ROT3. Although it is not a robust method of encryption, Caesar was able to use it with great success.

Ancient Hebrews used a similar cryptographic system called ATBASH that worked by replacing a letter with another letter the same distance away from the end of the alphabet; for example, *A* was sent as a *Z*, and *B* was sent as a *Y* (see Figure 5.15).

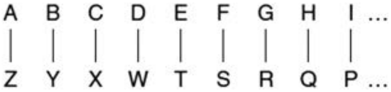


FIGURE 5.15 **ATBASH**

More complicated substitution ciphers were developed through the Middle Ages as individuals became better at breaking simple encryption systems. In the ninth century, Abu al-Kindi published what is considered to be the first paper that discusses how to break cryptographic systems. This paper, titled "A Manuscript on Deciphering Cryptographic Messages," discusses using frequency analysis to break cryptographic codes. *Frequency analysis* is the study of how frequently letters or groups of letters appear in ciphertext. Uncovered patterns can aid individuals in determining patterns and breaking the ciphertext.

These early ciphers all had weaknesses, and people worked to improve them. A *polyalphabetic cipher* makes use of more than one arrangement of the alphabet. The alphabetic cipher known as the Vigenère cipher uses the following encryption/decryption chart:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

B C D E F G H I J K L M N O P Q R S T U V W X Y Z A

C D E F G H I J K L M N O P Q R S T U V W X Y Z A B

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

E F G H I J K L M N O P Q R S T U V W X Y Z A B C D

F G H I J K L M N O P Q R S T U V W X Y Z A B C D E

G H I J K L M N O P Q R S T U V W X Y Z A B C D E F

H I J K L M N O P Q R S T U V W X Y Z A B C D E F G

I J K L M N O P Q R S T U V W X Y Z A B C D E F G H

J K L M N O P Q R S T U V W X Y Z A B C D E F G H I

K L M N O P Q R S T U V W X Y Z A B C D E F G H I J

L M N O P Q R S T U V W X Y Z A B C D E F G H I J K

M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

The Vigenère chart is simply the alphabet written repeatedly for a total of 26 times, with each new line shifting the alphabet by one letter. You need a key to use the Vigenère system. To illustrate how Vigenère encryption works, here is an example of a plaintext, key, and ciphertext using this method of encryption:

Plaintext Cryptorocks
Key QUEEXAMCRAM
Ciphertext Slctqocqtke

Item	Value
Plaintext	Cryptorocks
Key	QUEEXAMCRAM
Ciphertext	Slctqocqtke

Note that the first letter of the plaintext is C, and the first letter of the key is Q. Compare the natural alphabet to the alphabet arrangement in the encryption/decryption chart that begins with Q:

A B **C** D E F G H I J K L M N O P Q R S T U V W X Y Z
Q R **S** T U V W X Y Z A B C D E F G H I J K L M N O P

You can see that a plaintext C correlates to a ciphertext S. Next, encrypt the second plaintext letter, R, according to the alphabet that starts with the second letter of the key, U:

A B C D E F G H I J K L M N O P Q **R** S T U V W X Y Z

U V W X Y Z A B C D E F G H I J K **L** M N O P Q R S T

Plaintext R becomes ciphertext L. This process continues until the entire plaintext is encrypted. If the key is shorter than the plaintext (as it usually is), you start at the beginning of the key again.

Note that using a different key with the same algorithm would result in a completely different ciphertext.

Tip

The Caesar, ATBASH, and Vigenère ciphers are considered symmetric substitution ciphers that operate by replacing bits, bytes, or characters with alternative bits, bytes, or characters. Substitution ciphers are vulnerable to frequency analysis and are not considered secure.

Substitution ciphers use an encryption method to replace each character or bit of the plaintext message with a different character. The Caesar cipher is a basic example of a substitution cipher. Ciphers can also use transposition, which was the basis of the scytale cipher. Transposition ciphers use algorithms to rearrange the letters of a plaintext message. The result is a ciphertext message. The decryption process reverses the encryption process to retrieve the original message. The transposition cipher is different in that the letters of the original message remain the same, but their positions are scrambled in an ordered way. This can be demonstrated with a simple column array transposition. The letters of the message are written in a rectangular array by rows and then read out by columns. Say that the message is CRYPTO IS MY FAVORITE SUBJECT. The message can be written in a 5 × 5 array as follows:

C R Y P T

O I S M Y

F A V O R

I T E S U

B J E C T

To encrypt the message, each column is processed into the ciphertext:

> COFIB RIATJ YSVEE PMOSC TYRUT

Although it appears complex, a transposition cipher can easily be broken given enough time and resources.

Tip

Modern cryptographic systems do not use simple substitutions or transpositions. However, these substitutions and transpositions are mixed together with other Boolean math operations to create sophisticated algorithms that result in the block and stream ciphers we use today.

History offers many other examples of systems developed to act as codes and ciphers. For example, the *concealment cipher* hides a message inside another message. One concealment cipher works by burying the intended message a word at a time inside an innocuous message. The intended message might be found as every third word in a sentence. A famous example is the letter received by Sir John Trevanion in the 1600s. Sir John was awaiting execution during the English civil war and was eager to escape his captors. The letter stated:

> Worthie Sir John: Hope, that is ye beste comfort of ye afflicted, cannot much, I fear me, help you now. That I would saye to you, is this only: if ever I may be able to requite that I do owe you, stand not upon asking me. 'Tis not much that I can do: but what I can do, bee ye verie sure I wille. I knowe that, if dethe comes, if ordinary men fear it, it frights not you, accounting it for a high honor, to have such a rewarde of your loyalty. Pray yet that you may be spared this soe bitter, cup. I fear not that you will grudge any sufferings; only if bie submission you can turn them away, 'tis the part of a wise man. Tell me, an if you can, to do for you anythinge that you wolde have done. The general goes back on Wednesday. Restinge your servant to command.—R.T.

When the message is divided up and every third letter after a punctuation mark is read, the following message emerges:

> Panel at east end of chapel slides

A similar technique is a book or running key cipher that uses references to pages, paragraphs, or words in a book. The running key cipher is a form of symmetric substitution cipher in which text, typically from a book, is used to provide a very long key stream. Usually, the book or text would need to be agreed to ahead of time. These ciphers don't actually encrypt the message using modern mathematical operations or even scramble the message with older techniques; however, they do hide the message from unintended recipients. A variation of this used to be seen in some computer games. To start the game, you had to input a certain word from a specific page of the game's printed manual. Without the manual, the game could not be started.

Are any ciphers or codes unbreakable? The only known system unbreakable by brute force is a one-time pad called a Vernam cipher. (Think of a brute-force attack as an exhaustive search of all possible keys that could be used in an algorithm in an attempt to decrypt the message.) Gilbert Vernam created the one-time pad in 1917 while investigating methods to potentially improve the polyalphabetic cipher. The one-time pad is a plaintext combined with a random key. This cryptographic system relies on several mechanisms to work correctly:

- The message and the key must be stored securely, and the key must be the same length as or longer than the message.
- The key can be used only once.
- The key must be random.
- The key must be distributed by an out-of-band mechanism. *Out-of-band* means that communications are outside a previously established method of communication.

Tip

Another cryptographic advancement of the twentieth century is the Feistel network. A German-born cryptographer, Horst Feistel, is the creator of this cryptofunction, which is the foundation of many symmetric key block ciphers, such as DES and 3DES. A key feature of the Feistel network is that it uses the well-known round function.

The early twentieth century was dominated by mechanical encryption devices. Some examples include the German *Enigma machine*, which used a series of internal rotors to perform encryption, and the Japanese *Purple Machine*. These devices were developed in an attempt to counter the weaknesses of early substitution ciphers, but both systems were eventually broken. Today, the military, government, industry, and individuals use cryptographic systems. Cryptography is used, for example, by the movie industry for DVD and Blu-ray encryption, by PGP for email and file security, and by IPsec for data transfers.

In the United States, the NSA is responsible for cryptology and the creation and breaking of codes. Cryptography continues to advance; new implementations of cryptography based on light are being created today. This is known as *quantum cryptography*, and it operates by securing optical communications using properties and phenomena of quantum physics.

The Longest-Running Suppressed Patent Application

Although many people are happy just to know enough about cryptographic processes to perform jobs and pass the CISSP exam, William Friedman always wanted to learn more, and he made a career out of cryptography. Friedman, who is considered one of the best cryptologists of all time, holds the record for longest-running suppressed patent—originally requested in 1933 and finally granted in 2001. Friedman did a huge service to the United States by leading the team that broke the Japanese Purple Machine.

Friedman's role in cracking the encryption scheme used by the Japanese Purple Machine helped save lives and aided the Allies in winning World War II. Although Friedman never actually saw one of these devices, he was still able to lead his team in understanding how the device worked and enabled the United States to decrypt many of the messages being sent by the Japanese. Many of Friedman's inventions and cryptographic systems were never patented because they were considered so significant that the release of any information about them might aid an enemy. Much of his work remains secret to this day. Before his death in the 1960s, the NSA went to Friedman's house to retrieve many of his personal writings. After his death, his remaining journals and writings were confiscated by the NSA on grounds of national secrecy.

Voice over IP (VoIP)

Before the year 2000, multimedia services such as voice and video were deployed on stable circuit-switched networks. This guaranteed that the bandwidth and the allowed latency could be controlled. Today, many networks use packet-switching technologies. VoIP involves using a data network to transmit voice communication. VoIP is not a traditional packet-switching protocol but is carried on packet-switched networks in IP packets. Networks configured to carry VoIP treat voice communications as just another form of data. This is one of the big changes in networking that has occurred in recent years. *Network convergence* refers to the provision of telephone (VoIP), streaming video, and network data communication services within a single network. Basically, one pipe is used to transport all forms of communication services.

Quality of service (QoS) is an important concern when discussing VoIP traffic because a portion of a phone call is useless. QoS is the capability of a network to provide dedicated bandwidth and control of jitter and latency. QoS makes it possible for real-time traffic like voice and video to coexist with bursty traffic like HTTP.

VoIP has replaced most of the circuit-switched POTS phone service that was common years ago. There is a good chance that if you still have a home phone, it's actually a VoIP connection. The following are some basic characteristics of VoIP:

- SIP-based signaling
- User-agent client
- User-agent server
- Three-way handshake
- Voice stream carried by RTP

VoIP Vulnerabilities

Companies have moved to VoIP because it offers major cost savings. However, using VoIP is not without risks. As a network service, it is vulnerable in some of the same ways as other data traffic. Attackers can intercept the traffic, hack the VoIP server, or launch DoS attacks against VoIP servers and cause network outages. Attacks against IP phones are also problematic, as are LAN hopping and TFTP alteration for phone firmware image loading. Another consideration is that the vulnerabilities of the operating system the VoIP application is running on are inherited.

One key concern with VoIP is sniffing because protocols like SIP provide little security by default. Without the proper security controls, sniffing a VoIP call can be as easy as using the common network sniffer Wireshark. One security issue related to VoIP is loss of the data network, which can disable VoIP. Other VoIP vulnerabilities include the following:

- **Open network**: After VoIP packets leave an organization's network, the network is not in charge of where they are routed or who might have access to them. Therefore, any unencrypted traffic could potentially be recovered.
- **DoS attacks**: Because VoIP uses UDP for portions of the communication process, it is extremely susceptible to disruption and DoS attacks. VoIP uses an isochronous process in which data must be delivered within strict timelines.

- **Eavesdropping**: Because VoIP relies on UDP and Session Initiation Protocol (SIP), it is an open service, and communications can potentially be sniffed and replayed. Other protocols used by various vendors of VoIP products include IAX, IAX2, SCCP, and UNISTIM.
- **Unauthorized phone use**: Services like Skype and GoogleTalk open a corporate network to exposure to attack and potential policy violations. Such tools can even result in violations of regulation, depending on the industry or how they are used.
- **Spam over Internet Telephony (SPIT)**: SPIT is bulk unsolicited SPAM delivered using VoIP.

Note

You can use Secure Real-Time Transport Protocol (SRTP) to secure VoIP. SRTP uses AES for confidentiality and SHA-1 for integrity.

Cell Phones

Cell phones are another technology that has matured over the years. Cell phone technology can be broadly categorized into the following generations:

- **1G**: This generation of phones enabled users to place analog calls on their cell phones and continue their conversations as they moved seamlessly from cell to cell around an area or a region.
- **2G**: The second generation changed analog mechanisms to digital. Deployed in the 1990s, these phones were based on the technologies GSM (Global System for Mobile Communications) and CDMA (Code-Division Multiple Access).
- **3G**: The third generation saw phones become mobile computers, with fast access to the Internet and additional services. Downstream speeds range from 400 Kbps to several megabits per second.
- **4G**: Fourth-generation cell phones were designed to support TV in real time as well as video downloads at much higher speeds. Two of the most widely deployed 4G standards are Mobile WiMAX and Long Term Evolution (LTE).

- **5G**: The fifth generation of wireless network technology is expected to change the way people live and work. 5G offers connections with average download speeds of around 1 Gbps. 5G architectures are software-defined platforms, in which networking functionality is managed through software rather than hardware.

As of December 2020, most cell providers had migrated to 5G networks. The mobile communication infrastructure throughout the world is growing at an incredible rate, and some might argue that, after the Internet, mobile phones are the second most important invention in globalizing the world.

Table 5.11 lists some common cell phone technologies and the generations to which they correspond.

TABLE 5.11 **Cell Phone Technologies**

Technology	Generation
AMPS	1G
TACS	1G
GSM	2G
CDMA	2G
GPRS	2.5G
EDGE	3G
WWRF	4G
SDN	5G

Most Americans now have cell phones, and very few have landlines. Mobile phones have revolutionized connectivity; however, they have also given rise to security concerns. Organizations must consider what controls to place on these devices.

With so many cell phones in use, there are numerous ways in which attackers can try to exploit their vulnerabilities. One is through the practice of *cloning*. Cell phones have an electronic serial number (ESN) and an International Mobile Station Equipment Identity (IMEI). Attackers can use specialized equipment to capture and decode these numbers from someone's phone and install them in another phone. The attacker then can sell or use the cloned phone.

Tumbling is another technique used to attack cell phones. Specially modified phones tumble and shift to a different pair of ESN/IMEI numbers after each call. This technique makes the attacker's phone appear to be a legitimate roaming cell phone. First-generation cell phones were vulnerable to this type of attack. GSM phones also make use of an International Mobile Subscriber

Identity (IMSI) to identify the user of a cellular network. For example, an IMSI that starts with 310 identifies a user from the United States, whereas an IMSI starting with 460 identifies a user from China.

People who attack phone systems are called *phreakers*.

Note

Phone systems can be targets of caller ID spoofing and SMShing (see https://www.cbsnews.com/news/cell-phones-easy-id-theft-targets/).

Although they are rarely used anymore, cordless phones also have security issues. They are still vulnerable to eavesdropping by someone who has the right equipment.

802.11 Wireless Networks and Standards

The 802.11 family of protocols, which is often called *802.11x*, covers a broad group of wireless standards governed by the IEEE. Most of these wireless devices broadcast by using *spread-spectrum technology*. This method of transmission transmits data over a wide range of radio frequencies. Spread-spectrum technology reduces noise interference and allows data rates to increase and decrease, depending on the quality of the signal. Obstructions like walls, doors, and other solid objects tend to block or reduce signal strength.

The following are the most common spread-spectrum technologies:

- **Orthogonal frequency-division multiplexing (OFDM)**: OFDM splits the signal into smaller subsignals that use a frequency-division multiplexing technique to send different pieces of the data to the receiver on different frequencies simultaneously.

- **Direct-sequence spread spectrum (DSSS)**: This spread-spectrum technology uses a spreading code to simultaneously transmit the signal on a small (22 MHz wide) range of radio frequencies. The wider the spreading code, the more resistant the signal is to interference, but at the cost of a smaller data rate.

- **Frequency-hopping spread spectrum (FHSS)**: FHSS works somewhat differently from OFDM and DSSS in that it works by dividing a broad slice of the bandwidth spectrum into smaller subchannels of about 1 MHz each. The transmitter then hops between subchannels. Each subchannel is used to send out short bursts of data for a short period, called the *dwell time*. For devices to communicate, each must know the proper dwell time and must be synchronized to the proper hopping pattern.

Table 5.12 summarizes the primary standards for wireless LANs (WLANs).

TABLE 5.12 **WLAN Standards and Details**

Service	Frequency	Transmission Scheme
802.11a	5 GHz	OFDM
802.11b	2.4 GHz	DSSS
802.11g	2.4 GHz	OFDM/DSSS
802.11n	2.4 GHz or 5 GHz	MIMO-OFDM
802.11ac	2.4 GHz or 5 GHz	MIMO-OFDM

ExamAlert

For the CISSP exam, you must know WLAN standards, speeds, and transmission schemes.

Other devices beyond wireless access points and equipment can pose threats to an organization. All wireless devices should have enforced security and strong policies dictating their use. Smartphones and tablets allow users to take photos in otherwise secure areas. In addition, these devices can be easily lost or stolen, and a number of forensic tools are available to extract data from these types of wireless devices. Portable wireless devices can also support onboard removable storage that can be lost or removed. It's unfortunate, but these devices usually lack the level of security of wired devices. Corporate security officers must understand that the default wiping options for many modern devices do not remove all stored data.

Wireless Topologies

Wireless networks can operate in either ad hoc mode or infrastructure mode. *Ad hoc mode*, or *peer-to-peer mode*, doesn't require any equipment except wireless network adapters. Ad hoc mode allows a point-to-point type of communication that works well for the temporary exchange of information. *Infrastructure mode* centers around a wireless access point (AP). A wireless AP is a centralized wireless device that controls the traffic in the wireless medium. Wireless devices use CSMA/CA to communicate efficiently. 802.11 wireless NICs can operate in four modes:

- **Managed**: This mode is the most generic wireless option. Clients communicate only with the access point and do not directly communicate with other clients.

- **Master**: Wireless access points use this mode to communicate with connected clients in managed mode.
- **Ad hoc**: This mode is a peer-to-peer mode with no central access point.
- **Monitor**: This mode is a read-only mode used for sniffing WLANs. Wireless sniffing tools such as Kismet use monitor mode to sniff 802.11 wireless frames.

Wireless Standards

The standard for WLANs is IEEE 802.11, commonly called *Wi-Fi*. Some of the important amendments to this standard include the following:

- **802.11a**: This amendment defines physical access that can operate in the 5 GHz frequency range and support speeds up to 54 Mbps at a range of 60 feet.
- **802.11b**: This amendment defines physical access that can operate in the 2.4 GHz frequency range and can reach speeds of up to 11 Mbps and ranges of 300 feet.
- **802.11g**: This amendment defines physical access that can operate in the 2.4 GHz frequency range and support speeds up to 54 Mbps.
- **802.11i**: This amendment provides for secure authentication and encryption that permanently replaces the deficient Wired Equivalent Privacy (WEP) mechanism. 802.11i also makes use of Robust Security Network (RSN), which uses pluggable authentication modules, allowing for changes to cryptographic ciphers as new vulnerabilities are discovered.
- **802.11ac**: This wireless networking standard includes multistation WLAN throughput of at least 1 Gbps and single-link throughput of at least 500 Mbps.
- **802.11n**: This amendment defines wireless access that operates in the 2.4 GHz frequency. Data rates can exceed 200 Mbps.
- **802.16**: This broadband wireless access standard, also known as WiMAX, was designed to deliver last-mile connectivity to broadband users at speeds of up to 75 Mbps.

Table 5.13 summarizes the primary standards for wireless LANs (WLANs).

TABLE 5.13 **Some Common WLAN Speeds and Frequencies**

Standard	Top Speed (Mbps)	Frequency (GHz)
802.11	2	2.4
802.11a	54	5
802.11b	11	2.4
802.11g	54	2.4
802.11n	144+	2.4 and/or 5

The IEEE has written standards in support of other wireless technologies as well. For example, 802.15 defines the use of Bluetooth and RFID (radio frequency identification) for wireless PANs (WPANs).

Bluetooth

Bluetooth technology is designed for short-range wireless communication between mobile and handheld devices. Bluetooth started to grow in popularity in the mid- to late 1990s. Versions include 1.2, 2, 3, and 4. Bluetooth technology has facilitated the growth of a variety of personal and handheld electronic devices. For example, in a WPAN, Bluetooth enables a smartphone to communicate with a tablet and a laptop when these devices come in range of each other or are activated. The classifications of Bluetooth are as follows:

- **Class 1**: This classification has the longest range (up to 100 m) and offers 100 mW of power.
- **Class 2**: Although this classification is not the most popular, it allows transmission of up to 20 m and offers 2.5 mW of power.
- **Class 3**: This is the most widely implemented classification. It supports a transmission distance of 10 m and offers 1 mW of power.
- **Class 4**: This classification supports a transmission distance of 0.5 m and offers 0.5 mW of power.

Note

Although you have undoubtedly heard of Bluetooth, you might not have heard of Zigbee. It’s another wireless standard that is designed for low data rates, can operate for many years, and is well suited for smart home applications such as controlling lights, transferring data from an electrical power meter, and sending temperature data to a thermostat.

Although Bluetooth does have some built-in security features, it has been shown to be vulnerable to attack. At a recent DEFCON security conference, security professionals demonstrated ways to sniff Bluetooth transmissions from up to a kilometer away.

Bluetooth is part of the IEEE 802.15 family of protocols designed for WPANs. Although Bluetooth is extremely popular, competing 802.15 technologies, such as wireless USB and infrared, diversify the market.

Note

Bluejacking involves the unsolicited delivery of data to a Bluetooth user. *Bluesnarfing* is theft of data or information from a user. *BlueBorne* is a buffer overflow attack that provides the attacker with access to a device.

Wireless LAN Components

Wireless LANs include the following components:

- **Service set ID (SSID)**: For a computer to communicate or use a WLAN, it must be configured to use the WLAN's SSID, which distinguishes the wireless network from others.
- **Wireless access point**: A wireless access point is a centralized wireless device that controls the traffic in the wireless medium and can be used to connect wireless devices to a wired network.
- **Wireless networking cards**: These cards are used to connect devices to a wireless network.
- **Encryption**: 802.11 encryption was originally provided by the aging protocol WEP, which was intended to provide the same level of privacy that a user might have on a wired network. WEP used RC4 symmetric encryption, but it was a flawed implementation. The 802.11i amendment offers secure replacements for WEP: Wi-Fi Protected Access (WPA, which uses RC4) and WPA2 (which uses AES). These encryption mechanisms are discussed in detail in the next section.

In North America, 802.11 supports bandwidth of 2.4 GHz for 11 channels, 3 of which (1, 6, and 11) can be used simultaneously as non-overlapping. The channel designates the frequency on which the network will operate. European units support 13 channels (up to 4 of them non-overlapping), and Japanese units support 14 channels. At 5 GHz, there are 24 non-overlapping channels.

Worldwide, frequency availability differs depending on the pertinent licensing authority. Equipment adjusts to different demands by asking what country the installation is occurring in and either adjusting the frequencies to the local authority or terminating transmissions (according to the licenses that the vendor is granted). The 802.11d amendment enables client equipment to ask what country it finds itself in and dynamically adjust its frequencies.

Note

Two very basic wireless security precautions are MAC address filtering and SSID filtering. Both provide only limited security as MAC addresses are transmitted in plaintext and thus can be easily sniffed. Setting SSIDs to non-broadcast is also a poor security strategy because wireless sniffers such as Kismet can detect non-broadcast SSIDs used by clients to bypass this weak control.

Wireless Protection Mechanisms

The original technology used to protect wireless communications was WEP. WEP is implemented at the data link layer and encrypts data by using the RC4 encryption algorithm. The key was limited to 40 bits because of export rules that existed during the late 1990s, when the 802.11 protocol was developed. This is considered a very weak key today.

The RC4 algorithm used either a 64-bit (IEEE standard) or a 128-bit (commercial enhancement) key. However, the keys can't use that many bits because a 24-bit initialization vector (IV) was used to provide randomness. Therefore, the real WEP key is actually 40 or 104 bits long. Many people are reluctant to learn about such an old and broken technology as WEP; however, it is important to appreciate that WEP is still with us.

WEP is a *static* mechanism because everyone has the same key. Two of the first weaknesses realized about WEP are that this static encryption key was the same key being used for the Shared Key Authentication (SKA), and the authentication used a challenge-handshake mechanism that was dictionary crackable. The immediate solution was to throw away SKA and use only Open System Authentication (OSA) and the WEP encryption key. That way, everyone could connect, but no one could communicate without the encryption key.

One way the industry responded to these potential issues was by incorporating 802.1X (port-based access) into many wireless devices. When used in conjunction with Extensible Authentication Protocol (EAP), 802.1X can be used to authenticate devices that attempt to connect to a specific LAN port. Although it was an improvement over WEP, 802.1X has been shown to be vulnerable.

To better understand the WEP process, you need to understand how the exclusive-or (XOR) function works in Boolean logic. Specifically, XOR means exclusively or, which is a simple binary comparison between two bits that produces another bit as the result. When the two bits are compared, XOR looks to see whether they are different. If the answer is yes, the resulting output is a 1. If the two bits are the same, the result is a 0. Seven steps are involved in encrypting a message:

1. The transmitting and receiving stations are initialized with the secret key. This secret key must be distributed using an out-of-band mechanism such as by being emailed, posted on a website, or given to someone on a piece of paper (as a Wi-Fi key is provided in a hotel).

2. The transmitting station produces a seed, which is obtained by appending the 40-bit secret key to the 24-bit IV, for input into a pseudorandom number generator (PRNG).

3. The transmitting station uses the secret key and a 24-bit IV as input into the WEP PRNG to generate a key stream of random bits.

4. The key stream is XORed with plaintext to obtain the ciphertext.

5. The transmitting station appends the ciphertext to a copy of the IV for the receiver to use and sets a bit in the header to indicate that the packet is WEP encrypted, and the WEP frame is transmitted. Because WEP encrypts at Layer 2 of the OSI model, the Layer 2 header and trailer are sent in plaintext.

6. The receiving station checks whether the encrypted bit of the frame it received is set. If it is, the receiving station extracts the IV from the frame and inputs it and the secret key into its WEP PRNG.

7. The receiver generates the same key stream used by the transmitting station and XORs it with the ciphertext to obtain the plaintext that was sent.

WEP's immediate successor was a stopgap measure that was popularized as *Wi-Fi Protected Access* (*WPA*). WPA certification meant that a piece of hardware was compliant with a snapshot of the 802.11i amendment (which was still under design at the time WPA was created). One of the jobs of the 802.11i working group was to reverse engineer WEP and develop a software-only upgrade for wireless users that would deploy Temporal Key Integrity Protocol (TKIP) for encryption. TKIP uses a mixing algorithm to scramble the user key with network state information and adds an integrity-checking feature (that is much stronger than the WEP mechanism) to verify that the frames haven't been tampered with. WPA certification tested equipment for the implementation of TKIP.

In 2004, the IEEE completed the 802.11i amendment and released Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), an AES solution, as a complete replacement for the outdated RC4 mechanism used in WEP and TKIP. CCMP is also tested for and certified by the Wi-Fi Alliance and is recognized as *WPA2*. WPA2 can use key sizes of up to 256 bits, which is a vast improvement over the original 40-bit encryption WEP used.

Keep in mind that in the IT security field, nothing remains static. Additional tools and techniques continue to be developed to attack newer security mechanisms. coWPAtty is one such tool.

Note

War driving is the practice of driving around, finding, mapping, and possibly connecting to open wireless networks. War drivers use tools such as NetStumbler, Kismet, and AirSnort.

War chalking is the practice of marking the locations and statuses of wireless networks. The practice can be traced to a system hobos used during the Depression to mark the locations of food and work.

Other Wireless Technologies

As technology continues to change, a number of standards are emerging. One example is *i-mode*, a packet-based service for mobile phones that is used in Japan. Another is Digital Enhanced Cordless Telecommunication (DECT), a technology widely used for cordless phones outside the United States. DECT allows handsets and base units from different manufacturers to work together.

Another standard you should know is Wireless Application Protocol (WAP). WAP is an open standard that enables cell phone users to get the same types of content available to desktop and laptop users. A WAP-enabled device customizes the content of a website to work with the small screen size of a mobile phone. A key component of this technology is Wireless Markup Language (WML). Security issues in WAPv1 have been fixed in WAPv2. Anyone considering the use of WAP for sensitive information exchange should understand these issues. WAP, which was created by the WAP Forum, was an attempt to rewrite the upper layers of the OSI model to minimize the overhead of a mini-browser inside a cell phone. The WAP Forum created its own encryption protocol called WTLS, which was based on Transport Layer Security (TLS). When a client's signal reached the ISP's gateway, the WTLS packet had to be decrypted from WTLS to re-encapsulate it as a TLS signal and then to send it on to the Internet. This was a vulnerable moment, during which data was fully decrypted, and it became known as the *GAP in WAP* (see Figure 5.16). WAP2 has been rewritten as an abbreviated form of TLS instead of WTLS, and the packet no longer needs to be decrypted.

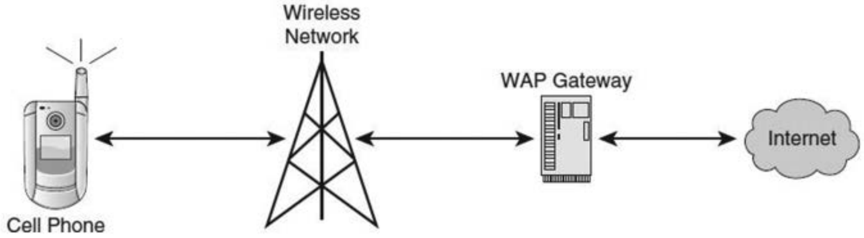


FIGURE 5.16 **WAP Gateway**

Securing TCP/IP with Cryptographic Solutions

It is best to have the option of security in all the layers of a network. Cryptography can be layered to help build *defense in depth*. This is not to say that cryptographic controls should be applied at every layer, just that defense in depth should be the target. Too many layers of cryptography will slow down a system or process, and users might look for ways to bypass some of these controls. Many types of cryptographic solutions are available, from the application layer all the way down to the physical frame. Your job as a security professional is to understand these potential solutions and be able to determine which of them should be used to meet the goals of the organization.

Because security wasn't one of the driving forces when the TCP/IP protocols were developed, the cryptographic solutions discussed here can go a long way toward protecting the security of an organization. Although in reality encryption at any layer is accomplished on the payload of the next higher layer, most CISSP exam questions will focus on basic knowledge of encryption processes and the layers at which they are found. Figure 5.17 shows some common cryptographic solutions and their corresponding layers. The following sections start at the top of the stack and work down through the layers.

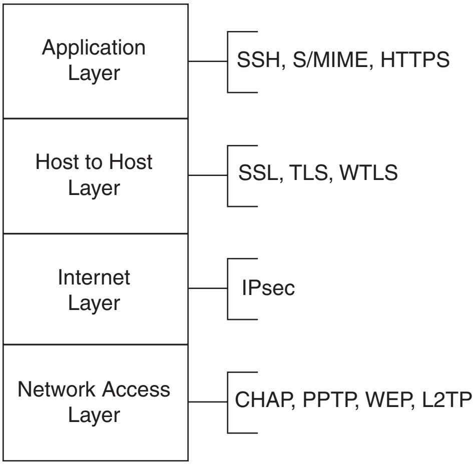


FIGURE 5.17 **Layered Security Controls**

Application/Process Layer Controls

The following application-layer protocols can be used to add confidentiality, integrity, or nonrepudiation to a network:

- **Secure Shell (SSH)**: SSH is an Internet protocol that provides secure remote access. It is considered a replacement for FTP, Telnet, and the Berkley "r" utilities. SSH defaults to TCP port 22. SSH Version 1 has been found to contain vulnerabilities, so it is advisable to use SSHv2.

- **Secure FTP (SFTP)**: SFTP uses an SSH connection and then tunnels FTP through SSH. The latest version of SSH, is Version 2.0, which typically runs on TCP port 22. SFTP can be used only if the FTP client software supports it.

- **FTP Secure (FTPS)**: FTPS establishes an SSL secure channel and then runs the FTP session through SSL. IANA assigned ports 989 (data) and 990 (control) for FTPS, but vendors are free to use custom port numbers and often do.

- **Secure Hypertext Transfer Protocol (S-HTTP)**: S-HTTP is a modification of HTTP that was developed to provide secure communication with a web server. S-HTTP is a connectionless protocol designed to send individual messages securely.

- **Secure Electronic Transaction (SET)**: Visa and MasterCard wanted to alleviate fears related to using credit cards over the Internet, so they developed the SET specification, which uses a combination of digital certificates and digital signatures among the buyer, merchant, and the bank to ensure privacy and confidentiality. While this sounds like a great idea, one of the problems with SET was that the banks wanted to charge for this service and required hardware and software changes. Many vendors fought these fees, and so SET is not widely used. Out of the ashes of SET came the Payment Card Industry Data Security Standard (PCI-DSS). PCI-DSS requires all vendors who accept credit cards to meet and guarantee specific information system security standards designed to protect the credit card data.

Host-to-Host Layer Controls

The host-to-host layer of the TCP/IP stack can be used to add cryptographic solutions to data communications. Some common examples follow:

- **Secure Sockets Layer (SSL)**: SSL was developed by Netscape for transmitting private documents over the Internet. Unlike S-HTTP, SSL is application independent. One of the advantages of SSL is its cryptographic independence. The protocol itself is merely a framework for communicating certificates, encrypted keys, and data. The most current version of SSL is SSLv3, which provides for mutual authentication and compression. Figure 5.18 illustrates the transactions in an SSL session. SSLv3 is considered insecure and is vulnerable to the POODLE exploit. If attackers successfully exploit this vulnerability, they only need to make about 256 SSLv3 requests to break the encryption. TLS 1.2 is the current standard for HTTP encryption.

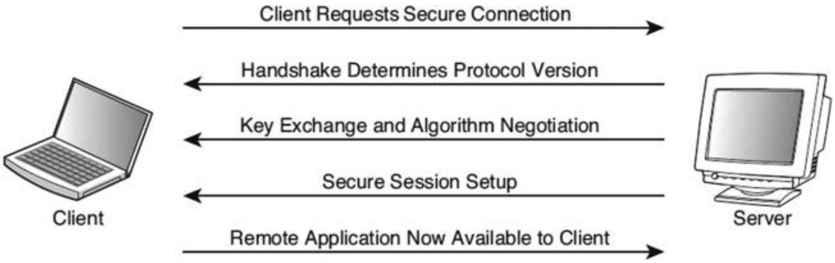

Client Requests Secure Connection
Handshake Determines Protocol Version
Key Exchange and Algorithm Negotiation
Secure Session Setup
Remote Application Now Available to Client
Client
Server

FIGURE 5.18 Secure Sockets Layer (SSL)

- **Transport Layer Security (TLS)**: TLS encrypts the communication between a host and a client. TLS typically makes use of an X.509 digital certificate for server authentication. This mechanism provides strong authentication of the server to the client, so the client can trust that it is connected to the correct remote system. TLS consists of two layers: TLS Record Protocol and TLS Handshake Protocol. One of the most common implementations of TLS is HTTPS, which is simply HTTP over TLS.

- **Secure Socket Tunneling Protocol (SSTP)**: SSTP is a form of VPN tunnel that was released in 2008 and provides a mechanism to transport PPP or L2TP traffic through an SSLv3 connection. SSTP requires a digital certificate on the server side and establishes an SSL tunnel that encrypts all traffic over TCP port 443. Because it uses the same port used by HTTPS, it can be used through corporate firewalls.
- **Wireless Transport Layer Security (WTLS)**: WTLS is a security protocol developed for cellular technology. In an attempt to minimize upper-layer support code, the cellular industry developed its own Wireless Application Protocol (WAP) stack. WTLS encrypts the communication between the cellular wireless client and the ISP tower that the cell phone is connecting to. At the tower, the WTLS packet is decrypted, and then it is re-encrypted with standard TLS and routed on to the Internet. This means that customer data exists unencrypted for a moment. This is a security vulnerability that has become known as the *gap in WAP*. The cellular industry has since released WAPv2, which incorporates industry-standard TLS so that decryption is no longer necessary.

Internet Layer Controls

Internet Protocol Security (*IPsec*) resides at the Internet layer and is a well-known cryptographic solution. IPsec is an end-to-end security technology that allows two devices to communicate securely. IPsec was developed to address the shortcomings of IPv4. Although it is an add-on for IPv4, it was created for and is built into IPv6. IPsec can be used to protect just the data or the data and the original IP header. This level of protection can provide integrity and/or encryption. (IPsec is covered in more detail later in this chapter.)

Two less frequently used cryptographic solutions are found at the Internet layer:

- **Simple Key-Management for Internet Protocol (SKIP)**: SKIP, which was developed by the IETF, is rarely used and requires no prior communication; it is similar to SSL. SKIP was evaluated as a key exchange mechanism for IPsec before the adoption of IKE in 1998.

- **Software IP Encryption (swIPe)**: swIPe was an early attempt to develop an open standard for VPNs. Although freely available, it was available only for SunOS and is not widely used.

Network Access Layer Controls

Several cryptographic solutions are available at the TCP/IP network access layer or Layer 2 of the OSI model:

- **Point-to-Point Tunneling Protocol (PPTP)**: PPTP, which was developed by a group of vendors, consists of two components: transport, which maintains the virtual connection, and encryption, which ensures confidentiality. It can operate at a 40-bit or 128-bit key length.
- **Layer 2 Tunneling Protocol (L2TP)**: L2TP was created by Cisco and Microsoft to replace L2F and PPTP. L2TP merged the capabilities of L2F and PPTP into one tunneling protocol. By itself, it provides no encryption, but it is deployed with IPsec as a VPN solution.

> Note
>
> L2F does not provide encryption or confidentiality by itself; it relies on the protocol being tunneled to provide privacy.

- **WPA2 Enterprise**: This Wi-Fi Alliance certification identifies equipment capable of establishing a secure channel of communication at TCP/IP Layer 1/OSI Layer 2 using EAP for authentication and AES-CTR-CBC-MAC for encryption. Cisco LEAP can be used with WPA and WPA2 networks.

> Note
>
> Extensible Authentication Protocol (EAP) is an authentication protocol that is widely used in point-to-point and wireless connections. It is discussed in more detail later in the chapter.

Link and End-to-End Encryption

As you can tell based on the various protocols discussed so far, there are many ways to encrypt and secure data. One final decision that must be considered is how information is to be moved between clients. In reality, encryption can happen at any one of many different layers. The important question is: What is actually getting encrypted? The layer at which you choose to encrypt forces encryption of all layers above your chosen layer.

End-to-end encryption encrypts the message and the data packet. Header information, IP addresses, and routing data are left in plaintext. Although this means that a malicious individual can intercept packets and learn the source and target destination, the data itself is secure. The advantage of this type of encryption is speed. No time or processing power is needed to decode address information at any intermediate points. The disadvantage is that even with the data encrypted, an attacker might be able to make an *inference attack*.

Sending information by means of end-to-end encryption prevents the attacker from sniffing host-to-host or application data, but it does not mean the attacker cannot understand something about the actual communication. The attacker may observe activity and make *inferences* about the traffic. Inference is possible any time an attacker notices a change in activity at a client. For example, some news agencies allegedly monitor the White House for pizza deliveries. They infer that when a spike in pizza deliveries occurs, officials are working overtime, and there is a pending event of importance. Similarly, a spike in encrypted email traffic could allow an attacker to make similar inferences.

Traffic padding can be used to defeat an inference attack. For example, a military agency could have a connection between the United States and Afghanistan. Although third parties might be able to see that traffic is flowing, the amount of traffic transmitted maintains a constant flow and thereby prevents attackers from performing an inference attack.

Your choice for encryption at the physical for the encryption available at the physical layer is *link-to-link encryption*, which encrypts all the data sent from a specific communication device to another specific device. This includes the headers, addresses, and routing information. The primary strength of this type of encryption is that it provides added protection against sniffers and eavesdropping. The disadvantage is that all intermediate devices must have the keys, software, and algorithms necessary to encrypt and decrypt the encrypted packets at each hop along the trip. This adds complexity, consumes time, and requires additional processing power.

Network Access Control Devices

Security should be implemented in layers to erect multiple barriers against attackers. One good example of a network access control is a firewall. The firewall can act as a choke point to control traffic as it ingresses and egresses the network. Another network access control is a DMZ (demilitarized zone), which establishes a safe zone for internal and external users to work. The sections that follow describe these network security devices and techniques in more detail.

Firewalls

The term *firewall* has been used since the 1990s to describe hardware or software that guards the entrance to a private network. Firewalls were developed to keep unauthorized traffic out. Firewalls have undergone generations of improvements, and today several different types of firewalls exist, including packet filters, application proxies, circuit proxies, and stateful inspection.

It's a sad fact that we need firewalls. Just as in the real world, on networks, some individuals enjoy destroying other people's property. A firewall is a computer, a router, or a software component implemented to control access to a protected network. It enables an organization to protect its network and control traffic. Remember that the models addressed here, such as stateful inspection and proxies, are theoretical, and most vendor products do not match one design perfectly.

Packet Filters

Packet filters are devices that filter traffic based on IP addresses. Savvy hackers use spoofing tools and other programs that are easily available on the Internet to bypass packet filters. The first firewalls ever implemented were packet filters. These devices inspect the TCP/IP headers and make decisions based on a set of predefined rules. Packet filters simply drop packets that do not conform to the predefined rule set. These devices are considered stateless. Packet filters are based on access control lists (ACLs), which can deny or permit packet transmission based on IP addresses, protocol types, TCP ports, and UDP ports.

Stateful Firewalls

Stateful firewalls keep track of every communication channel by means of a state table. They are considered intelligent firewalls and are part of the third generation of firewall design. Packet filters do not have this capability.

Proxy Servers

By definition, the word *proxy* means "agency or power to act for another." An Internet proxy is a hardware or software device that can perform address translation and that communicates with the Internet on behalf of the network. The real IP address of the user remains hidden behind the proxy server. The proxy server can also be configured to filter higher-layer traffic to determine whether the traffic is allowed to pass. Proxy servers offer increased security because they don't allow untrusted systems to have direct connections to internal computers. Proxy servers function as follows:

1. A proxy server accepts packets from an external network.
2. It copies the packets.
3. It inspects the packets for irregularities.
4. It changes the address on packets to the address of the correct internal device.
5. It puts the packets back on the wire to the destination device.

There are a number of types of proxies, including the following:

- **Application-level proxy**: Not all proxies are made the same. An application-level proxy inspects an entire packet and then makes a decision based on what it discovered while inspecting the contents. This method is very thorough and slow. For an application-level proxy to work correctly, it must understand the protocols and applications it is working with.
- **Circuit-level proxy**: A circuit-level proxy closely resembles a packet-filtering device in that it makes decisions based on addresses, ports, and protocols. It does not care about higher-layer applications, so it works for a wider range of protocols but doesn't provide the depth of security that an application-level proxy does. Squid is an example of an open-source proxy. Table 5.14 summarizes the primary differences between application- and circuit-level proxies.

TABLE 5.14 **Application- and Circuit-Level Proxies**

Application-Level Proxy	Circuit-Level Proxy
Each protocol must have a unique proxy	Does not require a proxy for every protocol
Slower than a circuit-level proxy	Faster than an application-level proxy
Requires more processing per packet	Does not provide deep packet inspection
Provides more protection	Is acceptable for a wide range of protocols

Caution

An application-level proxy provides a high level of security and offers a very granular level of control. Its disadvantages include the possibility that it could break some applications and that it can be a performance bottleneck.

- **SOCKS**: SOCKS takes the proxy servers concept to the next level. SOCKS must be deployed as a client/server solution. It provides a secure channel between two devices and examines individual applications to determine whether they are allowed access. Common SOCKS applications include the following:
    - **FTP**: Blocks or allows files to be transferred into or out of the network
    - **HTTP**: Blocks or allows Internet access
    - **SMTP**: Blocks or allows email

Note

One type of proxy that is widely used today is a content delivery network (CDN). A CDN provides low-latency performance and a high-availability way to host content. The purpose of a CDN is to minimize the distance between a visitor and a website's server. A CDN stores a cached version of its content in multiple geographic locations to reduce latency.

Demilitarized Zone (DMZ)

In the computer world, a DMZ prevents outsiders from getting direct access to internal services. A DMZ is typically set up to allow external users access to services within the DMZ. Basically, shared services like Internet, email, and DNS might be placed within a DMZ. The DMZ provides no other access to services located within the internal network. If an attacker is able to penetrate and hack computers within the DMZ, no internal computers should be accessible (as long as no internal machines trust these DMZ computers). Usually the computers placed in the DMZ are *bastion hosts*, or computers that have had all unnecessary services and applications removed in order to be hardened against attack. To add security to the devices in the DMZ, a screened host is sometimes used. A *screened host* is a firewall that is partially shielded by a router acting as a packet filter. This provides a good example of the concept of defense in depth.

Note

Zero trust is another defense-in-depth technique. The idea is to remove the concept of trust from the network architecture. Zero trust is based on the principle of never trusting but treating all traffic, including traffic already inside the perimeter, as hostile. Only if workloads have been identified by a set of attributes as trusted are they allowed to communicate; otherwise, by default they are not trusted.

Network Address Translation (NAT)

Network Address Translation (*NAT*) was originally developed because the explosive growth of the Internet and the increase in home and business networks meant that the number of available public IP addresses quickly became insufficient to support everyone. NAT allows a single device, such as a router, to act as an agent between the Internet and the local network. This device or router provides a pool of addresses for use by the local network. Only a single, unique IP address is required to represent this entire group of computers. The outside world is unaware of this division and thinks that only one computer is connected. NAT can provide a limited amount of security because it can hide internal addresses from external systems. When private addressing is used, NAT is a requirement because packets with private IP addresses cannot be routed to external IP addresses, and external traffic cannot be routed into a network that has NAT applied. RFC 1918 defines three ranges of private addresses: 10.0.0.0–10.255.255.255, 172.16.0.0–172.31.255.255, and 192.168.0.0–192.168.255.255.

NAT is available in several forms:

- **Static NAT**: Static NAT uses a one-to-one mapping between public and private IP addresses.
- **Dynamic NAT**: Dynamic NAT uses a pool of public addresses. When an internal device needs Internet connectivity, it is mapped to the next available public address. When the communication session is complete, the public address is returned to the pool.
- **Port Address Translation (PAT)**: Most home networks using DSL or cable modems use this type of NAT. PAT is designed to provide many internal users Internet access through one external address.

Remote Access

Well-designed networks require authentication and access control. Users might be internal to an organization or in a hotel on the road. Being outside the organization raises concerns in addition to proper authentication, such as confidentiality and privacy. This section discusses an array of topics related to remote access, including Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), VPNs, and IPsec.

Point-to-Point Protocol (PPP)

PPP is the most commonly used protocol for dialup connections. It can run on a line of any speed, from POTS to T1. Developed in 1994 by the IETF, PPP is a replacement for Serial Line IP (SLIP). SLIP is capable of carrying only IP and had no error detection, whereas PPP supports many types of authentication, including PAP, CHAP, and EAP.

Password Authentication Protocol (PAP)

PAP uses a two-way handshake to authenticate a client to a server when a link is initially established. PAP sends a password in plaintext, which makes it highly vulnerable to sniffing attacks.

Challenge Handshake Authentication Protocol (CHAP)

CHAP is an improved version of PAP. It uses a four-way handshake to authenticate the client. CHAPv2 provides for mutual authentication. When a client requests authentication, the server sends the client a challenge. The client hashes the challenge with its password and returns it to the server. This hashed value is compared on the server with a hash that the server created. Although no plaintext ever crosses the network, anyone who knows the hashing functions and who captures the exchange can use a dictionary attack in an attempt to defeat the mechanism. CHAP was specifically created to defeat replay attacks because the challenge would vary with each client request, and reauthentication could be periodically demanded by the server.

Extensible Authentication Protocol (EAP)

EAP makes PPP more robust by adding the capability to implement a variety of authentication mechanisms, including digital certificates, token cards, and

MD5-Challenge-Response. EAP is used with 802.1X and implemented in amendments, such as 802.11i, WPA Enterprise, and WPA2 Enterprise.

When EAP is used by wireless devices to authenticate end users or devices, the client (supplicant) initiates the EAP request to the wireless access point (authenticator) that is responsible for keeping the network port closed until the authentication process completes successfully. The authenticator becomes a proxy, forwarding requests and replies between the supplicant and the authenticating server (RADIUS, TACACS+, and so on). During this protected series of frames, usually inside an encrypted tunnel, a *pairwise master key* (*PMK*) is developed between the supplicant and the authenticating server. If the authentication exchange is successful, the authenticating server delivers the PMK to the access point. The PMK is used to develop transient AES or TKIP encryption keys for the duration of the client's session.

Table 5.15 summarizes some of the types of EAP.

TABLE 5.15 **EAP Types**

EAP Type	Security Status	Description
EAP-LEAP	Weak	LEAP (Lightweight Extensible Authentication Protocol) is a Cisco-proprietary protocol released before 802.1X was finalized. LEAP has significant security flaws and should not be used.
EAP-MD5	Weak	This is a weak form of EAP. It offers client-to-server authentication only and is vulnerable to man-in-the-middle attacks and password-cracking attacks.
EAP-PEAP	Better	Protected EAP (PEAP), which was developed by Cisco Systems, Microsoft, and RSA Security, is similar to EAP-TTLS. It does not require client-side certificates.
EAP-TTLS	Better	EAP Tunneled Transport Layer Security (EAP-TTLS) does not use a client-side certificate, allowing other authentication methods (such as passwords) for client-side authentication. EAP-TTLS is thus easier to deploy than EAP-TLS, but it is less secure when omitting the client-side certificate.
EAP-SIM	Better	EAP Subscriber Identity Module (EAP-SIM) is used for authentication and session key distribution for mobile phones using GSM.
EAP-FAST	Better	EAP Flexible Authentication via Secure Tunneling (FAST) was designed by Cisco to replace LEAP. It uses a Protected Access Credential (PAC), which acts as a pre-shared key.

ExamAlert

Although EAP-TLS is one of the most secure and most costly forms of EAP, EAP can be implemented in many different ways. Some methods include EAP-MD5, EAP-TLS, EAP-SIM, LEAP, and EAP-TTLS. Although EAP-MD5 is not appropriate for use by itself (because it is a simple hash), and LEAP is dictionary-crackable, the other EAP types are robust. You do not need to memorize the details of all the EAP types, but you do need to be able to select the appropriate protocol, depending on the policy established for authentication strength.

Remote Authentication Dial-in User Service (RADIUS)

RADIUS was designed to support dialup users and originally used a modem pool to connect to an organization's network. Because of the features RADIUS offers, it is now used for more than just dialup users. Enterasys uses it for secure network products, and 802.1X/EAP also uses it widely.

A RADIUS server contains usernames, passwords, and other information to validate the user (supplicant). A *supplicant* is a client machine that wants to gain access to the network. RADIUS is a well-known UDP-based authentication and accountability protocol. Information is passed to the NAS, which is the RADIUS client. The RADIUS client then forwards the information to the RADIUS server to be authenticated. Traffic from the RADIUS client to the RADIUS server typically protects the password by means of a shared secret.

RADIUS has improved with the IETF's approval of Diameter, and it continues to be the most widely deployed AAA (authentication, authorization, and accountability) server protocol.

Terminal Access Controller Access Control System (TACACS)

TACACS is an access-control protocol used to authenticate a user logging on to a network. TACACS is a UDP-based protocol that provides authentication, authorization, and accountability. It was originally used in Cisco devices.

TACACS is very similar to RADIUS. When TACACS receives an authentication request, it forwards the received username and password to a central database. This database verifies the information received and returns it to TACACS to allow or deny access based on the results. The fundamental reason TACACS did not become popular is because TACACS is a proprietary solution from Cisco, and its use would require the payment of royalties.

TACACS+ is a completely new rewrite of the TACACS protocol that separates authentication and authorization. TACACS+ is not compatible with TACACS. TACACS+ is TCP based and offers extended two-factor authentication. When most people today say “TACACS,” they really mean TACACS+.

Internet Protocol Security (IPsec)

IPsec was developed to provide security for IP packets. Without IPsec, someone could capture, read, or change the contents of data packets and then send them back to the unsuspecting target. The current version of IP, IPv4, supports IPsec as an add-on; IPv6 has IPsec built in. IPsec offers its users several levels of cryptographic security:

- **Authentication header (AH)**: The AH protects data against modification but does not provide privacy. The AH uses a hashing algorithm and symmetric key to calculate a message authentication code known as the integrity check value (ICV). When the AH is received, an ICV is calculated and checked against the received value to verify integrity.
- **Encapsulating Security Payload (ESP)**: ESP provides privacy and protects against malicious modification. ESP provides confidentiality by encrypting the data packet. The encrypted data is hidden from prying eyes, so its confidentiality is ensured.
- **Oakley protocol**: Oakley is a portion of IKE that is responsible for carrying out the negotiations.
- **Security association (SA)**: For AH and ESP to work, there must be some negotiations regarding the rules of conduct for exchanging information between the client and server. These negotiations include the type of symmetric and asymmetric algorithms that will be used, as well as state-specific information in support of the secure channel. The results of these negotiations are stored in an SA. The SA identifies the details of each one-way connection. Two-way communication channels have two SAs, each distinguished by its *Security Parameter Index* (*SPI*). If both AH and ESP are used, four SAs are required. IPsec uses a symmetric shared key to encrypt bulk communications. The Diffie-Hellman algorithm is the key agreement protocol used to generate this shared key.
- **Internet Key Exchange (IKE)**: IKE allows secret keys to be exchanged securely before communications begin. IKE is responsible for creating IPsec’s SA and is considered a hybrid protocol because it combines the functions of two other protocols: Internet Security Association and Key Management Protocol (ISAKMP) and Oakley.

Key exchange must be handled securely. IPsec uses ISAKMP. It is defined by RFC 2408 and is used for establishing SAs and cryptographic keys in an Internet environment. Basically, IPsec defines procedures and formats to establish, negotiate, modify, and delete SAs, and it defines payloads for exchanging key generation and authentication data. Each has an IP protocol number; ESP is protocol 50, and AH is protocol 51. Because IPsec is applied at Layer 3 of the OSI model, any layer above Layer 3 can use it transparently. Other Internet security systems in widespread use, such as Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers of the OSI model. IPsec has two modes of operation:

- **Transport mode**: Protects just the payload.
- **Tunnel mode**: Protects the payload and the header. In this configuration, IPsec acts as a gateway; traffic for any number of client computers can be carried. IPsec in tunnel mode provides link encryption and is compatible with IPv6. It can be used to encrypt any traffic supported by IP.

Figure 5.19 illustrates the differences between the two modes.

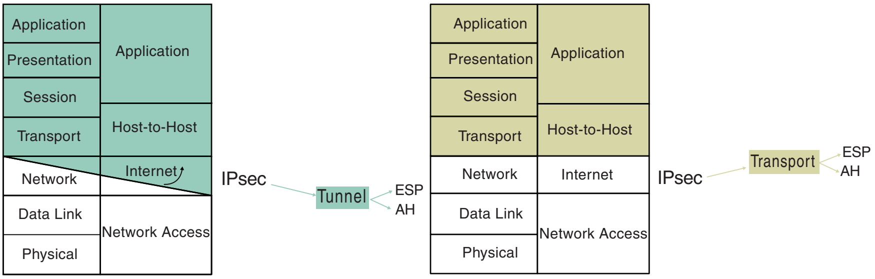


FIGURE 5.19 **IPsec Tunnel and Transport Modes**

RFC 2401 defines three different implementation architectures for IPsec:

- **Host-to-gateway**: Used to connect one system that runs IPsec client software to an IPsec gateway.
- **Gateway-to-gateway**: Connects two IPsec gateways to form an IPsec connection that acts as a shared routable network connection.
- **Host-to-host**: Connects two systems to each other via IPsec.

Message Privacy and Multimedia Collaboration

New technologies make it possible to monitor all types of information that one individual might send to another. *Bullrun* is one example of such a program. The NSA developed this controversial program to give the U.S. government the means to defeat the encryption used in specific network communication technologies. Its full capability is unknown.

Some Internet applications have little or poor built-in security. *Instant messaging* (*IM*) is a good example. Many corporations allow or use IM applications such as WhatsApp, Viber, and Telegram. However, many IM applications lack strong end-to-end encryption capabilities, have insecure password management, and have features that may work to bypass firewalls. IM can be vulnerable to sniffing attacks, can be used to spread viruses and worms, and can be targeted for buffer overflow attacks. If these programs are going to be used, security controls such as the Pidgin-Encryption plug-in and SSL-based chat should be considered. IM products are highly vulnerable to malware, such as worm viruses, backdoor Trojan horses, hijacking, impersonation, and denial of service. IM can also be used to exfiltrate sensitive information.

Web conferencing is a low-cost method that allows people in different locations to communicate over the Internet. Common solutions include Adobe Connect, Zoom, and Microsoft Teams. Though useful, web conferencing can potentially be sniffed and intercepted by an attacker. These technologies usually allow users to display PowerPoint slides, share audio or video, and even share documents. Some solutions allow users to remotely control another connected PC.

Remote meeting and web conferencing software is typically designed to tunnel outbound SSL or TLS traffic. These technologies often pass outside the corporate network and as such should be understood, controlled, and made compliant with all applicable policy as they offer attackers and others the ability to exfiltrate data.

Finally, email is a common network application that, in its native state, can be very insecure. As mentioned earlier in this chapter, sending an email message is much like your parents sending a postcard about their vacation to you through the U.S. mail. Anyone who happens to see the card during transit can read the message they sent you from their trip to Niagara Falls. If you need email privacy, you must use encryption. Using encryption is the equivalent of sending a coded letter in a sealed envelope: Even if someone opens the sealed envelope, the coded letter will prevent anyone from learning about your mother's trip to see the majestic falls. Email protection mechanisms, as described earlier in this chapter, include PGP, Secure Multipurpose Internet Mail Extensions (S/MIME), and Privacy Enhanced Mail (PEM).

Exam Prep Questions

1. You are a security consultant for a new company that is going to sell products online. Customers will be expected to pay for their products on the company website. It is necessary to establish a secure connection between two TCP-based machines to ensure web communications for financial transactions. You have been asked to suggest some type of Extensible Authentication Protocol to help secure this traffic. Which of the following would you consider the most secure and also the most costly?

❍ **A.** EAP-LEAP

❍ **B.** EAP-MD5

❍ **C.** EAP-TLS

❍ **D.** EAP-SIM

2. You just overheard two people discussing ways to steal electronic serial numbers (ESNs). What type of attack are they discussing?

❍ **A.** Bank card hacking

❍ **B.** Modem hacking

❍ **C.** PBX hacking

❍ **D.** Cell phone hacking

3. You are a security consultant for a company that has locations in Houston, New York City, and Dallas. Your client requires link-to-link communications from the LAN to the WAN for data/traffic encryption supported by IP that includes encryption and authentication. They will be using L2TP at Layer 3 of the OSI model. The CIO for the company plans to migrate to IPv6 over the next year, and he wants something that will be compatible with IPv6. What is the BEST protocol to use for this client?

❍ **A.** IPsec transport mode

❍ **B.** IPsec tunnel model

❍ **C.** PPTP

❍ **D.** L2F

4. Which of the following is a mechanism for converting internal IP addresses found in IP headers into public addresses for transmission over the Internet?

❍ **A.** ARP

❍ **B.** DNS

❍ **C.** DHCP

❍ **D.** NAT

5. Samuel has been asked to start the implementation of IPv6 on an existing IPv4 network. The current system has no native connection to an IPv6 network. It has about 130 hosts. The internal routing protocol is OSPF. Which technology would you recommend that Samuel use?

○ **A.** VRRP

○ **B.** Teredo

○ **C.** 802.1AE

○ **D.** 6to4

6. You have been brought on as a consultant to a small nonprofit that is using a routing protocol based on Bellman-Ford algorithms. Although the network has reached convergence, one path is no longer available and shows an infinite hop count. What is the proper term to describe this situation?

○ **A.** Loopback

○ **B.** Split horizon

○ **C.** Classless inter-domain routing

○ **D.** Poison reverse

7. Which of the following is considered an update to WEP?

○ **A.** WPA2

○ **B.** SMLI

○ **C.** PGP

○ **D.** POP

8. Which of the following closely resembles a packet-filtering device that makes decisions on addresses, ports, and protocols?

○ **A.** Stateless firewall

○ **B.** Circuit-level proxy

○ **C.** Application proxy

○ **D.** Stateful firewall

9. Which protocol is considered a forerunner to Frame Relay and works over POTS lines?

○ **A.** SMDS

○ **B.** ATM

○ **C.** X.25

○ **D.** T-carrier

10. Which of the following is true of RADIUS?

❍ **A.** It provides authentication and accountability.

❍ **B.** It provides authorization and accountability.

❍ **C.** It provides authentication and authorization.

❍ **D.** It provides authentication, authorization, and accountability.

11. You have been asked to implement a WAN technology for your client. The client is based in a rural area in the southern United States. The client does not want to use a circuit-switched technology. In this situation, which of the following is a cell-switched technology that you could use?

❍ **A.** DSL

❍ **B.** T1

❍ **C.** ISDN

❍ **D.** ATM

12. Which of the following is considered a third-generation firewall?

❍ **A.** Packet filter

❍ **B.** Circuit-level proxy

❍ **C.** Application-level proxy

❍ **D.** Stateful firewall

13. Which of the following is a list of protocols that work at OSI Layers 2, 6, 3, 4, and 7?

❍ **A.** ARP, SQL, ICMP, SMB, and SNMP

❍ **B.** L2TP, SMB, IP, SQL, and HTTP

❍ **C.** WEP, ASCII, IPX, TCP, and BootP

❍ **D.** PPP, ZIP, SPX, UDP, and TFTP

14. Which of the following wireless standards has a frequency range of 5.15–5.35 GHz to 5.725–5.825 GHz and can be used for distances of approximately 60 feet?

❍ **A.** 802.11a

❍ **B.** 802.11b

❍ **C.** 802.11g

❍ **D.** 802.11n

15. Which of the following is the BEST description of ISAKMP?

❍ **A.** Defines procedures and packet formats to establish, negotiate, modify, and delete security associations and defines payloads for exchanging key generation and authentication data. Typically uses IKE for key exchange, although other methods can be implemented.

❍ **B.** Enables the authentication of the parties involved in a secure transition and contains the certificate issuer's name, a valid from date and a valid to date, the owner of the certificate (the subject), the subject's public key, the timestamp, and the certificate issuer's digital signature.

❍ **C.** A framework for managing private keys and certificates that provides a standard for key generation, authentication, distribution, and storage; establishes who is responsible for authenticating the identity of the owners of the digital certificates; and follows the X.509 standard.

❍ **D.** A standard that defines how to protect keys and establish policies for setting key lifetimes and that sets out essential elements of business continuity and disaster recovery planning.

Answers to Exam Prep Questions

1. **C.** EAP-TLS is one of the most secure but expensive solutions as it requires certificates for both the server and the client. Answers A and B are incorrect because both EAP-LEAP and EAP-MD5 are known to be insecure. Answer D is incorrect because EAP-SIM is used for smartphones and mobile devices.
2. **D.** Cell phone hackers scan for electronic serial numbers and mobile identification numbers, which are used to clone phones. Answer A is incorrect because bank card hacking would most likely target a database. Answer B is incorrect because the individuals who target modems are known as war dialers. Answer C is incorrect because PBX hacking is performed by phreakers.
3. **B.** IPsec in tunnel mode provides link encryption, is compatible with IPv6, and can be used to encrypt any traffic supported by IP. It can also be used with L2TP or alone and operates at Layer 3 of the OSI model. Answer A is incorrect because transport mode encrypts only the IP payload. Answer C is incorrect because PPTP does not offer encryption. Answer D is incorrect because it works at Layer 2 of the OSI model and does not provide data encryption.
4. **D.** NAT allows a single device, such as a router, to act as an agent between the Internet and the internal network. ARP is used for physical address resolution, so answer A is incorrect. DNS is used for IP address resolution, so answer B is incorrect. DHCP is used to assign dynamic addresses, so answer C is incorrect.
5. **B.** Teredo is a transition technology that can be used for IPv6-capable hosts that are on the IPv4 Internet and have no native connection to an IPv6 network. Answer A is incorrect because Virtual Router Redundancy Protocol (VRRP) is used for router redundancy. Answer C is incorrect because 802.1AE is a Layer 1 OSI technology known as MACsec. Answer D is incorrect because although 6to4 is an Internet transition mechanism for migrating from IPv4 to IPv6, it is typically used where there is connectivity to an IPv6 network.
6. **D.** Poison reverse sets the number of hops to the unconnected gateway to a number that indicates infinite. All other answers are incorrect. Answer A describes the loopback address, which has no relevance to the question. Answer B is incorrect because split horizon is a route advertisement that prevents routing loops in distance-vector routing protocols by prohibiting a router from advertising a route back onto the router interface from which it was discovered. Answer C is incorrect because classless inter-domain routing was designed to slow the growth of routing tables on routers across the Internet and to help slow the rapid exhaustion of IPv4 addresses.
7. **A.** WPA2 is the current standard for wireless security. Answer B is incorrect because SMLI is a firewall technology. Answer C is incorrect because PGP is an email-protection mechanism, and POP, answer D, is associated with email, so it is incorrect.
8. **B.** Circuit-level proxies closely resemble packet-filtering devices because they examine addresses, ports, and protocols. Stateless firewalls are packet-filtering devices and application proxies, and stateful firewalls examine higher-level content, so answers A, C, and D are incorrect.

9. **C.** X.25 predates Frame Relay. Although it is not fast, it is reliable and works over analog phone lines. SMDS is a high-speed MAN/WAN packet-switched protocol, so answer A is incorrect. ATM is a modern protocol that offers high speed and various classes of service, so answer B is incorrect. T-carrier is a circuit-switched technology, so answer D is incorrect.

10. **C.** RADIUS is a client/server protocol used to authenticate dial-in users and authorize access. The other answers are incorrect because they do not meet the specification of RADIUS.

11. **D.** ATM is a cell-switched technology. DSL, T1, and ISDN are not based on cell-switching technology, and therefore answers A, B, and C are incorrect.

12. **D.** Stateful firewalls are considered intelligent firewalls and are third-generation devices. Circuit-level proxies and application-level proxies are second-generation devices, and packet filters are first-generation devices, so answers A, B, and C are incorrect.

13. **C.** WEP is found at Layer 2. ASCII is found at Layer 6, IPX is found at Layer 3, TCP is found at Layer 4, and BootP is found at Layer 7.

14. **A.** 802.11a has a frequency range of 5.15–5.35 GHz to 5.725–5.825 GHz and can operate over a distance of approximately 60 feet.

15. **A.** ISAKMP is Internet Security Association and Key Management Protocol. It defines procedures and packet formats to establish, negotiate, modify, and delete security associations, and it defines payloads for exchanging key generation and authentication data. It typically uses IKE for key exchange, although other methods can be implemented. Answers B and C are both incorrect because they deal specifically with certificate management. Answer D is incorrect because it deals with key management.

Need to Know More?

Introduction to TCP/IP: www.cse.wustl.edu/~jain/tutorials/ftp/t_2tcp.pdf

Introduction to the OSI model: www.studynotesandtheory.com/single-post/Quick-Breakdown-of-OSI-Model

Encapsulation: www.tcpipguide.com/free/t_IPDatagramEncapsulation.htm

Bluetooth keyboard sniffing: www.helpnetsecurity.com/2016/07/26/keystroke-sniffing-wireless-keyboards/

Microsegmentation: www.cisco.com/c/en/us/products/security/what-is-microsegmentation.html

Securing OSI: www.infosecwriters.com/text_resources/pdf/KRodriguez_OSI_Model.pdf

Content delivery networks: www.akamai.com/us/en/resources/content-distribution-network.jsp

Software-defined networking: https://docs.microsoft.com/en-us/windows-server/networking/sdn/software-defined-networking

Li-Fi technology: www.technipages.com/what-is-li-fi

Zero trust security: www.microsoft.com/en-us/security/business/zero-trust

Containers and dockers: https://docs.microsoft.com/en-us/dotnet/architecture/microservices/container-docker-introduction/

Converged protocols: www.centurylink.com/business/networx/products/ipbased/cips.html

This page intentionally left blank

CHAPTER 6

Identity and Access Management

Terms you'll need to understand:

- Identification and authentication of people and devices
- Employee access control
- Mandatory access control (MAC)
- Discretionary access control (DAC)
- Role-based access control (RBAC)
- Attribute-based access control (ABAC)
- Single sign-on (SSO)
- Federated identity management
- Crossover error rate (CER)
- Zephyr analysis

Topics you'll need to master:

- Identity and access management
- How to control physical and logical control to assets
- Methods to integrate identity as a third-party service
- Differences between discretionary, mandatory, attribute-based, and role-based access control
- How to manage the identity and access provisioning lifecycle
- How to differentiate authorization types

Introduction

Identity and access management is about controlling access to assets and can include controls on systems, information, devices, and facilities. Access control is a key component of security and can be thought of in both physical and logical senses. Access management is critical because it helps to keep unauthorized users out and keeps authorized users honest; it is critical for accountability and auditing. Access management is crucial to the triple-A process: *authentication*, *authorization*, and *accountability*.

Note

You may see accountability and auditing used synonymously; these terms mean the same thing.

Authentication systems based on passwords have been used for many years because they can be integrated relatively easily and inexpensively. Today, many more organizations are using tokens and biometrics. Some organizations even enforce two-factor authentication, and other entities are moving to federated identity management.

Physical access is a key element of asset management. Many people underestimate the importance of physical controls. If you can gain access to something, you have a good chance of being able to control it. Physical controls are one of the three key categories (along with administrative and logical controls) into which all controls are sorted. Each control can be measured against the basic requirements of availability, confidentiality, and integrity. After all, if attackers can walk off with a portable hard drive, USB thumb drive, or smartphone, they have (at the least) denied you availability. If a coworker loses an unencrypted USB drive containing proprietary information that a criminal could recover, confidential information can be disclosed to unauthorized persons. If a disgruntled employee can physically access a server on which a key database resides and change amounts or values, data integrity can be compromised.

Implementations of physical security surround us. For example, you might have a radio frequency ID (RFID) tag on your car that permits you access to park in the company parking garage. Perhaps company policy requires you to get a new photo taken each year for your company ID badge. Access to the equipment room might be limited to employees who have been assigned access via their badge. You deal with physical access controls every day.

Security administrators have more to worry about than just physical access. Many employees have logical access to multiple company resources that may reside locally, in remote servers and in the cloud. Users might be tied to many roles and accounts that must be managed. Luckily, there is a way to consolidate these accounts: through the use of single sign-on solutions. A single sign-on solution allows users the ability to authenticate only once to access all needed resources and systems. Authentication systems can be centralized, decentralized, or hybrid. This chapter introduces all these concepts.

Tip

Single sign-on (*SSO*) is not the same as *password synchronization*. Password synchronization typically involves using a static password that is shared across multiple systems or programs, whereas in an SSO solution, a user must authenticate to an authentication server, and the authentication server provides further provisional access control privileges for the user.

Although knowing who to authenticate serves as a basis of access control, there also exists the issue of authorization. *Authorization* defines what access the user has and what abilities are present. Authorization is a core component of access control. Once a user has been authenticated to a domain, a server, an application, or a system, what is that person authorized to do? As you can see from this brief introduction, controlling access is the first line of defense in allowing authorized users access while keeping unauthorized users out.

Authorization can be accomplished by using several types of access controls, including discretionary, nondiscretionary, attribute-based, and role-based access controls. Authorization should be implemented to allow the minimum access required for each user to accomplish his or her tasks. This approach helps control access, minimizes the damage that a single employee can inflict on the organization, and mitigates the risks associated with access control. The principle that employees should be provided only the amount of control and access that they need to accomplish their job duties—and nothing more—is referred to as the *principle of least privilege*.

If something does go wrong, a method will be required to determine who has done what. That is the process of audit and accountability. In an audit, individuals tasked with enforcement of network security review records to determine what was done and by whom. Accountability enables malicious and repetitive mistakes to be tracked and tied to a specific individual—or at least traced to that individual's credentials.

Perimeter Physical Control Systems

Physical security controls should be designed so that the breach of any one of them will not compromise the physical security of the organization. Many types of physical controls can be deployed to protect the perimeter of a facility. The overall idea is to provide *defense in depth*. This approach involves creating layers of defensive mechanisms, using different types of controls. Closed-circuit television (CCTV) cameras, gates, lighting, guards, dogs, and locks are but a few of the layers of physical security that can be added to build a defense-in-depth strategy. The following sections describe physical controls from the outside in.

Fences

Consider the Berlin Wall. This monument to the Cold War was quite effective at preventing East Germans from escaping to the West. Before the fall of the wall in 1989, most people who escaped to the West did so by hiding in trunks of cars or by bribing guards. The wall worked as both a strong physical barrier and as a psychological barrier. The amount of control provided by a fence depends on the type (see Table 6.1). A 3- to 4-foot fence will deter only a casual trespasser, but an 8-foot fence will deter and delay a determined intruder. Adding three strands of razor wire at the top is an additional effective security measure. If you are trying to keep individuals inside an area, you should point the razor wire in, and if you are trying to keep individuals out, you should point the razor wire out.

If you are really concerned about who's hanging around the perimeter of your facility, you might consider installing a perimeter intrusion and detection assessment system (PIDAS). This is a special fencing system that has sensors to detect intruders. The downside is that stray deer or other wildlife might also trigger alarms.

TABLE 6.1 **Fence Heights**

Height	Purpose
3–4 feet	Will deter only casual trespassers.
6–7 feet	Considered too tall to easily climb.
8 feet	Should deter a determined intruder. A topping of three strands of razor wire should be pointed out, in, or in both directions at a 45° angle. Pointed inward toward the facility typically is a security measure to keep people in; pointed outward is a security measure to keep people out.

Fencing can be made from a range of components, such as steel, wood, brick, or concrete. Chain link, wire, and steel mesh fences are used at many facilities and can provide various degrees of security. The gauge of the wire and the size of the mesh help determine the security of these fences. The gauge is the measurement of the diameter of the wire, where the higher the gauge number, the smaller the wire diameter. Table 6.2 lists the common wire gauges and diameters.

TABLE 6.2 **Wire Gauges and Diameters**

Gauge	Diameter
6 gauge	.192 inch
9 gauge	.148 inch
11 gauge	.120 inch
11½ gauge	.113 inch
12 gauge	.106 inch
12½ gauge	.099 inch

The ASTM (formerly the American Society for Testing and Materials) defines fence standards and certifies vendors' fencing. ASTM has established standards for residential, commercial, and high-security products. The distance between the two wires in a fence is the *mesh size*. Table 6.3 lists common fence mesh sizes and their corresponding security ratings. In general, a high fence with small holes is difficult for an intruder to climb, whereas a high fence with large holes can be easily climbed.

TABLE 6.3 **Fence Mesh Size**

Mesh Size	Rating
2 inch	Normal usage
1 inch	Higher security
³/₈ inch	Extremely high security

Gates

Whereas a fence acts as a barrier, a *gate* is like a firewall in that it is a choke point and controls ingress and egress of pedestrian and vehicle traffic. A gate must be of the same level of security as the fence to act as an effective deterrent. Gates are covered by UL Standard 325 and ASTM-F2200. Gates can be designed as swing gates, rolling gates, and cantilever gates. There are four classes of gates, as shown in Table 6.4.

TABLE 6.4 **Gate Classes**

Class	Rating
Class I	Residential
Class II	Commercial
Class III	Industrial
Class IV	Restricted access, high security

Turnstiles and mantraps are additional types of gates. A *turnstile* is a form of gate that prevents more than one person at a time from gaining access to a controlled area. Turnstiles usually rotate in only one direction, restricting flow. Turnstiles are commonly used at sporting events and subway stations.

A *mantrap* is a set of two doors, sometimes called *deadman doors*, that together control access. With a mantrap, one or more people must enter the mantrap and shut the outer door before the inner door will open. Some mantraps lock both the inner and outer doors if authentication fails so that the individual cannot leave until a guard arrives to verify the person's identity. Mantraps can be used to control the flow of individuals into and out of sensitive areas. Mantraps can help prevent *piggybacking*, which is commonly attempted at controlled-entry points where authentication is required. Although some individuals use the terms *piggybacking* and *tailgating* synonymously, tailgating is also associated with the practice of attempted unauthorized access at vehicle access points and gates where the access point opens long enough that a second car can attempt to pass through.

ExamAlert

A mantrap is used to prevent piggybacking, and additional layers of compensating controls, such as using guards and CCTV, can be added.

Bollards

Bollards are another means of perimeter control. Made of concrete or steel, they block vehicular traffic or protect areas where pedestrians might be entering or leaving buildings. Since the attacks of 9/11, these barriers have advanced far beyond the standard steel poles of the past. Organizations now make bollards with electronic sensors to notify building inhabitants that someone has rammed or breached the bollards. Although fences act as a first line of defense, bollards are a close second because they can deter individuals from ramming a facility with a car or truck. Figure 6.1 shows an example of bollards.

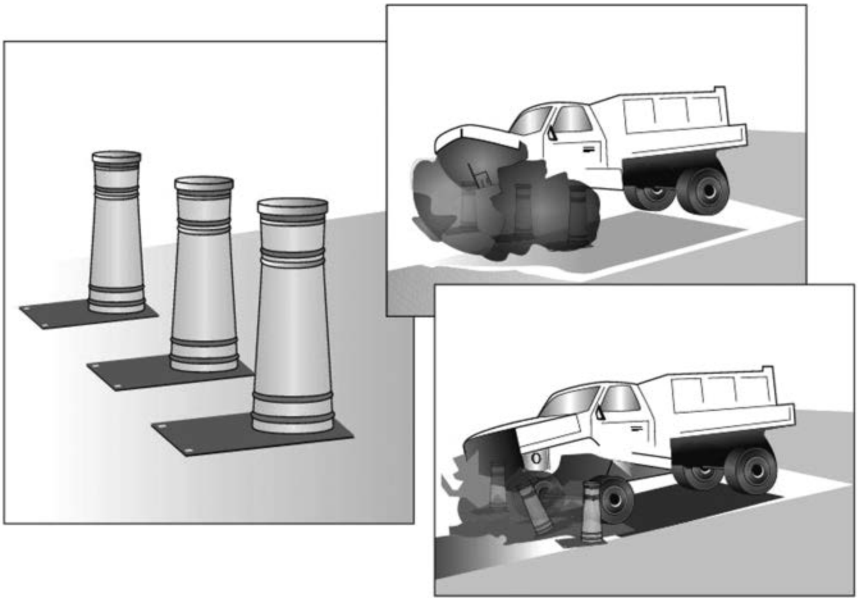


FIGURE 6.1 **Bollards**
Source: www.deltascientific.com/bollards2.htm

Additional Physical Security Controls

Perimeter controls need not look like concrete and steel. Have you ever noticed the majestic ponds located next to many corporate headquarters? Don't be lulled into believing they were placed there merely as a community beautification project. They are another form of a barricade or barrier. They are also useful in case of fire because they can serve as an additional water source. Access controls are a critical piece of premises security that can be either natural, such as a body of water, or structural, such as a fence.

What else can be done? Warning signs or notices should be posted to deter trespassing. A final review of the grounds area should be conducted to make sure that nothing has been missed. This includes any opening that is around 96 square inches or larger and 18 feet or less above the ground, such as manholes/tunnels, gates leading to the basement, elevator shafts, ventilation openings, and skylights. Even the roof, basement, and walls of a building might contain points vulnerable to entry and should be assessed.

After the premises of the facility have been secured, a security professional should move on to an analysis of other perimeter control mechanisms, such as CCTV, card keys, RFID tags, lighting, guards, dogs, locks, and biometric access controls. Just as networks use choke points and multiple layers of defenses, so should physical security controls. Each of these is explained in more depth in the sections that follow.

CCTV Cameras

CCTV can be used for monitoring or for physical detection to assess and identify intruders. A CCTV system also serves as a great deterrent. Before the first camera is installed, several important questions must be considered: Will the video feed be monitored in real time? How long will recordings be stored? What type of area will be monitored? A CCTV system by itself cannot prevent anything. If the system is to be used in real time as a preventive control, human intervention is required: A guard or another individual must watch as events occur. A CCTV system that is not used in real time but after events occur functions as a detection control. Different environments require different systems.

If a CCTV system is to be used outside, the amount of illumination is important. Illumination is controlled by an iris that regulates the amount of light that enters the CCTV camera. An automatic iris lens is designed to be used outside where the amount of light varies between night and day; a manual iris lens is used for cameras used indoors. CCTV cameras can be equipped with built-in LEDs or configured for infrared recording.

The focal length of the lens controls a CCTV camera's depth of field, which determines how much of the visual environment is in focus on the CCTV monitor. The depth of field is critical if there is not a human being monitoring the system to make adjustments to the focus. Whereas some systems have fixed focal lengths, others offer the capability to pan, tilt, and zoom (*PTZ*), allowing the operator to zoom in or adjust the camera as needed. Older CCTV cameras are analog, whereas most modern cameras are digital, capturing enhanced detail quickly through the use of *charge-coupled devices* (*CCDs*). A CCD is similar to the technology found in a fax machine or a photocopier.

A CCTV system can be wired or wireless and comprises many components, including cameras, transmitters, receivers, recorders, monitors, and controllers. CCTV systems provide effective surveillance of entrances and critical access points. If employees are not available to monitor in real time, activity can be recorded and reviewed later. An *annunciator* can be used to reduce the burden on the individual monitoring the alarm by detecting intrusions or other types of noise and tripping an alarm so that a guard does not have to constantly watch a monitor.

If you are considering using a CCTV system, remember to provide for the rights of worker privacy or notification of the absence of privacy and consider the existence of potential blind spots.

Lighting

Lighting is a common type of perimeter protection. Some studies have found that up to 80% of criminal acts at businesses and shopping centers happen at night in adjacent parking lots, so organizations need to practice due care when installing exterior lights. Failure to provide adequate lighting in parking lots and other high-traffic areas could lead to lawsuits if an employee or a visitor is attacked. Outside lighting discourages prowlers and thieves. The following are some common types of exterior lights:

- Floodlights
- Streetlights
- Searchlights

Terms used for the measurement of light include *lumen*, *lux*, and *foot-candle*. One lux is one lumen per square meter, and one foot-candle is one lumen per square foot. The National Institute of Standards and Technologies (NIST) states that for effective perimeter control, buildings should be illuminated with 2 foot-candles of light in a projection that is 8 feet high.

The next time you visit a mall or department store, take a moment to look at how the lights are configured. You will see rows of lights placed evenly around the facility. That is an example of *continuous lighting*. Areas such as exits, stairways, and building evacuation routes are equipped with *standby lighting*, which activates only in the event of power outages or during emergencies; however, standby lighting is more commonly used with homes and/or businesses that are set to turn on after at a certain time after normal operating hours late at night to give the appearance that the home or business is occupied, thus deterring intruders and trespassers.

As with all other security measures, the provision of lighting takes planning. Effective lighting requires more than the placement of a light bulb atop a pole. Security professionals need to consider what areas need to be illuminated, which direction lights should be directed, and how bright the lights will be. Some lights make use of a *Fresnel lens*. These lenses are designed to focus light in a specific direction and were originally used in theaters and lighthouses.

Security checkpoints are another location where you will see careful design of the illumination. Here, lights are aimed away from the guard post so that anyone approaching the checkpoint can easily be seen and guards are not exposed in the light. This is an example of *glare protection*. If lights are used for perimeter detection, they are typically mounted above the fence. This positioning allows the lights to blind intruders to the surrounding view and enables the guard force to more easily see intruders.

Just as too little light can be a problem, too much light can lead to a less secure environment. Glare and over-lighting can cause problems by creating very dark areas just outside the range of the lighted area. In addition, neighboring businesses or homes might not appreciate residing in a very brightly lit area. Therefore, exterior lighting must be balanced to provide neither too little nor too much light. You should ensure that each exterior light covers its own zone but also allows for some overlap between zones.

Guards and Dogs

Guards can offer the best and worst in the world of access control protection. Although our increased need for security has driven the demand for more guards, they are only human, and their abilities vary. Technology has also driven our need for security guards. As we get more premises control equipment, intrusion detection systems, and computerized devices, additional guards are required to control these systems.

Unlike computerized systems, guards have the ability to make judgment calls and think through how they should handle specific situations; they have *discernment*. Guards can also take on multiple tasks—including greeting, signing in, escorting, and monitoring visitors. Just by having guards in a facility or guarding a site, an organization provides a visual deterrence. Before you go out and hire your own personal bodyguard, however, you should be aware that guards do have some disadvantages. Guards can be expensive, make mistakes, be poorly trained, make policy exceptions for people they like or trust, be manipulated, sleep on the job, steal organizational property, and even injure people.

Dogs have also been used to secure property throughout time. Breeds such as Chows, Dobermans, and German Shepherds were bred specifically for guard duty. Although dogs can be trained, loyal, obedient, and steadfast, they are sometimes unpredictable and could bite or harm the wrong person. Because of these factors, dogs are usually restricted to exterior premises control and should be used with caution.

Locks

Locks are all about access control. Locks come in many types, sizes, and shapes, and they are some of the oldest access control devices; the Egyptians used them as long ago as 2000 BCE. Locks are the most commonly used deterrents, and they provide a high return on investment.

It's important to select the appropriate lock for an area. Different types of locks provide different levels of protection, and they are designed to various strengths and levels of security. The grade of a lock specifies its level of construction. Table 6.5 lists the three basic grades of locks and their common uses.

TABLE 6.5 **Lock Strengths**

Grade	Use	Usage Cycles
Grade 3	Residential and consumer use	200,000
Grade 2	Light-duty commercial and heavy-duty residential locks	400,000
Grade 1	High-security commercial and industrial-use locks	800,000

Some common lock types include combination locks, mechanical locks, cipher locks, and device locks.

A basic *combination lock*, which a user unlocks by inputting a correct combination of numbers, usually has a series of wheels inside. The longer the combination, the more combinations are possible, and the more effort required to brute-force the lock. Figure 6.2 shows examples of three- and four-digit combination locks. With a three-digit lock, there are 1,000 possible combinations, and with a four-digit lock, 10,000 combinations are possible. Let's not forget people like easy-to-remember patterns such as 43210, 1234, or 007, so if a basic combination lock uses such an easy-to-guess combination, it is more of a deterrent than a preventive control.

Mechanical locks have been used for hundreds of years to secure items of importance. Early locks were made of wood, and attempts to improve lock designs increased throughout the 1700s. Mechanical locks include warded locks and pin-and-tumbler locks. The modern tumbler lock was patented by Linus Yale in 1848.

A *warded lock* is a basic padlock that uses a key with a spring-loaded bolt. This type of lock uses a series of wards, or blockages, that a key must match up to. It is the cheapest type of mechanical lock and is also the easiest to pick. It can be picked by inserting a stiff piece of wire or thin strip of metal; a simple warded lock can be opened with a skeleton key. Warded locks do not provide a high level of security.

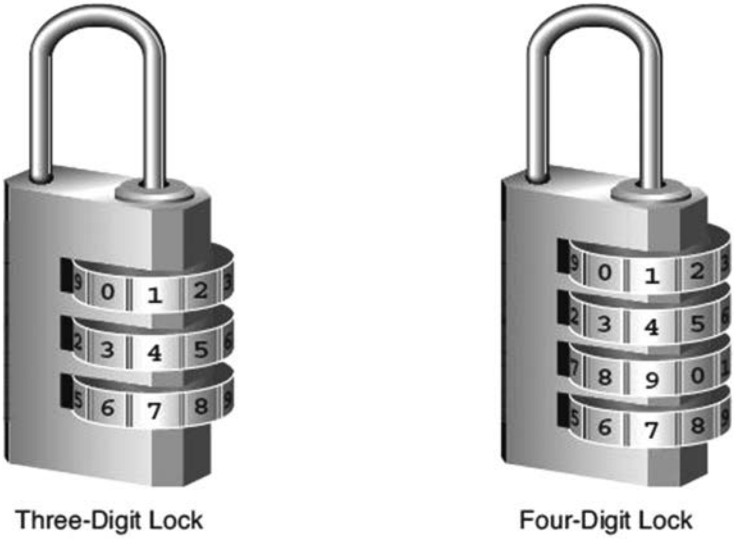


FIGURE 6.2 **Combination Locks**

Tumbler locks are somewhat more complex than warded locks. Instead of using wards, they use tumblers, which makes it more difficult to open a lock with the wrong key. When the right key is inserted into the cylinder of a tumbler lock, the pins are lifted to the right height so that the lock can open or close. Figure 6.3 illustrates a basic tumbler lock design.

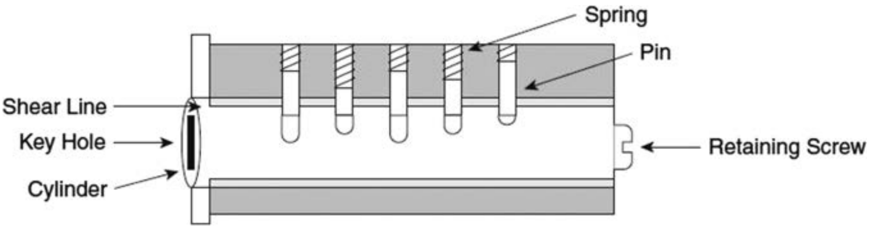


FIGURE 6.3 **Tumbler Lock Design**

In a tumbler lock, the correct key has the notches and raised areas to shift the pins into the proper position. The pins are spring-loaded so that when the key is removed, the pins return to the locked position. Tumbler locks can be designed as pin tumblers, wafer tumblers, lever tumblers, or tubular locks. Tubular locks, also known as *ace locks*, are secure locks that are often used for computers, vending machines, and other high-security devices.

These are not the only types of locks. There is also a category of locks known as cipher locks, or *programmable locks*, which require the user to enter a preset or programmed sequence. With a cipher lock, you use a keypad or cipher to control access into restricted areas. One shortcoming with a keypad device is that bystanders can shoulder surf and steal passcodes. To increase security and safety, visibility shields should be used to prevent bystanders from viewing the passcodes that are entered. Another problem with keypad locks is that someone who knows the code might prop the door open so others can easily enter. To prevent this type of activity, door delay alarms should be considered. One main advantage to cipher locks is that some systems, referred to as *smart locks*, allow for granular roles and rule-based access control of physical security along with user access auditing. Such a system makes it very easy to quickly revoke user access to a secure area by deleting the access code; it is not necessary to collect a key or access card. In addition, a smart lock functions as a detective control and allows for effective auditing of who has accessed secured areas.

Locks can also be used to secure a wide range of devices. Device locks can be used to secure ports and laptops. Employees who are issued laptops should be given laptop-locking devices. Although data security is important, the security of the device should also be considered; it takes only a moment for someone to take a laptop or other mobile device. Device locks can help protect physical assets and signal to employees your concern that devices issued to them should be protected.

Caution

Although it is important to use locks to secure laptops, it's also important to use encryption because the data on a laptop is most likely worth more than the hardware.

Many organizations don't change locks frequently. Others fail to require terminated employees to return keys. Some locks even have master keys so that a supervisor or housekeeper can bypass use of the normally required key and gain entry. Finally, there is the issue of lock picking, described in the next section. Although locks can be used to deter and delay, all locks are subject to attack.

Note

Keep in mind that a lock is a deterrent and not a preventive control. Most locks keep out honest people and should work as a layer of security in your overall security solution. Even high-end cipher locks have been bypassed in a number of ways including strong magnets.

Lock Picking

Lock picking is one way to bypass the security intended with a lock. Although lock picking is not the fastest way to break in, it does offer a stealthy way to bypass a lock, and it might not be evident to the victim that a security violation has occurred. If you have any doubts about whether lock picking is a common hacker skill, check out any of the large hacking conferences, such as DEF CON. This yearly hacker conference usually features presentations and contests devoted to lock picking.

Lock picking basically involves manipulating a lock's components to open it without a key. Several basic tools are used to pick locks:

- **Tension wrench**: This type of wrench is not much more than a small angled flathead screwdriver. It can be a variety of thicknesses and sizes.
- **Pick**: A pick for lock picking is much like a dentist's pick. It is small, angled, and pointed.

Together, these tools can be used to pick a lock. One basic technique is *scrubbing*, or *raking*. Scrubbing is the act of scraping the pins quickly with a pick while using a tension wrench to place a small amount of force on the lock. Some of the pins are then placed in a mechanical bind and get stuck in the unlocked position. With practice, this can be done quickly so that all the pins stick and the lock disengages.

Key bumping is another lock-picking technique that has gained notoriety. Key bumping is performed by using a key for a specific brand of lock that has been cut to the number nine position. This is the lowest possible cut for the key. For example, in Figure 6.4, notice how the four inner ridges are very low.

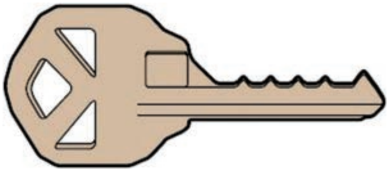


FIGURE 6.4 **Bump Key**

The user inserts a bump key into a lock and applies slight pressure while tapping (bumping) the key. This transference of force causes the pins to jump inside of the cylinder so that the lock is disengaged. An Internet search will return many videos about key bumping.

Other tools to bypass locks include the following:

- **Lock pick set**: Lock pick sets vary in price and design and might contain anything from a couple of tools to more than two dozen various picks and tension wrenches.
- **Electric lock pick gun**: This type of device can speed up manual lock picking by working somewhat like an electric toothbrush or an electric knife.
- **Tubular pick**: This type of pick is designed to pick tubular locks (sometimes referred to as ACE locks), which are the same kind as used on Kryptonite bicycle locks, which were thought to be highly secure until 2004, when someone demonstrated that such a lock could be opened with a Bic pen. The same issue exists with Kensington-style laptop locks.
- **Lock shim**: A formed piece of thin, stiff metal can be inserted into the latch of a padlock and used to push back the locking mechanism.

Employee Access Control

Several forms of physical access control are likely performed before employees ever reach their desks. The information provided by these controls is critical not only for monitoring access control but for reconstructing events following an intrusion, a theft, or an attack. The following sections describe tools that keep track of where employees go and what they do.

Badges, Tokens, and Cards

Tokens, cards, and keys are all means of access control. The physical characteristics and use of these controls are discussed here.

Table 6.6 details common types of access cards and badges.

TABLE 6.6 **Card Key Types**

Type of Card	Description
Photo card	Contains a facial photograph of the card holder
Active electronic	Can transmit electronic data
Magnetic stripe	Has a stripe of magnetic material
Magnetic strip	Contains rows of copper strips
Optical coded	Contains a laser-burned pattern of encoded dots or 3D bar codes
Smart card	Has an electronic circuit and processor embedded
RFID card	Has a small RFID circuit embedded

Physical access control cards can be separated into two broad categories: *dumb cards* and *smart cards*. Dumb cards contain no electronics and often include an individual's photo to verify a person's right to be in a particular area. These photo ID cards are really just a form of identity badge. Photo badges are effective only if controls are in place to ensure that they are inspected by guards at key points in and around a facility.

Caution

It is unfortunate but true that cleaning crews are sometimes overlooked as potential security threats. They are typically around after everyone else leaves, and they have full access to the facility. Unlocked computers can make tempting and easy targets. One of the editors of this book shared a story of how the cleaning crew of his former employer shared badges and often had friends or relatives fill in for them for a day or two using the same badge.

The second type of access control is a smart card. European countries have long used smart card technology in credit cards, and the United States began to implement it in late 2015. Smart cards are much more versatile than photo cards. Smart cards can make entry decisions electronically. These devices can be configured in several different ways. Some require only that the user get close to the access control device. These proximity readers don't require the user to physically insert the card. Some identification technologies use RFID. Others require user activation, such as requiring the user to input a key code. One example of a deployed smart card is the Common Access Card (CAC) used by the U.S. Department of Defense. CACs are considered to be dual-factor (or multifactor), and they provide strong authentication; they are used with a public key infrastructure (PKI).

Some organizations provide card users with two key codes. One of the codes is used for normal access, and the second is used as a *silent hostage alarm or duress alarm*. The silent hostage alarm code allows an employee to gain access and also silently alerts the authorities of a hostage situation.

Caution

High-security facilities have a history of mandating that employees make sure their badges are not visible after leaving the workplace to go home or out to lunch. This is an effective control for any organization that uses badges to reduce social engineering or targeting of specific vehicles, briefcases, laptops, tablets, smartphones, and so on.

RFID Tags

RFID tags are becoming popular physical access controls. An RFID tag is an extremely small electronic device composed of a microchip and an antenna. These devices transmit small amounts of information. RFID tags can be designed in different ways:

- **Active**: An active tag has a battery or power source used to power the microchip and constantly transmits a weak signal.
- **Passive**: This type of device has no battery. It is powered by an RFID reader/transponder, which generates an electromagnetic wave that induces a current in the RFID tag.
- **Semipassive**: This is a hybrid device that has a battery to power the microchip but still transmits data by harnessing energy from the reader.

RFID tags are manufactured in various sizes, down to dust particle size, and their placement possibilities are endless. The U.S. military has conducted trials to test the possibility of using RFID tags to control vehicle traffic at military locations. Some states are considering embedding RFID tags in automobile license plates and automobile registrations so that passing police cars can be alerted about out-of-date registrations. Many countries are using RFID tags in passports. RFID is also being used in implantable devices for access control. For example, Sweden has widely adopted RFID technology in its move toward a cashless economy, and the country has less cash in circulation than anywhere else in the world. Sweden also has thousands of citizens who have been voluntarily implanted with RFID tags to monitor their health and even replace keycards to allow them to enter offices and buildings (see https://www.washingtonpost.com/news/on-leadership/wp/2017/04/04/some-swedish-workers-are-getting-microchips-implanted-in-their-hands/).

Many other countries and businesses are moving to this emerging technology. Amazon Go stores allow shoppers to buy without cashiers or checkout and are expanding across the United States; these stores are based on RFID technology. Microsoft has patented an implantable RFID tag system that could use the human body to mine cryptocurrency (see https://patentscope2.wipo.int/search/en/detail.jsf?docId=WO2020060606&tab=PCTBIBLIO). The U.S. Food and Drug Administration (FDA) has approved an RFID tag that will be used to prevent the possibility of wrong-site, wrong-procedure, and wrong-patient surgeries. Government officials have advocated that these devices become standard issue for firefighters, police officers, and emergency rescue individuals because their jobs place them in situations in which their identification could be lost or destroyed.

Biometric Access Controls

Biometrics can be used for physical or logical access. Biometric controls are based on physiological attributes or behavioral characteristics of an individual. For example, one consulting job I had was with a government agency that took security seriously. This agency implemented two-factor authentication for physical access by means of an access card and a biometric sensor. As if these two were not enough, I was also weighed while in the mantrap before being allowed access to the data center.

With biometric access controls, biometric data is collected from humans and turned into binary data, formatted, and then hashed and stored in a reference file. When a user wants to authenticate, the user's biometric sample is collected again, hashed using the same algorithm as before, and compared to the reference file; a match to a certain degree is required for access.

All biometric systems follow a similar usage pattern:

1. Users must first enroll in the system. Enrollment requires allowing the system to take one or more samples for later comparison.
2. A user requests to be authenticated. Statistics collected during enrollment are used to compare to data scanned during the user's authentication request.
3. A decision is reached. A match allows the user access, whereas a discrepancy causes the user to be denied access.

We discuss biometrics in more detail later in this chapter.

Identification, Authentication, and Authorization

Identification, authentication, and authorization are three of the core concepts of access control. Together, they determine who gets into the network and what they have access to. When someone thinks of authentication, what might come to mind is who gains access; however, identification comes first. At the point of identification, you as the user are a *claimant*. This simply means that you may say you are Michael. But how does the system actually know this? This is where authentication comes into play by proving the veracity of a claim. Let's look at some basic concepts and terms before reviewing more in-depth topics:

- **Identification**: This is the process of identifying yourself to an authentication service.

- **Authentication**: This is the process of proving the veracity of an identity claim; that is, authentication is used to determine whether a user is who he or she claims to be.
- **Authorization**: This is the process of determining whether a user has the right to access a requested resource.
- **Accountability**: This is the ability to relate specific actions and operations to a unique individual, system, or process.
- **Access**: This is the transfer of information between two entities. When access control is discussed, it is usually in terms of access, subjects, and objects.
- **Subject**: This is an active entity that can be a person, an application, or a process.
- **Object**: This is a passive entity that contains or holds information. An object can be a server, a database, or information system.

Tip

It is important to note that a person can be a subject or an object. In this domain, the person is typically the active entity, or subject. In other domains, the application, for example, can be the subject.

Authentication Techniques

In logical security, authentication is the process of determining the legitimacy of a user, a process, or an application. Various identity management implementation schemes have been developed over the years to ensure that the right people have the right access to the right resources and to prove that all the access is legitimate. Some common categories that have been established are as follows:

- **Something you know (type 1)**: This is typically an alphanumeric password or PIN.
- **Something you have (type 2)**: This can be a smart card, token, memory card, or key fob.
- **Something you are (type 3)**: This can be a fingerprint scan, facial scan, retina scan, or voice recognition.

Tip

Some sources list a fourth type of authentication: *somewhere* you are. For example, consider a callback system that requires you to be in a specific location to receive a call to authenticate. Another example is the use of GPS in a smartphone or tablet to identify where you are.

Identity assurance is the level of confidence a system can provide that a user is who he or she claims to be. NIST 800-63 defines three *Identity Assurance Levels* (*IALs*) for registration and identity proofing:

- **IAL 1**: Self-asserted identity
- **IAL 2**: Remote or in-person identity proofing
- **IAL 3**: In-person identity proofing with verification by a credential service provider (CSP)

NIST 800-63 also specifies Authenticator Assurance Levels (AALs), which indicate the level of confidence that the user controls the authenticators (such as passwords):

- **AAL1**: Provides some confidence. Can be one- or two-factor authentication, such as a password or a password and another factor.
- **AAL2**: Provides high confidence. A minimum of two factors must be provided.
- **AAL3**: Provides very high confidence. Two factors are required, with the added requirement of a cryptographic key and a physical device (or a single device that can provide both). When combined with a username/password combination, this provides the highest level of confidence in the authentication.

The authentication process is something that most individuals have performed thousands of times. Consider the login prompt at the website of your bank. You are prompted to enter your username and password. You might be asked to pick a specific image that maps to your account. If the device you are logging in from is unknown, you might be asked to receive a text code to your cell phone. If all this information is entered correctly, you are provided with access.

When you authenticate, you should be able to access your own bank records, but you should not be able to see someone else's bank balance or access their funds. Your level of authorization as a bank user will be much different from that of a bank manager or loan officer. Authorization can offer a wide range of access levels from all to nothing.

Organizations require this level of control to enforce effective controls and maintain a secure environment. *Enforcement* also requires auditing and accountability. Enforcement means that someone must review employee and user activities. A bank manager has a greater level of access than does an average bank user, but this doesn't mean that his or her access is unchecked. Controls are needed to limit what the bank manager can access; furthermore, it is important to enforce accountability so that fraud can be detected if the manager decides to take a small amount of customer money each month and stash it away in an offshore account.

When you need to log in to multiple sites, federated identity management (FIM) can help. FIM can be considered a form of centralization that allows disparate organizations a means to share information. FIM allows you to log in once and access multiple resources without having to log in to each unique site or service.

FIM uses two XML-based options, SAML by OASIS, and WS-Security, which is promoted by Microsoft and IBM.

With FIM, organizations share authentication information over the World Wide Web using Security Assertion Markup Language (SAML) or OAuth. SAML has three roles:

- **Identity provider (IdP)**: SAML provides an assertion about another identity based on information it has, basically asking the user for a username/password pair.
- **Service provider (SP)**: This is the relying party, service, or resource, the user is trying to access.
- **Subject or principal**: This is the user or person who is being vouched for by the IdP.

SAML has four components:

- **Assertions**: An identity provider makes statements about the user that the relying party uses to make access control decisions. The statement vouches for the user and can also specify authorization and level of permissions.
- **Protocols**: These are the rules that specify the format and content of exchanges.
- **Bindings**: These are details of encapsulation protocols in messages.
- **Profiles**: The three components above can be put together into a profile for a particular use case.

OAuth is an open standard that is commonly used to enable Internet users to grant websites or applications access to their information on other websites without providing them the passwords. The OAuth roles are as follows:

- **Resource owner**: This is the entity controlling access to the resource.
- **Resource server**: This is the resource host/server.
- **Client application**: This is the application that requests access to the protected resources.
- **Authorization server**: This is the entity that issues access tokens to the client.

A third solution is OpenID. Whereas SAML and OAuth are more focused on the enterprise, OpenID is focused more on the consumer market. However, the concepts are similar. OpenID allows you to use an existing account to sign in to multiple websites, without needing to create new passwords.

SAML and OAuth only provide authorization. OpenID provides authentication and authorization and acts as a tiny layer that sits on top of OAuth and provides login and profile information about the person who is logged in.

Once users have proven their identity, if two organizations trust each other, a user's shopping experience online gets easier, and the user's security token goes with him or her. For example, if you were to book an airline ticket, you might be presented with a pop-up that asks if you also need to book a hotel room. Clicking Yes might take you to a major hotel chain website to which your identity and travel information have already been passed. This would prevent you from having to log in to the hotel website.

The technologies just described allow for third-party identity management and function by establishing a trust relationship between the identity provider and the service or application. In addition, more organizations are starting to adopt *identity-as-a-service* (IDaaS). IDaaS enables organizations to easily apply strong authentication delivered from the cloud and use it as needed—from anywhere. IDaaS has three elements:

- **Identify Governance and Administration (IGA)**: Password resetting and user provisioning
- **Access**: Authentication, single sign-on, authorization, and federation standard/protocol support
- **Intelligence**: Identity access logging, monitoring, and reporting

Organizations must control access to sensitive data, and they must be able to create and revoke credentials as customers and employees are onboarded or offboarded. Many organizations use a credential management system to manage users' credentials when SSO isn't available. Credential management is needed because users have a limited ability to remember different credentials for different sites. Users can store these credentials securely and use the management system for authorized access. Microsoft Windows has a basic tool called Credential Manager; BeyondTrust, CyberArk, and Thycotic are several other examples of credential management tools. Next, we will examine three basic methods of authentication.

Something You Know (Type 1): Passwords and PINs

Of the three types of authentication, passwords are the most widely used. The problem is that passwords are typically weak. Consider the following:

- People use passwords that are easy to remember.
- Difficult passwords might be written down and left where others can find them.
- Most of us are guilty of reusing passwords.
- Reputability is a real issue with passwords because it is hard to prove who made a specific transaction or gained access.
- Passwords can be cracked, sniffed, observed, replayed, or broken. Password cracking can involve dictionary, hybrid, or exhaustive search (brute-force) attacks.
- Dictionary attacks use common dictionary words, and hybrid password cracking uses a combination of words as random characters, such as 1password or p@ssw0rd. Brute-force attacks attempt all possible variations, which can be time-consuming. Rainbow table attacks use precomputed hash tables to reduce password cracking time and recover plaintext passwords.
- Many people are predictable and use passwords that are easily guessed, such as passwords based on birthdays, anniversaries, a child's name, or a favorite pet. Thanks to the massive growth of the Internet and big data, it is easy to use social engineering to find this information.

Tip

In March 2020, news sources reported that CAM4 had suffered a massive security breach and advised all users that their sensitive records had been exposed. This breach exposed more than 10 billion records.

Password security is an important topic for anyone studying access control. Many times, a password is all that stands between an unauthorized user and account access. If you can't make the change to a more robust form of authentication, you can implement controls to make passwords more robust. A few of these options are as follows:

- **Password length**: Short passwords can be broken quickly via brute-force attacks. Use longer complex passwords.
- **Password composition**: Passwords should not be based on personal information or consist of common words or names. If you use cognitive information such as birthdate, high school, pets name, etc., you should make up this information during enrollment. Remember that your "real" information can be found on the Internet.
- **Password complexity**: A password should be a combination of numbers, symbols, and uppercase and lowercase letters. For example, NIST 800-63 suggests an eight-character minimum with a maximum length of 64 characters or higher that uses number, letters, and special characters.
- **Password aging**: Unlike fine wine, passwords do not get better with age. Two items of concern are maximum age and minimum age. Maximum age is the longest amount of time a user can use a password. Minimum age is the minimum amount of time the user must keep the password.
- **Password history**: Authentication systems should track previous passwords so that users cannot reuse them.
- **Password attempts**: Logon attempts should be limited to a small number, such as three successive attempts. Applying this control is also called setting a *clipping* or *threshold* level. The result of a threshold or clipping event can be anything from locking the account to delaying the ability to log in to the account.
- **Password storage**: Use the strongest form of one-way encryption available for storage of passwords and never store them in plaintext.
- **Session management**: Ensure the integrity of user login connections by using timeouts and password screensavers to terminate users who have gone idle.

ExamAlert

The CISSP exam will expect you to understand some terminology. For example, you need to know that *clipping level* refers to a logon limit—a threshold or limit that must be reached before action is taken. A big part of preparing for the exam is understanding the terms that might be used and being able to apply them in the context of the test question.

Another area of concern is password management. Organizations have developed different methods to address the password management needs of a complex world. Several techniques include the following:

- **Self-service password reset**: This approach allows users to reset their own password. For example, if you cannot access your LinkedIn account, the site allows you to reset your own password.
- **Assisted password reset**: This method provides help desk and other authorized personnel a standardized mechanism to reset passwords. For example, Hitachi Systems makes a web portal product for just this application.
- **Password synchronization**: These systems are used to replicate a user's password so that all systems are synchronized.

Tip

Take a moment to check out the site https://haveibeenpwned.com. It lists more than 10,000,000,000 pwned (that is, compromised) accounts. By entering your email address and phone number at this site, you can quickly determine if these credentials have been put at risk due to a data breach.

One approach to creating good passwords is to use passphrases. A *passphrase* is often a modified sentence or phrase, like "Uaremy#1lady4l!fe." After you enter a passphrase into a computer system, software converts, or *hashes*, that phrase into a stronger virtual password that is harder for an attacker to crack. Using a passphrase adds another layer of protection because it involves a secret key.

Static and Dynamic Passwords

When evaluating password-based authentication, it is important to consider what type of password-based system is being used. Is it a static, dynamic, or cognitive password system?

Static passwords are fixed and do not normally change. For example, I once set up a ProtonMail account for email and assigned a password. This password remained in effect until I no longer used the account. *Dynamic passwords* are also known as *single-use passwords* and can be thought of as the facial tissue of the security world: You use them once or for a short period, and then they are discarded. One-time passwords might be provided through a token device that displays the time-limited password on an LCD screen. Finally, there are cognitive passwords, which are discussed next.

Tip

Cracking passwords is just one technique that hackers can attempt. Attacks against access control systems can also include directly targeting the hashes. There are tools to attempt this remotely, and attackers can also attempt to gain physical access and carry out hashing attacks.

Cognitive Passwords

Cognitive passwords are a password mechanism that has gained popularity and can be used for identity proofing. For example, when signing up for a service, you may be asked to provide answers to personal questions about your past addresses and information that is unique to you, such as your email address or information that would be difficult for others to know about you. The following are some examples:

- What country were you born in?
- What department do you work for?
- What is your pet's name?
- What is the model of your first car?
- What is your mother's maiden name?

Later, when you log in to the service again, you need to answer some or all of these questions again. If you answer the questions correctly, you are authenticated. Cognitive passwords are widely used during enrollment processes and when individuals call help desks or request other services that require authentication.

Cognitive passwords are not without problems. For example, if your name is Adam Sandler, and the question you need to answer is "What's your hometown?" anyone who knows that you grew up in Manchester, New Hampshire, might easily access your account.

Cognitive passwords are most commonly used in self-service password reset systems. If you forget your password, you are prompted with several questions that you answered during registration to verify your authenticity. If you answer correctly, the password is emailed or sent to you to restore access.

ExamAlert

CISSP exam candidates must understand the strengths and weaknesses of passwords and how password-based authentication can be enhanced. Passwords should always be created by means of a one-way process (hashing), should be randomized (salted), and should never be stored in plaintext.

Something You Have (Type 2): Tokens, Cards, and Certificates

Something you have can be a token, smart card, magnetic stripe card, or certificate.

One of the most common examples of type 2 authentication is a token. If you go to a sports event, you are likely to need a token—in the form of a ticket—to enter the game. In the world of network security, a token can be a *synchronous token* or an *asynchronous token* device. Tokens are widely used with *one-time passwords* (*OTPs*), or single-use passwords, which change every time they are used. OTPs are often implemented with tokens.

A great feature of token-based devices is that they can be used for two-factor authentication. Although physical tokens and key fobs can suffer from problems like battery failures and device failures, using tokens offers a much more secure form of authentication than using passwords.

Synchronous Tokens

Synchronous tokens are synchronized to the authentication server. This type of system works by means of a clock or time-based counter. Each individual passcode is valid for only a short period. Even if an attacker were able to intercept a token-based password, it would be valid for only a limited time. After that small window of opportunity, it would have no value to an attacker. For example, RSA's SecurID changes user passwords every 60 seconds. Figure 6.5 shows an example.

Asynchronous Tokens

Asynchronous token devices are not synchronized to the authentication server. These devices use a challenge/response mechanism and usually require the user to press a key on the token and on the authentication server. The server sends the user a random value that the user must enter into the device along with a username and password. This method is considered strong authentication as it is multifactor authentication (something you know and something you have). Figure 6.6 shows an example.

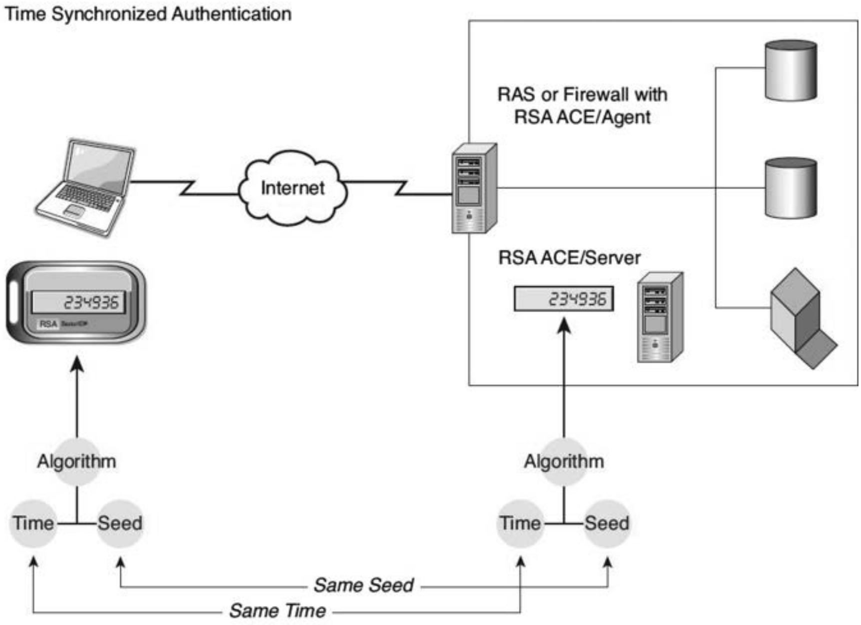


FIGURE 6.5 RSA Token Authentication

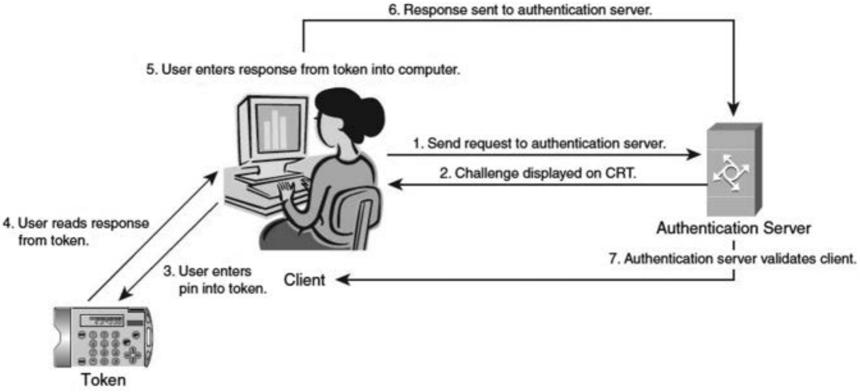

6. Response sent to authentication server.
5. User enters response from token into computer.
1. Send request to authentication server.
2. Challenge displayed on CRT.
4. User reads response from token.
Authentication Server
7. Authentication server validates client.
3. User enters pin into token.
Client
Token

FIGURE 6.6 Asynchronous Token Authentication

Cards

Card-based authentication can be accomplished by means of a smart card, memory card, or magnetic stripe card. A smart card is an intelligent token with an embedded integrated circuit chip. It provides not only memory capacity but computational capability because of its built-in microprocessor. There are several types of smart cards:

- **Contact smart cards**: When this type of card is inserted into a reader, electrical contacts touch the card in the area of the integrated circuit (IC). These contacts provide power and a data path to the smart card.
- **Contactless smart card**: When this type of card is brought near a reader, an embedded antenna provides power to the IC. When the correct PIN is entered into the smart card reader, processing begins. Figure 6.7 shows an example of a generic smart card.

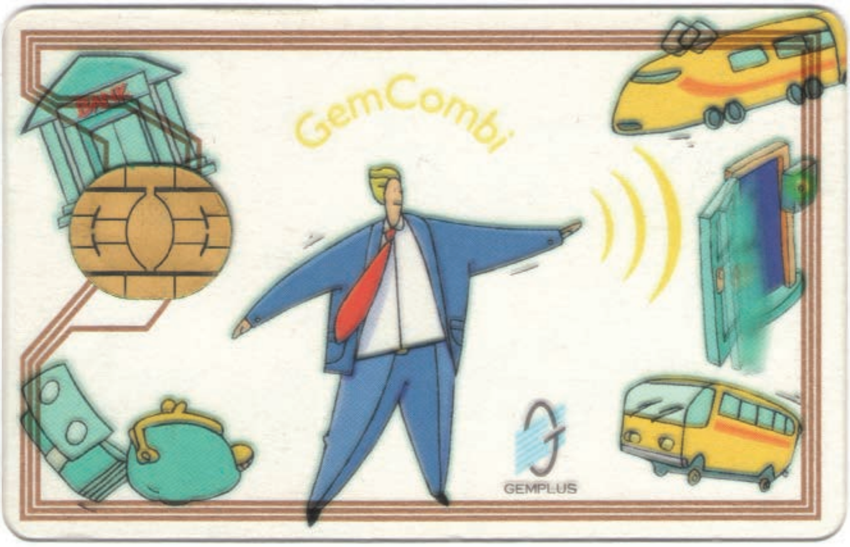


FIGURE 6.7 **Generic Smart Card**

Memory cards are like smart cards but cannot process information. They must be used in conjunction with readers and systems that can process the data held on the memory cards. One of the primary advantages of a memory card is that, unlike passwords, memory cards require the user to possess the card to perform authentication.

An older form of a card token is the magnetic stripe card, established as a widely used standard in the 1970s. The magnetic stripe contains information used to authenticate the user. Care must be exercised in the storage of information on a magnetic card. Although plaintext should not be used, some credit cards still hold information in plaintext. Magnetic stripe readers are cheap and easy to use. Anyone possessing such a device and a PC can steal card information anywhere cards are used, such as at a restaurant or store. Memory cards typically hold a PIN that, when activated by a computer system, pulls authentication information from a database.

Certificates

Some authentication methods, such as Protected Extensible Authentication Protocol (PEAP) and Extensible Authentication Protocol (EAP), can use certificates for authentication of computers and users. Certificates can reside on a smart card or can be used by Internet Protocol Security (IPsec) and Secure Sockets Layer (SSL) for web authentication. These digital certificates provide some basic information to prove the identity of the holder.

Digital certificates typically contain the following critical pieces of information:

- Identification information such as username, serial number, and validity dates of the certificates
- The public key of the certificate holder
- The digital signature of the signature authority, which is critical because it validates the entire package

X.509 is the standard for digital signatures and specifies information and attributes required for the identification of a person or a computer system. Version 3 is the most current version and is considered a secure standard for storing digital certificates in tokens.

Something You Are (Type 3): Biometrics

Biometrics is a means of authentication based on personal attributes or behavioral or physiological characteristics that are unique to an individual. Personal attributes are more closely related to identity features such fingerprints and retina scans, whereas an example of a behavioral trait is the way an individual signs his or her name, referred to as signature dynamics. (Signature dynamics is not the same as a digital signature.) Biometrics is a very accurate means of authentication but is typically more expensive than the password systems discussed earlier in this chapter.

Many organizations are using biometric authentication systems as a way to meet the need for stronger security. Biometric authentication offers the capability of unique authentication of every single person on the planet. Biometric systems work by recording information that is very minute and unique to every person.

When a biometric system is first used, the system must develop a database of information about each user. This is considered the enrollment period. When enrollment is complete, the system is ready for use. For example, if an enrolled employee places her finger on her company laptop's fingerprint scanner, the scanner compares the ridges and creases on the employee's finger to the fingerprint identified as belonging to that individual in the device's database. This process is considered a one-to-one match of the individual's biometric data.

In reality, a user's unique attribute value is converted into a binary value and then hashed before being stored in an authentication server. Different biometric systems have varying levels of accuracy and sensitivity.

> **Note**
>
> In organizations that implement strong security, a user may use multiple forms of authentication. A user might enter a password on his computer, use his fingerprint to unlock the phone and approve a text containing a one-time password, and then enter that one-time password into his computer. Microsoft MFA and others provide this type of functionality. This type of defense-in-depth approach is useful for increasing security and reducing risk.

Attributes are measured by the percentage of Type I and Type II errors they produce:

- **Type I errors**: These errors occur when individuals who should have been allowed access were not; these errors are compiled into the *false rejection rate* (*FRR*). The FRR is often called the insult rate because valid users are insulted that they were denied access even though they are legitimate users.
- **Type II errors**: These errors occur when individuals or subjects got in but should not have been allowed access; these errors are compiled into the *false acceptance rate* (*FAR*). Consider a situation where I, the author of this book and not an employee of your organization, show up at your work site and attempt to authenticate to one of the organization's systems. If I were allowed in, that would be an example of a Type II error.

Together, the FRR and FAR can be used to determine the overall accuracy of a system. Suppose you have been asked to assess similar biometric devices. In this situation, you can use the *crossover error rate* (*CER*) to select the best system for your organization. This rate is determined by mapping the point at which Type I errors equal Type II errors. As illustrated in Figure 6.8, the lower the CER, the more accurate the biometric system. For example, if system A has a CER of 4, and system B has a CER of 2, system B has the greater accuracy.

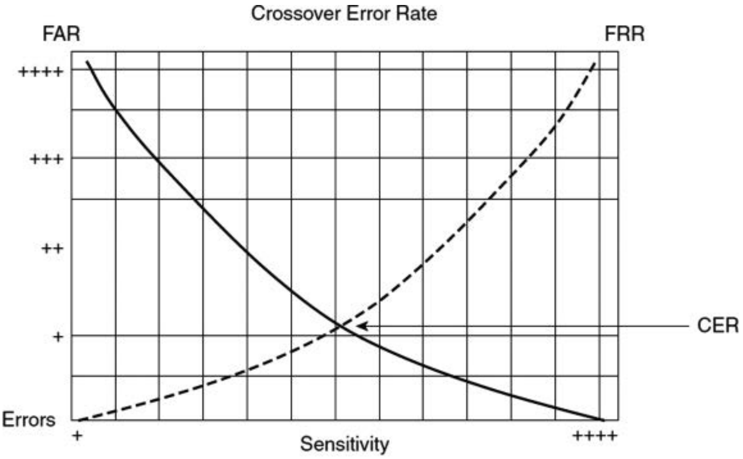


FIGURE 6.8 **Crossover Error Rate**

ExamAlert

Before you take the CISSP exam, make sure you understand the difference between Type I and Type II errors and the CER. The FAR is considered the most critical error rate to examine, and the CER is considered to be the best measurement of biometric system accuracy.

The following are some of the most common biometric authentication systems. These systems are listed in order of best response times and lowest error rates:

- **Hand geometry recognition**: This type of biometric system uses the unique geometry of a user's fingers and hand—shape, length, and width—to determine the user's identity. It is one of the most mature biometric techniques.

- **Iris recognition**: An iris recognition system is an accurate biometric system because there are more than 400 points of reference when matching the irises of an individual's eyes. This type of system typically works by taking a picture of the iris and comparing it to one stored in a database. Benefits include high accuracy, passive scanning, and no exchange of bodily fluids.

- **Retina pattern recognition**: This is another ocular-based technology that scans the blood vessels in the back of the eye. It requires users to place their eye close to the reader. Although retina-based biometric systems are considered very accurate, drawbacks include the fact that the retina can change due to medical conditions like diabetes and pregnancy and the fact that bodily fluids can be exchanged due to the need for proximity. Because of privacy concerns related to revealed medical conditions, retina scans are not readily accepted by users.

- **Fingerprint recognition**: This method is widely used for access control to facilities and items such as laptops and smartphones. It works by distinguishing up to 30 to 40 details about the peaks, valleys, ridges, and minutiae of the user's fingerprint. However, many commercial systems limit the number that is matched to around 8 to 10.

- **Facial recognition**: This method requires a user to place her face in front of a camera. The facial scan device performs a mathematical comparison with the face prints (*eigenfeatures*) it holds in a database to allow or block access. These systems have grown in popularity over the past few years and are included on a number of smartphones and tablets.

- **Voice recognition**: Voice analysis for identification and authentication can be used for telephone applications. It has been around for several decades. The 1992 movie *Sneakers* includes the line, "Hi, my name is Werner Brandes. My voice is my passport. Verify me." However, voice recognition is vulnerable to replay attacks.

Different biometric systems have varying levels of accuracy. For example, the accuracy of fingerprint-scanning systems is based on fingerprint patterns and minutiae. Fingerprint patterns include arches, loops, and whorls, and minutiae include ridge endings, bifurcations, and short ridges (see Figure 6.9).

Although the number of minutiae varies from finger to finger, the information can be stored electronically in file sizes that are usually between 250 and 1,000 bytes. When a user logs in, the stored file containing the minutiae is compared to the finger being scanned.

FIGURE 6.9 **Fingerprint Patterns and Minutiae**

A number of considerations are important when deploying a biometric system:

- **Employee buy-in**: Users might not like or want to interact with the system, and the performance of the system will suffer. Some individuals oppose biometric authentication systems for privacy-related reasons. Some users find biometric devices too Big Brotherish. Some might not like the idea that the organization's new retina scanner could be used to detect medical conditions, such as pregnancy. Users who perform physical labor or work in an unclean environment might find fingerprint scanners frustrating. Sanitization can be an issue with biometrics because users often have to touch authentication devices. When considering biometric systems, you should ensure that they do not cause undue psychological stress for users or raise unwarranted privacy issues.
- **The physical status of the user**: Users who are physically disabled might find eye scanners difficult to reach. Those missing hands or fingers will be unable to use fingerprint readers, palm scanners, or hand geometry systems.
- **Whether the user can use the biometric**: Some users may not be able to use the biometric. For example, some people cannot have their fingerprints read. This may be genetic or based on the job the person does. For example, brick layers and bank tellers typically cannot use fingerprint readers because their fingerprints may be worn off.

A final consideration with biometrics is selection. With so many technologies, it takes a significant amount of effort to choose a system that meets user criteria and is technologically feasible. One tool that can aid in this task is the International Biometric Group's Zephyr Analysis, which provides a means of evaluating different biometric technologies based on two categories:

- **User criteria**: Effort and intrusiveness
- **Technology criteria**: Cost and accuracy

ExamAlert

CISSP exam candidates must understand the different ways in which biometric systems can be evaluated. When comparing like devices, the CER can be used; for unlike devices, a Zephyr analysis is the preferred method.

Strong Authentication

To make authentication stronger, you can combine several of the methods discussed so far in this chapter. This combination is referred to as *multifactor*, or *strong*, *authentication*. The most common form of strong authentication is two-factor authentication. Tokens combined with passwords provide effective and strong authentication. If you have a bank card, you are familiar with two-factor authentication. Bank ATMs require two items to successfully access an account: something you have (bank card) and something you know (your PIN).

The decision to use strong authentication depends on your analysis of the value of the assets being protected. What are the dollar values of the assets being protected? What might unauthorized access cost the organization in dollars, lost profit, potential public embarrassment, or liability?

ExamAlert

CISSP exam questions are known for their unique style of wording. For example, the exam is particular about the term *two-factor authentication*, which requires items from two of the three categories. As such, a password and a token would be two-factor authentication, whereas a password and a PIN would not (because they are both something you have).

Identity Management Implementation

Identity management involves a lifecycle of access control from account creation to decommissioning and the management of each process in between (see Figure 6.10). Employees are hired, change roles, are promoted, gain additional duties, and are fired or resign. This constant state of flux requires organizations to develop effective user management systems to handle provisioning and deprovisioning. *User provisioning* is the creation, management, and deactivation of services and accounts of user objects.

ExamAlert

The processes of provisioning and deprovisioning involve giving users or applications the levels of access they need to do their jobs and then taking them away when their jobs are complete.

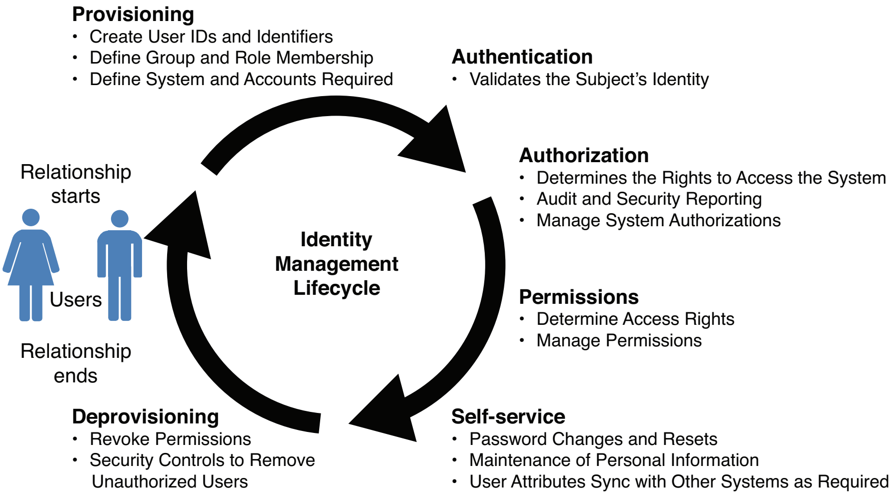

Provisioning
• Create User IDs and Identifiers
• Define Group and Role Membership
• Define System and Accounts Required
Authentication
• Validates the Subject's Identity
Authorization
• Determines the Rights to Access the System
• Audit and Security Reporting
• Manage System Authorizations
Permissions
• Determine Access Rights
• Manage Permissions
Self-service
• Password Changes and Resets
• Maintenance of Personal Information
• User Attributes Sync with Other Systems as Required
Deprovisioning
• Revoke Permissions
• Security Controls to Remove Unauthorized Users
Relationship starts
Users
Relationship ends
Identity Management Lifecycle

FIGURE 6.10 **Identity Management Lifecycle**

Provisioning and deprovisioning are just the start of the process. Identity management must also include the following:

- Establishing, managing, and closing accounts
- Periodically performing account review
- Periodically rescreening individuals in sensitive positions

Typically when an account is established, a profile is created. *Profile management* involves the control of information associated with an individual or a group. Profiles can contain information such as name, age, date of birth, address, and phone number. Modern corporations have so much data to manage that they use systems such as directory management systems in order to simplify the management of data. One of the primary disadvantages of such systems has to do with integration of legacy systems. Mainframes, non-networked applications, and applications written in archaic languages like Fortran and COBOL make it difficult to centrally manage users. (And yes, some legacy systems that use this technology are still around.)

Another approach to the management of user access to multiple sites is federation. *Federation* is used in identity management systems to manage identity across multiple platforms and entities. Some of the directory standards used to ease user management are the X.500 standard, Lightweight Directory Access Protocol (LDAP), and Active Directory.

Today's systems are much more distributed than those of the past and have a much greater reliance on the Internet. In addition, there has been a move toward service-enabled delivery of services. There has also been a move to create web services that have a more abstract architectural style, known as service-oriented architecture (SOA), which attempts to bind together disjointed pieces of software. SOA allows for an organization with distributed departments using different systems and services in different business domains to access services with security designed into the process. For example, suppose the legal department and the IT department provide different services on different systems, and you want to have the legal department programs loaded on IT department systems. With the use of a web portal, the other department can access the service if required by using SAML and HTTP.

A security professional should have some knowledge of components of identity management, such as the following:

- **WS-Security**: WS-Security is an extension to Simple Object Access Protocol (SOAP) that is designed to add security to web services.
- **XML**: Years ago, Hypertext Markup Language (HTML) dominated the web. Today, Extensible Markup Language (XML) is the standard framework. XML is a standard that allows for a common expression of metadata. XML typically follows the SOAP standard.

- **SPML**: Service Provisioning Markup Language (SPML) is an XML-based framework that can be used to exchange access control information between organizations so that a user logged in to one entity can have the access rights passed to the other.

Single Sign-On (SSO)

Single sign-on (SSO) addresses a problem that is common for all users and administrators: the need to log on multiple times to multiple systems in an organization. Each of many systems in an organization may require a user to remember a different username and password combination. When people become tired of trying to remember such information, they look for shortcuts. The most common shortcut is just to write down the information. Walk around your office, and you might see that many of your coworkers have regrettably implemented this practice. SSO is designed to address this problem by permitting users to authenticate once to a single authentication authority and then access all other protected resources without being required to authenticate again. Kerberos and SESAME are two examples of SSO.

Before you run out and decide to implement SSO at your organization, you should be aware that it is expensive. In addition, the main benefit of SSO is also its main downside: It simplifies the process of gaining access to multiple systems for everyone—and threat actors can also take advantage of this convenience. Multifactor authentication (MFA) can help reduce the risk.

Caution

Thin clients can be considered a type of single sign-on system because the thin client holds no data. All information is stored in a centralized server. Thus, after a user is logged in, there is no reason for that user to authenticate again.

Kerberos

Kerberos, created by Massachusetts Institute of Technology (MIT), is a network authentication protocol that uses secret-key cryptography. Kerberos has three parts: a client, a server, and a trusted third party called the key distribution center (KDC) to mediate between them. Clients obtain tickets from the KDC, and they present these tickets to servers when connections are established.

Kerberos tickets represent the client's credentials. Kerberos relies on symmetric key cryptography (shared, or *secret* key, cryptography). Version 5 of Kerberos was implemented with Data Encryption Standard (DES). However, Advanced Encryption Standard (AES), which has superseded DES, is supported in later versions of Kerberos and operating systems like Microsoft Windows 7, 8, 10, and Server 2012 and others. Kerberos communicates through an application programming interface (API) known as Generic Security Service (GSS-API). You need to understand a number of terms related to Kerberos:

- **Ticket**: A ticket is generated by the KDC and given to a principal for use in authenticating to another principal.
- **Realm**: A realm is a domain that consists of all the principals for which the KDC provides security services; it is used to logically group resources and users.
- **Credentials**: Credentials are a ticket and a service key.
- **Principal**: A principal can be a user, a process, or an application. Kerberos systems authenticate one principal to another.

The KDC is a service that runs on a physically secure server. The KDC consists of two components:

- **Authentication service**: The authentication service issues ticket-granting tickets (TGTs) that are good for admission to the ticket-granting service (TGS). Before a network client can get a ticket for a service, it must obtain a TGT from the authentication service.
- **Ticket-granting service**: Clients receive tickets to specific target services.

Note

Keep in mind that the TGT is an encrypted identification file with a limited validity window. The TGT is temporarily stored on the requesting principal's system and is used so that the principal does not have to type in credentials multiple times to access a resource.

The basic operation of Kerberos, as depicted in Figure 6.11, is as follows:

1. The client asks the KDC for a ticket, making use of the authentication service.
2. The client receives the encrypted ticket and the session key.

3. The client sends the encrypted TGT to the TGS and requests a ticket for access to the application server. This ticket has two copies of the session key: One copy is encrypted with the client key, and the other copy is encrypted with the application server key.
4. The TGS decrypts the TGT using its own private key and returns the ticket to the client, granting it access to the application server.
5. The client sends this ticket, along with an authenticator, to the application server.
6. The application server sends confirmation of its identity to the client.

Note

Kerberos authenticates only authentication traffic; subsequent communications are not protected. If the supplicant uses an insecure protocol like File Transfer Protocol (FTP), the network traffic is in plaintext.

Although Kerberos can provide authentication, integrity, and confidentiality, it's not without weaknesses. One weakness is that Kerberos cannot guarantee availability. Some other weaknesses are as follows:

- Kerberos is time-sensitive; therefore, it requires all system clocks to be closely synchronized.
- The tickets used by Kerberos, which are authentication tokens, can be sniffed and potentially cracked.
- If an attacker targets the Kerberos server, it can prevent anyone in the realm from logging in. It is important to note that the Kerberos server can be a single point of failure.
- Secret keys are temporarily stored and decrypted on user workstations, making them vulnerable to an intruder who gets access to the workstation.
- Kerberos is vulnerable to brute-force attacks.
- Kerberos may not be well suited for large environments that have many systems, applications, users, and simultaneous requests.

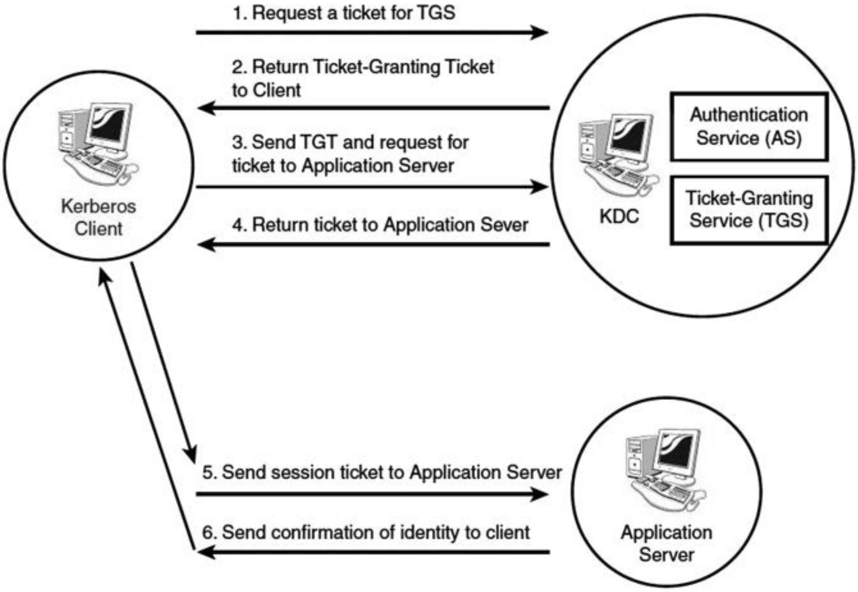

1. Request a ticket for TGS
2. Return Ticket-Granting Ticket to Client
3. Send TGT and request for ticket to Application Server
4. Return ticket to Application Sever
Kerberos Client
KDC
Authentication Service (AS)
Ticket-Granting Service (TGS)
5. Send session ticket to Application Server
6. Send confirmation of identity to client
Application Server

FIGURE 6.11 **Kerberos Operation**

SESAME

Kerberos is the most widely used SSO solution, but there are other options, including *Secure European System for Applications in a Multivendor Environment* (SESAME). The SESAME project was developed to address one of the biggest weaknesses in Kerberos: plaintext storage of symmetric keys. Whereas Kerberos uses only symmetric encryption, SESAME uses both symmetric and asymmetric encryption. In addition, SESAME incorporates MD5 and CRC32 hashing and uses two certificates. One of these certificates is used to provide authentication, as in Kerberos, and the second certificate is used to control the access privileges assigned to a client.

SESAME uses Privilege Attribute Certificates (PACs). A PAC contains the requesting subject's identity, access capabilities of the subject, and the life span of the subject requiring access. KryptoKnight by IBM and NetSP, an older KryptoKnight derivative, are also SSO technologies, but they are not widely deployed. Although you are unlikely to see these systems, you should know their names and that they are used for SSO as they might show up on the exam.

Authorization and Access Control Techniques

With a user identified and authenticated, the next step is authorization. What can a user who is logged in access, and what types of rights and privileges does that user have? At the core of this discussion is how subjects access objects and what they can do with these resources after access is established. There are five primary types of access control:

- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Role-based access control (RBAC)
- Attribute-based access control (ABAC)
- Rule-based access control

These might not be concepts that you are used to thinking about; however, access control decisions are made early on in the design of an operating system. For example, early Microsoft Windows products had a peer-to-peer design; this is much different from SUSE Linux 15.0, which has a Kubernetes management platform.

The following sections look at the five types of access control in detail.

Discretionary Access Control (DAC)

With DAC, access control is left to the owner's discretion. It is similar to a peer-to-peer computer network, where each user is left to control his or her own system and resources. The owner is authorized to determine whether other users have access to files and resources. One significant problem with DAC is that its effectiveness is limited by the user's skill and ability. A user who is inexperienced or simply doesn't care can easily grant full access to files or objects under his or her control.

DAC has two primary components:

- **File and data ownership**: Every object in a system must have an owner. Any object that does not have an owner is left unprotected.
- **Access rights and permissions**: DAC controls the access rights of an individual. Variations exist, but a basic *access control list* (*ACL*) checks read, write, or execute privileges.

The ACL identifies users who have authorization to specific information. This is a dynamic process that allows data to be easily shared. For example, I might inform my son that he may not download any more music from the Internet onto his computer upstairs. From my computer in the den, my son might simply deny me access to the folder he has been downloading music into to prevent me from accessing it to monitor his activities. This example also demonstrates the similarity of DAC to a peer-to-peer network in that users are in charge of their own resources and data.

Table 6.7 shows a sample ACL, with columns defining access to objects. Each row in the table shows a subject's capabilities and what actions can be taken.

TABLE 6.7 **Sample Access Control List**

Subject	Object 1	Object 2	Object 3	Object 4
Jeff	Full control	Full control	Full control	Full control
Michael	Read	Read	Read write	No access
Christine	Read	Read write	No access	No access

You can think of capabilities as the actions that a specific user can perform within the access matrix. DAC is based on this matrix, and you can think of it as a means to establish access permission of a subject to an object.

Although the data owner can create an ACL to determine who has access to a specific object, mistakes can lead to loss of confidentiality, and no central oversight exists, as in other more restrictive types of access control.

Mandatory Access Control (MAC)

MAC is static and based on a predetermined list of access privileges; therefore, in a MAC-based system, access is determined by the system rather than by the user. A MAC system uses labels and clearances. Figure 6.12 shows the differences between DAC and MAC.

MAC is typically used by organizations that handle highly sensitive data, such as the U.S. Department of Defense, NSA, CIA, and FBI. An example of a MAC system is SELinux. Systems based on MAC use clearance on subjects and mark objects by sensitivity label. For example, the military uses the clearances top secret, secret, confidential, sensitive but unclassified (SBU), and unclassified. (See Chapter 2, "Understanding Asset Security," for a more in-depth discussion of government data classification.)

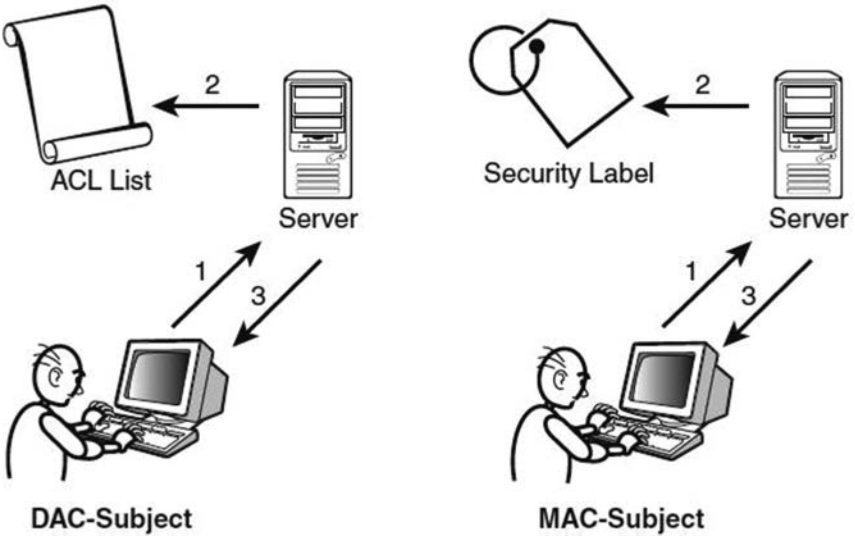


FIGURE 6.12 Differences Between DAC and MAC

You need to know the following terms related to MAC:

- **Object**: Objects are passive entities that provide data or information to subjects.
- **Subject**: A subject is an active entity that can be a user, system, program, or file.

When a subject attempts to access an object, the object's label is examined for a match to the subject's level of clearance. If no match is found, access is denied. MAC excels at supporting the need-to-know concept. Here is an example: Jeff wants to access a top secret file. The file is labeled "top secret, Joint Chiefs of Staff (JCS)." Although Jeff has top secret clearance, he is not JCS; therefore, access is denied. In reality, it is a little more complicated than this example indicates, but remember that the CISSP exam is considered a mile wide and an inch deep. Be sure you know these additional terms related to MAC:

- **Clearance**: Clearance determines the type of information a user can access.
- **Category**: Categories are applied to objects and used to silo information.
- **Sensitivity labels**: These labels are used to classify information.
  As mentioned earlier, the U.S. military uses the labels top secret, secret, confidential, sensitive but unclassified (SBU), and unclassified.

Caution

Any time you see the term *sensitivity label*, you should start thinking MAC because this system is most closely associated with this term.

For the CISSP exam, you should know that MAC systems can be hierarchical, compartmentalized, or hybrid. *Hierarchical designs* work by means of classification levels. Each level of the hierarchy includes the lower levels as well. For example, in a hierarchical system, Dwayne might be cleared for top secret, which means he can also view secret and confidential information because those are less sensitive. If Dwayne were authorized to access only confidential data, however, he would not be able to read up to higher levels like secret. Compartmentalized objects require clearance from a specific domain or group, such as the Department of Homeland Security.

In a *compartmentalized system*, it is possible to separate data into separate categories. For example, Dwayne, who works for the Department of Defense, would not be able to read documents cleared for the State Department; Dwayne would have a top secret—sensitive compartmentalized information (TS-SCI) clearance. The military would be exercising a MAC system with least privileges to ensure that because Dwayne has TS, he has only the necessary access required to complete his job.

A *hybrid design* combines elements of both hierarchical and compartmentalized designs.

Important items to know about MAC include the following:

- It’s considered a need-to-know system.
- It involves more overhead than DAC.
- All users and resources are assigned security labels.

Caution

Although MAC uses a security label system, DAC systems allow users to set and control access to files and resources.

Role-Based Access Control (RBAC)

RBAC, also known as nondiscretionary access control, enables a user to have certain preestablished rights to objects. These rights are assigned to users based on their roles in the organization. The roles almost always map to the organization's structure. Many organizations are moving to this RBAC because it eases access management. For example, if you are the IT administrator of a bank, there are some clearly defined roles, such as bank manager, loan officer, and teller. RBAC allows you to define specific rights and privileges to each group. The users are then placed into the groups and inherit the privileges assigned to their groups. If Joan is a teller and gets promoted to loan officer, all the administrator must do is move her from the teller group to the loan officer group. Many modern OS designs use RBAC.

RBAC is well suited to organizations that have a high turnover rate. Assigning access rights and privileges to a group rather than to an individual reduces the burden on administration. How RBAC is implemented is up to the individuals designing the operating system. For RBAC to work, roles within the organization must be clearly defined in policy.

Your organization might decide to use *static separation of duties* (*SSD*). SSD dictates that a member of one group cannot be a member of another group. Let's say Mike is a member of the network administrators group. In this case, Mike cannot also be a member of the security administrators group or the audit group. For SSD to work, roles must clearly be defined to make it clear where conflicts exist within the organization.

Another design is *dynamic separation of duties* (*DSD*). DSD dictates that a user cannot combine duties during any active session. Let's say Mike is a member of the audit group and the audit management group. If Mike logs on to perform an audit test, he does not have management rights. If Mike logs on under the audit management group, he cannot perform an audit test.

Table 6.8 provides an example of separation of duties.

TABLE 6.8 **Separation of Duties**

Role	Example of Allowed Access
User	Web browsing, approved applications, and changes to desktop appearance
Auditor	Review of firewall logs, server logs, and application logs
Security administrator	Firewall administration, ACL updates, and server patching

Task-based access control (TBAC) is similar to RBAC but instead of being based on roles, it uses tasks. TBAC is based on tasks so that the allowed duties are based on the types of tasks a specific individual would perform. A good example of this can be seen when you access Windows Server 2019. In the user administration group, you can see some predefined profiles, such as print manager, backup manager, and power user. The access assigned to each of these is based on the types of tasks the individual would perform.

Attribute-Based Access Control

Attribute-based access control (ABAC) is a more dynamic, flexible, context-aware and adaptive type of access control. ABAC has a much greater number of possible control variables than RBAC. ABAC has a set of characteristics called *attributes*, which can be any of the following:

- **User attributes**: These attributes include items such as a user's name, role, organization, and security clearance.
- **Environmental attributes**: These attributes include items such as the time of access, location of the data, and current organizational threat levels.
- **Resource attributes**: These attributes include items such as creation date, resource owner, filename, and data sensitivity.

ABAC can control security and access on a more fine-grained basis, and it is implemented to reduce risks due to unauthorized access. For example, ABAC can place granular limits on user access, such as only allowing user access during certain times, in certain regions, or for certain branch offices relevant to the employee in question. Keep in mind that ABAC is complex, and in some cases it may provide more control than is really needed; in such cases, RBAC might be a better option. As a security professional, you must always balance risk and cost. There's no reason to use the more granular option if it is not needed as using it would simply mean incurring additional resource costs.

ABAC is supported by Extensible Access Control Markup Language (XACML), which defines the policies, requests, and architecture. It is based on XML and includes policy decision points (PDPs), which evaluate policies against access requests provided by policy enforcement points (PEPs). A PDP may also need to query a policy information point (PIP) to gather descriptive attributes about the user or any other missing attribute in a request. A policy administration point (PAP) is used to manage the PDP and PIP functionality (see Figure 6.13).

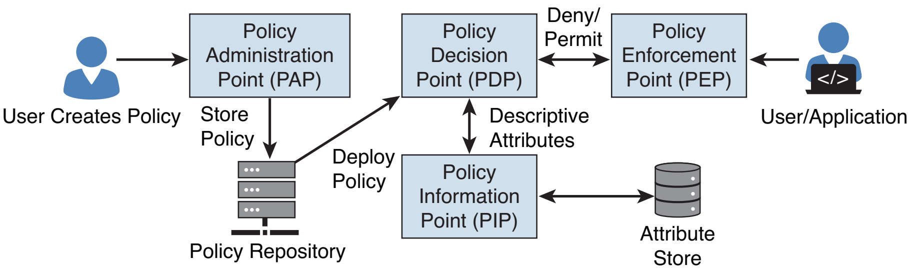


FIGURE 6.13 **XACML ABAC Architecture**

Rule-Based Access Control

Rule-based access control is based on a specific set of rules, much like a router ACL. Rule-based access control is considered a variation of DAC. Rule-based access control involves the following steps:

1. Intercept each request.
2. Compare it to the level of authorization.
3. Make a decision.

For instance, say that a router uses a rule-based ACL that has permissions set to allow web traffic on port 80 and deny Telnet traffic on port 23. These two basic rules define the ACL. ACLs are tied to objects. Permissions can be assigned in three different ways: They can be assigned explicitly or implicitly, or they can be inherited. ACLs have an implicit deny all statement that is the last item processed. A sample Cisco-formatted ACL with both allow (permit) and deny statements is shown here:

```
no access-list 111
access-list 111 permit tcp 192.168.13.0 0.0.0.255 any eq www
access-list 111 deny tcp any any eq telnet
access-list 111 deny icmp any any
interface ethernet0
ip access-group 111 in
```

ExamAlert

Although some people use the terms *access control list* and *capability table* interchangeably, they are not the same. Capability tables are bound to subjects; ACLs are bound to objects.

Other Types of Access Control

Content-dependent access control (CDAC) is based on the content of a resource. CDAC is primarily used to protect databases that contain potentially sensitive data. CDAC is also used to filter out unauthorized traffic and is typically used by proxies or firewalls. For example, you may be able to log in to your organization's SharePoint page and see the number of days you will be expected to travel next month but unable to see when or where the CEO will be traveling during the same period.

Lattice-based access control (LBAC) is a MAC-based type of access control that defines the least upper and greatest lower bounds. An upper bound is called a *join*, and a lower bound is called a *meet*. LBAC deals with access in complex situations. It allows access only if the subject's capability is greater than or equal to that of the object being accessed. For example, Figure 6.14 demonstrates the boundaries in LBAC. If you were cleared for top secret, you could read the level below, which is secret.

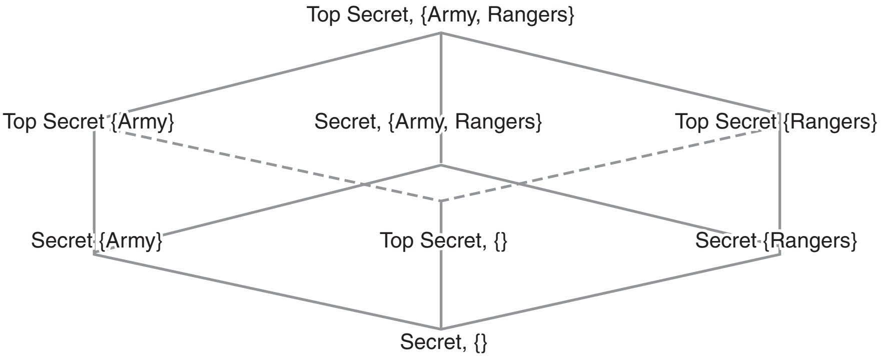


FIGURE 6.14 **Lattice-Based Access Control**

ExamAlert

Don't worry about the abbreviations of the types of access control. The CISSP exam will spell out these terms and most others. You are not expected to memorize the abbreviations but are expected to know the concepts.

Centralized and Decentralized Access Control Models

Access control models can be divided into two distinct types: *centralized* and *decentralized*. Depending on an organization's environment and requirements, one methodology typically works better than the other.

Centralized Access Control

Centralized access control systems maintain user IDs, rights, and permissions in one central location. Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access-Control System (TACACS), and Diameter are all examples of centralized access control systems. Characteristics of centralized systems include the following:

- One entity makes all access decisions.
- Owners decide what users can access, and the administration supports these directives.

Users are typically authenticated using one of the following authentication protocols:

- **Password Authentication Protocol (PAP)**: PAP uses a two-way handshake to authenticate a peer to a server when a link is initially established, but it is considered weak because it transmits passwords in plaintext. PAP also offers no protection against replay or brute-force attacks.
- **Challenge-Handshake Authentication Protocol (CHAP)**: CHAP uses a one-way hash function and a handshake to authenticate the client and the server. This process is performed when a link is initially established and may be repeated at defined intervals throughout the session. Although it is better than PAP, it is susceptible to replay attacks.
- **MS-CHAPv2**: This authentication method has been extended to authenticate both the client and the server. In addition, MS-CHAPv2 uses stronger encryption keys than CHAP and MS-CHAP.
- **Extensible Authentication Protocol (EAP)**: EAP is a framework that allows for more than just standard username and password authentication. It allows various authentication mechanisms, such as MD5 Challenge-Response, token cards, and digital certificates.

Caution

Regardless of the access control model being used, periodic access reviews and audits should be performed to determine if an organization's security policy related to user accounts is being followed. Audits related to provisioning, usage, and revocation are necessary. One key goal is to assess whether least privilege policies are being followed.

RADIUS

RADIUS is an open UDP client/server protocol defined in RFCs 2058 and 2059 that provides three services: authentication, authorization, and accountability. RADIUS facilitates centralized user administration and keeps all user profiles in one location shared by all remote services. When a RADIUS client communicates with a RADIUS server, it uses attribute/value pairs (AVPs), which are sets of defined fields that accept certain values. RADIUS was originally designed to provide protection against attacks over dialup connections. It has been used by ISPs for years and is now also used by mobile employees and integrated with Lightweight Directory Access Protocol (LDAP). RADIUS is considered a triple-A protocol (because it provides authentication, authorization, and accountability), and all these services are performed together. It is important to note that RADIUS only encrypts the user's password as it travels from the client to the server, and other information is sent in plaintext.

Note

LDAP can be used by a cluster of hosts to allow centralized security authentication as well as access to user and group information.

RADIUS is also used for wireless LAN authentication. The IEEE designed EAP to easily integrate with RADIUS to authenticate wireless users. A wireless user takes on the role of the supplicant, and the access point serves as the client. RADIUS uses UDP port 1812 for authentication and authorization services and UDP port 1813 for accounting of RADIUS services.

If an organization has an existing RADIUS server that's being used for remote users, it can be put to use authenticating wireless users, too.

RADIUS involves the following steps (see Figure 6.15):

1. The user connects to the RADIUS client.
2. The RADIUS client requests credentials from the user.

3. The user enters credentials.
4. The RADIUS client encrypts the credentials and passes them to the RADIUS server.
5. The RADIUS server accepts, rejects, or challenges the credentials.
6. If the authentication is successful, the user is authenticated to the network.

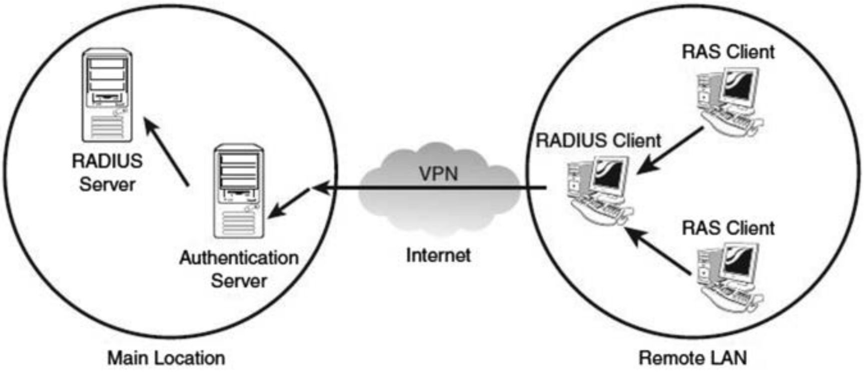


FIGURE 6.15 **RADIUS Authentication**

TACACS

TACACS allows authentication, authorization, and auditing functions to be split up, which gives an administrator more control over its deployment. (In contrast, RADIUS does not split up these functions.) TACACS is highly Cisco- and Microsoft-centric, and it is considered proprietary. TACACS has failed to gain the popularity of RADIUS, and it is now considered a somewhat dated protocol.

Two variations of TACACS are available: XTACACS (Extended TACACS) and TACACS+. XTACACS separates the authentication, authorization, and accountability processes, and TACACS+ features two-factor authentication and security tokens. TACACS+ is a completely new and revised protocol that is incompatible with other versions of TACACS.

There are some major differences between RADIUS and TACACS+. Whereas RADIUS only encrypts the password sent between the client and the server, TACACS+ encrypts all the information. TACACS+ also allows for more administration and has more AVPs because it can split up the AAA protocols. In addition, whereas RADIUS uses UPD, TACACS+ uses TCP.

Diameter

The creators of Diameter had a sense of humor: They named the protocol as they did because in a circle, the diameter is twice the radius. Actually, Diameter is enhanced RADIUS in that was designed to do much more than provide services to dialup users. A single Diameter peer can support over a million concurrent Diameter sessions, and Diameter can even do peer-to-peer authentication. Diameter, which is detailed in RFC 3588, can use TCP, UDP, or Stream Control Transport Protocol (SCTP). Diameter can support protocols and devices that were not even envisioned when RADIUS and TACACS were created, such as VoIP (voice over IP), Ethernet over PPP, and mobile IP. Diameter is considered a very secure solution because cryptographic support of IPsec or TLS is mandatory.

Diameter is designed to use two protocols. The first is the base protocol used to provide secure communication between Diameter devices and to enable various types of information to be transmitted, such as headers, security options, commands, and AVPs.

The second protocol is really a set of extensions. Extensions are built on top of the base protocol to allow various technologies to use Diameter for authentication. This component is what interacts with other services, such as VoIP, wireless, and cell phone authentication. In a world of the Internet of Things, Internet of Everywhere, and System of Systems, where organizations are subscribing to BYOD, and all the intelligence is at the edge of the network and growing, Diameter creates the way forward for authentication of these devices into the organization's network. It provides granular access and authorization beyond what an Active Directory domain controller can do.

Finally, Diameter is not fully backward compatible with RADIUS, but there are several options for upgrading RADIUS component communication paths.

Decentralized Access Control

Decentralized access control systems store user IDs, rights, and permissions in different locations throughout the network. For example, domains can be thought of as a form of decentralized access control. Large organizations typically establish multiple domains along organizational boundaries, such as manufacturing, engineering, marketing, sales, or R&D; or based on geographic boundaries, like New York, Atlanta, San Jose, and Houston. When more than one domain exists, there has to be some type of trust between them. A trust is simply a separate link between domains that is necessary to resolve their different security policies and security databases. Trusts can be one way or two way.

The important concept here is that although all of a domain's authentication is centralized on domain controllers, a domain's access control is distributed throughout the domain's members. Access to resources is assigned and defined on the resource wherever it might reside in the domain.

Characteristics of a decentralized system include the following:

- Gives control to individuals closer to the resource, such as department managers and occasionally users
- Maintains multiple domains and trusts
- Does not use one centralized entity to process access requests
- Is used in database management systems (DBMS)
- Is peer-to-peer in design
- Lacks standardization and overlapping rights and might include security holes

Audits and Monitoring

Regardless of what method of authorization is used and what types of controls are enforced, individuals must be held accountable. For auditing to be effective, administrative controls are needed in the form of policies to ensure that audit data is reviewed on a periodic basis and not just when something goes wrong. Technical controls are needed so that user activity can be tracked within a network. Physical and technical controls are needed to protect audit data from being tampered with.

Although auditing is used only after the fact, it can help detect suspicious activity or identify whether a security breach has taken place. For example, security administrators often review logs for failed logon attempts only, whereas successful logons hurt most and can show you who is in the network but should not be. For example, say that Mike, who works 9 to 5 Monday through Friday in Houston, has been logging in Sundays from 12 to 9 p.m. from San Jose. Maybe Mike is on vacation, but there is also a possibility that someone is using his account. Since he has a valid user account, however, the unusual logins do not raise an alarm.

Monitoring Access and Usage

Computer resources are a limited commodity provided by an organization to help meet its overall goals. Most people have no problem using computer resources at work for their own personal use. According to information on the Personal Computer World site, one-third of time spent online at work is not work related, and more than 75% of streaming radio downloads occur between 5 a.m. and 5 p.m.

Accountability must be maintained for network access, software usage, and data access. In a high-security environment, the level of accountability should be substantial, and the organization should hold users responsible by logging and auditing their activities. Of particular concern is system accounts. System accounts such as administrator or root are commonly targeted and often exploited by attackers. Therefore, system account access reviews should be part of an organization's normal audit process.

Sometimes security administrators attempt to disconnect an account name from its function by renaming the account to something that looks more like a traditional username or randomly generated name. This is an example of security by obscurity, but this practice is insufficient to protect against anything more than trivial exploitation efforts.

Audits and security reviews can be annual events or may be triggered by occurrences such as these:

- A user account is no longer appropriate for the user's job description or role.
- A user is voluntarily or involuntarily terminated from an organization.
- A user account has been inactive for a period that surpasses organizational policy.
- The user account privileges have experienced unnecessary access aggregation.

Audit logs should be transmitted to a remote centralized site. Centralized logging makes it easier for the person assigned the task to review the data. Exporting logs to a remote site also makes it harder for hackers to erase or cover their activity. If there is a downside to all this logging, it is that all the information must be recorded and reviewed. A balance must be found between collecting audit data and maintaining a manageable log size. Reviewing this information can be expedited by using *audit reduction tools*, which parse the data and eliminate unneeded information. Another useful tool is a variance detection tool, which looks for trends that fall outside the realm of normal activity. For example, if an employee normally enters the building around 7 a.m. and leaves about 4 p.m. but is seen entering at 3 a.m., a variance detection tool would detect this abnormality.

Intrusion Detection Systems (IDSs)

IDSs play a critical role in the protection of IT infrastructure. *Intrusion detection* involves monitoring network traffic, detecting attempts to gain unauthorized access to a system or resource, and notifying the appropriate individuals so that appropriate actions can be taken. An IDS is designed to function as an access control monitor. Intrusion detection is a relatively new technology, born in the 1980s when James Anderson put forth the concept in a paper titled *Computer Security Threat Monitoring and Surveillance*.

An IDS can be configured to scan for attacks, track a hacker's movements, alert an administrator to ongoing attacks, and highlight possible vulnerabilities that need to be addressed. What type of activity an IDS will detect depends on where the intrusion sensors are placed. This placement requires some consideration because, after all, a sensor in the DMZ will work well at detecting misuse there but will be useless against attackers inside the network. After you have determined where to place sensors, they still require specific tuning. Without specific tuning, a sensor will generate alerts for all traffic that matches given criteria, regardless of whether the traffic is indeed something that should generate an alert. An IDS must be trained to look for suspicious activity. I typically tell people that an IDS is like a 3-year-old: Both require constant care and nurturing and don't do well if left alone.

Note

Although the CISSP exam will examine IDSs in a very basic way, modern systems are a mix of intrusion detection and intrusion prevention. These systems are referred to as intrusion detection and prevention (IDP) systems and are designed to identify potential incidents, log information, attempt to stop events, and report events. Many organizations even use IDP systems for activities like identifying problems with security policies, documenting threats, and deterring malicious activity that violates security policies. NIST 800-94 is a good resource for more information (see csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf).

A huge problem with intrusion detection systems is that they are after-the-fact devices: They notify you about attacks that have already taken place. In addition, IDSs are subject to false positives and false negatives. *False positives* occur when an IDS has triggered an alarm for normal traffic. For example, if you go to your local mall parking lot, you're likely to hear some car alarms going off due to reasons other than car theft. These car alarms are experiencing false positives. False positives are a big problem because they desensitize an administrator. *False negatives* are even worse. A false negative occurs when a real attack occurs, but the IDS does not pick it up.

ExamAlert

A false negative is a dangerous type of event because it means an attack occurred, but the IDS failed to detect it.

All these types of IDSs involve some basic components:

- **Sensors or agents**: These components detect and send data to the system. You should place sensors where you want to monitor traffic. On a HIDS, there can be many agents that report back to a server in a large environment.
- **Central monitoring system**: This system processes and analyzes data sent from sensors.
- **Report analysis**: This type of analysis provides information about how to counteract a specific event.
- **Database and storage components**: These components perform trend analysis and store IP addresses and other information about attackers.
- **Response box**: This component inputs information from the previously listed components and forms an appropriate response.

IDSs can be divided into two basic types: *network-based intrusion detection systems* (*NIDSs*) and *host-based intrusion detection systems* (*HIDSs*).

Network-Based Intrusion Detection Systems (NIDSs)

Much like a protocol analyzer operating in promiscuous mode, a NIDS captures and analyzes network traffic. Such a device diligently inspects each packet as it passes by. When it detects suspect traffic, the action taken depends on the particular NIDS. Alarms could be triggered, sessions could be reset, or traffic could be blocked. Among the advantages of NIDSs are that they are unobtrusive, they have the capability to monitor the entire network, and they provide an extra layer of defense between the firewall and the host. Disadvantages include the fact that attackers can send high volumes of traffic to attempt to overload them, they cannot decrypt or analyze encrypted traffic, and they can be vulnerable to attacks. In addition, attackers may send low levels of traffic to avoid tripping the IDS threshold alarms. Tools like NMAP have the ability to vary timing to avoid detection.

Keep in mind the following facts about NIDSs:

- They monitor network traffic in real time.
- They analyze protocols and other relevant packet information.
- They integrate with firewalls and define new rules as needed.
- When used in a switched environment, they require the user to perform port spanning and/or port mirroring.
- They send alerts or terminate offending connections.
- When encryption is used, they cannot analyze the traffic.

Host-Based Intrusion Detection Systems (HIDSs)

HIDSs are similar to virus scanners in function and design because they are application-based programs that reside on the host computer. Running quietly in the background, they monitor traffic and attempt to detect suspect activity, which can range from attempted system file modification to unsafe activation of ActiveX commands.

Although HIDSs are effective in a fully switched environment and can analyze network-encrypted traffic, they can require a lot of maintenance, they cannot monitor network traffic, and they rely on the underlying operating system because they do not control core services. HIDSs are best served on high-value targets that require protection.

Keep in mind the following facts about HIDSs:

- They consume some of the host's resources.
- They analyze encrypted traffic.
- They send alerts when unusual events are discovered.
- They are in some ways just like other applications running on the local host that are subject to attack.

Signature-Based, Anomaly-Based, and Rule-Based IDS Engines

IDS uses *signature-based*, *anomaly-based*, and *rule-based* analysis. These types take different approaches to detecting intrusions.

A signature-based engine relies on a database of known attacks and attack patterns. This system examines data to check for malicious content, which could include fragmented IP packets, streams of SYN packets (DoS), or malformed Internet Control Message Protocol (ICMP) packets. Any time data is found that matches one of these known signatures, an alarm, an alert, or a change to the firewall configuration can be made to initiate further action.

Although signature-based systems work well, they are only as effective as their most current update. IDSs are unaware of new or varied attacks and ignore the problematic traffic.

There are two subcategories of signature-based systems:

- **Pattern-based IDS**: This type of IDS looks at specific signatures and compares packets to them. The open-source IDS Snort started as a pattern-based IDS.
- **State-based IDS**: This is a more advanced design that has the capability to track the state of traffic and data as it moves between host and target.

An anomaly-based (or sometimes referred to as behavior-based) IDS observes traffic and develops a baseline of normal operations. Intrusions are detected by identifying activity outside the normal range of activities. For example, if Mike typically tries to log on only between the hours of 8 a.m. and 5 p.m., and now he's trying to log on 5,000 times at 2 a.m., the IDS can trigger an alert that something is wrong. The big disadvantage with an anomaly-based IDS is that an activity taught over time is not seen as an attack but merely as normal behavior. These systems also tend to experience a high number of false positives.

Anomaly-based systems fall into three subcategories:

- **Statistical-based IDS**: This type of IDS compares normal activity to abnormal activity.
- **Traffic-based IDS**: This type of IDS triggers on abnormal packets and data traffic.

- **Protocol-based IDS**: This type of IDS can reassemble packets and look at higher-layer activity. If the IDS knows the normal activity of the protocol, it can pick out abnormal activity. Protocol-decoding intrusion detection requires the IDS to maintain state information. For example, DNS is a two-step process; if a protocol-matching IDS sees a number of DNS responses that occur without a DNS request ever having taken place, the system can flag that activity as cache poisoning.

An anomaly-based IDS often compares the behavior of a protocol against what the RFC states. For example, it looks at how the flags in a TCP packet are set during the startup session, where the SYN flag should be set to 1. The military has been using anomaly-based IDSs for years to monitor their employees.

A rule-based IDS involves rules and pattern descriptors that observe traffic and develop a baseline of normal operations. Intrusions are detected by identifying activity outside the normal range. This type of expert system follows a four-phase analysis process:

1. Preprocessing
2. Analysis
3. Response
4. Refinement

> **ExamAlert**
>
> Carefully read any CISSP exam questions that discuss IDSs. Remember that several variables can change the outcome or potential answer. Take the time to watch for words such as *network*, *host*, *signature*, and *behavior* to better understand what the exam is asking for.

Sensor Placement

Your organization’s security policy should detail the placement of your IDS and its sensors. The placement of IDS sensors requires some consideration. IDS sensors can be placed externally, in the DMZ, or inside the network. Your decision to place a sensor in any one or more of these locations will require specific tuning. Without proper tuning, the sensor will generate alerts for all traffic that matches given criteria, regardless of whether the traffic is indeed something that should generate an alert. The placement of sensors is dynamic and must constantly change as your environment changes. A sensor should be stealth, and may even be deployed via a one-way networking cable so that it is harder for a hacker to scanner and find it.

ExamAlert

An anomaly-based IDS can detect zero-day attacks, but signature-based and rule-based IDSs cannot.

Intrusion Prevention Systems (IPSs)

IPSs take IDS technology a step further. IPSs can react automatically and actually prevent security occurrences from happening—without user intervention. IPSs are considered the next generation of IDSs and can block attacks in real time. NIST uses the term IDP (intrusion detection and prevention) to define modern devices that provide the functionality of both IDS and IPS devices. These devices typically perform deep inspection and can be applied to devices that support OSI Layer 3 to OSI Layer 7 inspection.

Two Great Tools Combined as One

SIEM is a combination of the two separate services security information management (SIM) and security event management (SEM). SIM is used to process and handle the long-term storage of audit and event data, whereas SEM is used for real-time reporting of events. Combining these two technologies provides users with the ability to alert, capture, aggregate, and review log information from many different systems and sources. Vendors that offer SIEM tools include Splunk, LogRhythm, and QRadar.

Although technologies like SIEM are a great addition to a security professional’s toolkit, keep in mind that you should strive for defense in depth. For example, combining an IDS/IPS with SIEM provides much greater protection than either technology by itself.

Network Access Control (NAC)

IDSs and IDP systems can be seen as just the beginning when it comes to access control and security. The next step in this area is *network access control* (*NAC*), or IEEE 802.1x. NAC, which has grown out of the trusted computing movement, has unified security as its goal. NAC offers administrators a way to verify that devices meet certain health standards before they can connect to the network. Laptops, desktop computers, and any other devices that don’t comply with predefined requirements can be prevented from joining a network or can even be relegated to a controlled network where access is restricted until the device is brought up to the required security standards.

Currently, there are several different incarnations of NAC available, including the following:

- **Infrastructure-based NAC**: Requires an organization to upgrade its hardware and/or operating systems.
- **Endpoint-based NAC**: Requires the installation of software agents on each network client. These devices are managed using a centralized management console.
- **Hardware-based NAC**: Requires the installation of a network appliance. The appliance monitors for specific behavior and can limit device connectivity when noncompliant activity is detected.

Keystroke Monitoring

Keystroke monitoring can be accomplished with hardware or software devices and is used to monitor activity. These devices can be used for both legal and illegal activity. As a compliance tool, keystroke monitoring allows management to monitor a user's activity and verify compliance. The primary issue of concern is the user's expectation of privacy. Policies and procedures should be in place to inform users that such technologies can be used to monitor compliance.

In 1993, the U.S. Department of Justice requested that NIST publish guidance on keystroke monitoring. This guidance can be found in NIST Bulletin 93-03 (see csrc.nist.gov/publications/nistbul/csl93-03.txt). The following is an example of an acceptable use policy:

> This acceptable use policy defines the boundaries of the acceptable use of this organization's systems and resources. Access to any company system or resources is a privilege that may be wholly or partially restricted without prior notice and without consent of the user. In cases of suspected violations or during the process of periodic review, employees can have activities monitored. Monitoring may involve a complete keystroke log of an entire session or sessions to verify compliance with company policies and usage agreements.

Unfortunately, key logging is not just for good guys. Hackers can use the same tools to monitor and record an individual's activities. Whereas an outsider to an organization might have some trouble getting one of these devices installed, an insider is in a prime position to plant a keystroke logger. Keystroke loggers come in two basic types:

- **Hardware keystroke loggers**: These loggers are usually installed while users are away from their desks and are completely undetectable, except for their physical presence. Just take a moment to consider when you last looked at the back of a desktop or server. Even if you see it, a hardware keystroke logger can be overlooked because it resembles a dongle. These devices are even available in wireless versions that can communicate via 802.11b/g/n/ac and Bluetooth.
- **Software keystroke loggers**: This type of logger sits between the operating system and the keyboard. Most of these software programs are simple, but some are more complex and can even email the logged keystrokes back to a preconfigured address. What they all have in common is that they operate in stealth mode and can grab all the text, mouse clicks, and even all the URLs that a user enters.

Exam Prep Questions

1. Grace works for a government agency that is very concerned about the confidentiality of information. This agency has strong controls for the process of identification, authentication, and authorization. Before Grace, the subject, can access her information, the security label on objects and clearance on subjects must be verified. What type of access control is this?

❍ **A.** DAC

❍ **B.** LBAC

❍ **C.** RBAC

❍ **D.** MAC

2. Which of the following biometric systems would be considered the most accurate?

❍ **A.** Retina scan, CER 3

❍ **B.** Fingerprint, CER 4

❍ **C.** Keyboard dynamics, CER 5

❍ **D.** Voice recognition, CER 6

3. What are the two primary components of DAC?

❍ **A.** Access rights and permissions and security labels

❍ **B.** File and data ownership and access rights and permissions

❍ **C.** Security labels and discretionary access lists

❍ **D.** File and data ownership and security labels

4. You have been hired as a contractor for a government agency. You have been cleared for secret access based on your need to know. Authentication, authorization, and accountability are enforced at the agency. At the end of each week, the government security officer for whom you work is tasked with reviewing security logs to ensure that only authorized users have logged in to the network and ensure that they have not attempted to access unauthorized data. The agency's process for ensuring accountability for access to an information system includes four phases. What is this an example of?

❍ **A.** Identification

❍ **B.** Accountability

❍ **C.** Authorization

❍ **D.** Authentication

5. When registering for a new service, you are asked the following questions: "What country were you born in? What's your pet's name? What is your mother's maiden name?" What type of password system is being used?

❍ **A.** Cognitive

❍ **B.** One-time

○ **C.** Virtual

○ **D.** Complex

6. Mark has just completed his new peer-to-peer network for the small insurance office he owns. Although he will allow Internet access, he does not want users to log in remotely. Which of the following models most closely matches his design?

○ **A.** TACACS+

○ **B.** MAC

○ **C.** RADIUS

○ **D.** DAC

7. Which of the following features does TACACS+ feature? (Choose the best answer.)

○ **A.** One-factor authentication

○ **B.** Decentralized access control

○ **C.** Two-factor authentication

○ **D.** Accountability

8. A newly hired junior security administrator will assume your position temporarily while you are on vacation. You're trying to explain the basics of access control and the functionality of rule-based access control mechanisms like ACLs. Which of the following best describes the order in which ACLs operate?

○ **A.** ACLs apply all deny statements before applying allow statements.

○ **B.** Rule-based access control and role-based access control are basically the same thing.

○ **C.** An ACL ends with an implicit deny all statement.

○ **D.** ACLs are processed from the bottom up.

9. RADIUS provides which of the following?

○ **A.** Authorization and accountability

○ **B.** Authentication

○ **C.** Authentication, authorization, and accountability

○ **D.** Authentication and authorization

10. Which of the following is the best description of a situation in which a user can sign up for a social media account, for example, at Facebook and then use those credentials to log in and access another organization's sites, such as Yahoo?

○ **A.** Transitive trust

○ **B.** Federated ID

○ **C.** Nontransitive trust

○ **D.** Single sign-on

11. What type of attack targets pronounceable passwords?

❍ **A.** Brute-force attacks
❍ **B.** Dictionary attacks
❍ **C.** Hybrid attacks
❍ **D.** Rainbow tables

12. Which of the following is the best method of password storage?

❍ **A.** A plaintext file
❍ **B.** Symmetric encryption
❍ **C.** A one-way encryption process
❍ **D.** An XOR process

13. Which access control method makes use of a join and a meet?

❍ **A.** Rule-based access control
❍ **B.** Mandatory access control
❍ **C.** Discretionary access control
❍ **D.** LBAC

14. Which of the following access control methods is commonly used with firewall and edge devices?

❍ **A.** Rule-based access control
❍ **B.** Mandatory access control
❍ **C.** Discretionary access control
❍ **D.** LBAC

15. Due to recent highly publicized hacking news reports, senior management has become more concerned about security. As the senior security administrator, you are asked to suggest changes that should be implemented. Which of the following access methods should you recommend if the method should be primarily based on preestablished access, can't be changed by users, and needs to work well in situations where there is high turnover?

❍ **A.** Discretionary access control
❍ **B.** Mandatory access control
❍ **C.** Rule-based access control
❍ **D.** Role-based access control

16. In which of the following are the rights to access a resource based on policies that combine attributes?

❍ **A.** Constrained user interface

❍ **B.** Mandatory access control

❍ **C.** Discretionary access control

❍ **D.** Attribute-based access control

17. Which of the following does IAL 3 provide?

❍ **A.** Multifactor authentication

❍ **B.** Remote identity proofing

❍ **C.** In-person identity proofing

❍ **D.** Identity-as-a-service

18. Which of the following is not one of the OAuth roles?

❍ **A.** Resource owner

❍ **B.** Resource server

❍ **C.** Supplicant

❍ **D.** Authentication server

19. Which of the following describes an access control policy language, request/response language, and reference architecture?

❍ **A.** SAML

❍ **B.** OAuth

❍ **C.** XACML

❍ **D.** OpenID

20. Which of the following is not one of the roles of SAML?

❍ **A.** Identity provider

❍ **B.** Resource owner

❍ **C.** Service provider

❍ **D.** Subject

Answers to Exam Prep Questions

1. **D.** MAC is correct because it uses security labels and clearances. A is not correct because DAC uses ACLs; B is not correct because LBAC is lattice-based access control, which uses upper and lower limits; C is incorrect because RBAC uses roles or tasks in an organization based on the organization's security policy.
2. **A.** The lower the CER, the better, so retina scan, CER 3 (answer A) is correct. Fingerprint, CER 4 (answer B), keyboard dynamics, CER 5 (answer C), and voice recognition, CER 6 (answer D) are incorrect because they have higher CERs. The CER is determined based on Type I and Type II errors.
3. **B.** The two primary components of DAC are file and data ownership and access rights and permissions. With file and data ownership, every object in a system must have an owner. Objects without owners will be left unprotected. Access rights and permissions control the access rights of an individual. Variation exists, but a basic access control list checks read, write, and execute privileges. Answers A, C, and D are incorrect.
4. **B.** The four key areas of identity and access management are identification, authentication, authorization, and accountability. The fact that the security officer is reviewing the logs for accuracy is a form of accountability. Therefore, answers A, C, and D are incorrect.
5. **A.** Cognitive passwords are widely used during enrollment processes, when individuals call help desks, and when individuals request other services that require authentication. All other answers are incorrect: One-time passwords (answer B) are associated with tokens, virtual passwords (answer C) are a form of passphrase, and the question does not describe a complex password (answer D).
6. **D.** The discretionary access control (DAC) method is so named because access control is left to the owner's discretion. This can be thought of as being similar to a peer-to-peer computer network. All other answers are incorrect: A MAC model (answer B) is static and based on a predetermined list of access privileges, and both TACACS+ (answer A) and RADIUS (answer C) are used for remote access and do not properly address the question.
7. **C.** TACACS+ features two-factor authentication. All other answers are incorrect: TACACS+ offers more than one-factor authentication (answer A); it is a centralized, not decentralized, access control system (answer B); and although it offers accountability (answer D), it also offers authorization.
8. **C.** An ACL has an implicit deny all statement. For example, if an ACL had only the one statement "Deny ICMP any, any," ICMP would be denied; however, the implicit deny all would block all other traffic. Answers A and D are incorrect because ACLs are processed from top to bottom. Answer B is incorrect because rule-based access control and role-based access control are not the same thing.
9. **C.** RADIUS provides three services: authentication, authorization, and accountability. RADIUS facilitates centralized user administration and keeps all user profiles in one location that all remote services share. Answers A, B, and D are incorrect because they do not fully answer the question.
10. **B.** Federation is an arrangement that can be made among multiple enterprises (such as Facebook and Yahoo) that lets subscribers of one service use the same identification/authentication credentials to gain access to the second

organization's resources. It differs from single sign-on (SSO) in that SSO is used within a single organization. Examples of SSO include Kerberos and SESAME. Answers A and C are incorrect because a transitive trust is a two-way relationship automatically created between parent and child domains, and a nontransitive trust is a trust that will not extend past the domains with which it was created. Both of these terms are directly associated with Microsoft operating systems.

11. **B.** Dictionary attacks target pronounceable passwords. Brute-force attacks (answer A), hybrid attacks (answer C), and rainbow tables (answer D) are all used to target any password that includes a combination of A–Z, a–z, 0–9, and special characters.
12. **C.** The best way to store passwords is by means of a one-way process known as hashing that is used by operating systems like Microsoft Windows and Linux. A plaintext file (answer A) can be easily exposed. Symmetric encryption (answer B) would allow the process to be easily reversed by anyone with a key. An XOR process (answer D) would only obscure the password and would not provide any real protection.
13. **D.** Lattice-based access control model (LBAC) makes use of a join and a meet. LBAC is considered a complex method and is used to manage interactions between subjects and objects. Answers A, B, and C are incorrect as these methods do not use joins and meets.
14. **A.** Rule-based access control is used with firewalls and routers. RBAC is based on a specific set of rules, much like a router ACL. MAC (answer B) makes use of labels and is well suited for high-security environments. DAC (answer C) describes discretionary control, and LBAC (answer D) is a complex method that makes use of upper and lower bounds.
15. **D.** Role-based access control (RBAC) allows specific people to be assigned to specific roles with specific privileges. It allows access to be assigned to groups and works well where there are high levels of turnover. Answers A, B, and C do not meet that description.
16. **D.** With ABAC, the rights to access a resource are based on policies that combine attributes. All other answers are incorrect: A constrained user interface (answer A) limits what the user can see or do based on the user's privileges. MAC (answer B) is static and based on a predetermined list of access privileges. DAC (answer C) is a decentralized model.
17. **C.** IAL 3 provides for in-person identity proofing. All other answers are incorrect because IAL 3 does not provide multifactor authentication (answer A), remote identity proofing (answer B), or identity-as-a-service (answer D).
18. **C.** Supplicant is not an OAuth role. Answers A, B, and D are incorrect because the resource owner, resource server, and authentication server are all valid roles.
19. **C.** XACML is primarily an ABAC access control policy language, where attributes (bits of data) associated with a user or an action or a resource are inputs into the decision about whether a given user may access a given resource in a particular way. Answers A, B, and D are incorrect because they do not fully answer the question.
20. **B.** Resource owner is not one of the roles of SAML. The roles in SAML include the identity provider (answer A), the service provider (answer C), and the subject (answer D).

Suggesting Reading and Resources

Zephyr analysis: www.cse.unr.edu/~bebis/CS790Q/Lect/Chapter_8.ppt

Integrating physical and logical security: www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/pl-security.pdf

Understanding access control: www.owasp.org/index.php/Access_Control_Cheat_Sheet

Performance metrics for biometrics: www.biometric-solutions.com/index.php?story=performance_biometrics

Understanding session management: www.hackingarticles.in/beginner-guide-understand-cookies-session-management/

Credential management systems: https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html

Comparison of biometric methods: https://www.recogtech.com/en/knowledge-base/5-common-biometric-techniques-compared

Federated identity management (SAML versus OAuth): fedtechmagazine.com/article/2020/01/federated-identity-management-saml-vs-oauth-perfcon

System account access review: www.isaca.org/resources/isaca-journal/issues/2019/volume-4/effective-user-access-reviews

Provisioning and deprovisioning: www.identitymanagementinstitute.org/6-best-practices-for-managing-the-identity-lifecycle/

Attribute-based access control: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf

RADIUS best practices: msdn.microsoft.com/en-us/library/bb742489.aspx

CHAPTER 7

Security Assessment and Testing

Terms you'll need to understand:

- Audit
- Vulnerability assessment
- Penetration testing
- Trojan
- Malware
- Rootkit
- Logic bomb
- Interface testing
- Synthetic transaction
- Password cracking
- Social engineering
- Virus

Topics you'll need to master:

- Security assessment and testing
- Assessment and test strategies
- How to identify attack methodologies
- Automated and manual testing techniques
- Examples of penetration test methodology
- Log reviews
- Disaster recovery and business continuity
- How to perform security assessments and penetration tests
- Security metrics
- Incident response techniques

Introduction

When preparing for the (ISC)^2 CISSP exam or reviewing the Security Assessment and Testing domain, you need to know which resources should be protected, types of tests that can be used for security control testing, and the threats you might encounter in a network.

This chapter examines audits, vulnerability assessments, and penetration tests, each of which plays a role in securing an organization. Organizations carry out penetration tests to see what a criminal hacker can access, how such access can be used, and what risk or impacts that access might have. Security violations aren't always malicious, though; sometimes things break and accidents happen. Security testing is often conducted to deal with such incidents.

This chapter also discusses how the threat landscape has changed. The risks are many; in addition to viruses and worms, ransomware, supply chain attacks, and bitcoin mining have become more widespread. Attackers use a variety of different tools and techniques to hack, target, and monetize their activities. It is important to keep in mind that incidents can lead to outages, which requires disaster recovery planning and the implementation of a business continuity plan. An organization needs to have in place an incident response plan that has been tested and approved. This chapter covers these risks, along with investigations and legal proceedings.

Security Assessments and Penetration Test Strategies

The world of information security continually evolves. Today there are more tools available to attackers and defenders than ever before. It is therefore imperative that organizations periodically review their security. This section covers several techniques for remediation and review that can be used to meet this challenge, including policy reviews (audits), vulnerability scanning, and penetration testing. All these techniques are useful in identifying and resolving security architecture vulnerabilities.

Audits

Organizations use policy reviews—also called audits—to review the presence and strength of operation (management), technical, and physical controls and report on the capability of these controls to protect the organization.

Most organizations want to do the right thing and are interested in proper controls, but many of them are overwhelmed by the day-to-day demands of business. It is important for auditors to verify both security and compliance and demonstrate due diligence.

An audit is a planned, independent, and documented assessment to determine whether agreed-upon requirements and standards of operations are being met. Basically, it is a review of the operation and activities of an organization. An auditor uses the organization's policies, standards, and procedures to guide the audit and can also use appropriate laws, regulations, and industry standards and best practices. Some common types of audits include the following:

- **Internal audit**: Internal audits can be quick because the team knows the environment, and they enable the organization to be more agile. However, internal audits can be problematic because there could be conflicts of interest, the team might not have a lot of depth of experience, and management might seek to steer the outcome toward a specific goal.
- **External audit**: Today, most organizations focus on core competencies and outsource many activities. While you might not perform an audit on a partner, it is common to ask for proof of audit or bring in a third-party auditor to review specific parts of the organization's processes that might impact your organization. The main advantage of an external or third-party audit is that the auditors have no vested interest in the outcome of the audit. As noted earlier, such objectivity might be lacking in an internal audit. The biggest disadvantage of this type of audit is cost.

Sometimes an organization has little choice about what type of audit to perform. Regulatory requirements such as the Sarbanes-Oxley Act require that compliance audits be conducted by third parties.

Note

One of the most widely used frameworks for auditing is the Control Objectives for Information and Related Technology (COBIT), which is a system of best practices.

Regardless of the type of audit you perform, you must determine what testing technique to use: automated or manual. Automated tests are executed via test automation frameworks without human assistance. With manual testing, an individual or a team performs the tests step by step, without test scripts.

Another important consideration is *test coverage*, or how much of a system's output, coverage, or activity you are going to test. For example, an audit of a financial system that contains tens of thousands of records might examine only a subset of the records. The *sampling plan* allows an auditor to review a segment of the population by observing only a part of that group and to reach conclusions with a predictable level of certainty. In most cases, units from the group are picked at random. When using random sampling, all units/parts have the same likelihood of being selected for inspection. For example, your organization might have more than 200 security controls. Testing all of them would be difficult and time-consuming, so the sampling plan might indicate to sample only a portion of the controls such as 20% of areas picked at random.

Audits as Detective Controls

There may be times when you want to know more about organizations before doing business with them. For example, maybe you are a growing startup and need to select a cloud service provider. In such a situation, you might want to review the provider's SOC for Service Organizations report. These reports from independent CPAs are designed to help service organizations build trust and confidence in the services they perform and controls related to their services. Each type of SOC for Service Organizations report is designed to help service organizations meet specific user needs:

- **SOC 1**: These reports evaluate the effect of the controls at the service organization on the users' financial statements.
- **SOC 2**: These reports provide detailed information about how a service organization handles users' data and the confidentiality and privacy of the information processed by these systems.
- **SOC 3**: These reports, which are similar to SOC 2 reports, are general use reports that can be freely distributed.

During an audit, you might be asked to provide security metrics to demonstrate the effectiveness and state of security controls. It's common for such metrics to track key performance indicators (KPIs) and key risk indicators (KRIs).

KPIs provide insight into the success of a security program by looking at historical performance. Information Technology Infrastructure Library (ITIL) is a framework of best practices for delivering IT services that lists nine KPIs:

- Percentage decrease in security beaches reported
- Percentage decrease in the impact of breaches reported
- Percentage increase in service-level agreements (SLAs) that have appropriate security clauses
- Number of preventive security measures the organization has implemented in response to security threats

- Time lapse between identifying a threat and implementing appropriate controls
- The number of major security incidents
- The number of incidents that have created service outages
- The number of security test/training/awareness events
- The number of shortcomings identified during a security test

KRIs quantify security risk looking forward. ISACA (formerly Information Systems Audit and Control Association) recommends selecting KRIs based on four criteria:

- **Impact**: The impact is the likelihood that the indicator will identify potential risk.
- **Effort**: The effort is the work required for implementation, measurement, and support.
- **Reliability**: An indicator is reliable if it is a good predictor of risk.
- **Sensitivity**: Sensitivity refers to the ability to accurately capture variance in the risk.

Root Cause Analyses

Although audits can help verify that controls have been developed and are being implemented, an audit is just one part of ensuring operational security. Any time problems are found, an organization needs to follow its procedures to perform root cause analysis to discover the cause of the problem. Root cause analysis is a structured approach to identifying problems, assessing their magnitude, and determining what actions need to be taken to prevent the recurrence of similar situations.

Log Reviews

Closely related to audits are log reviews. A log review is a systemic examination of system logs in order to detect security events. Log files are a great source of information only if someone reviews them. The reality is that in many organizations, no one examines these logs until something goes wrong. When planning for log reviews, you must consider what logs you are going to store, how long you are going to store them, whether you will centralize this process, and how you will protect the integrity of the logs.

Security professionals should periodically monitor system logs to make sure no problems are occurring. The following are some of the logs that should be reviewed:

- **System logs**: These logs should be exported to a central location, and someone should be assigned to periodically review them. A system log should be backed up and have a hash/timestamp applied to verify that no tampering has occurred.
- **Event logs**: These logs are designed to record system occurrences related to memory, process, system performance, uptime, or hardware issues. While the event log is not focused on security concerns, it should be reviewed because it can provide useful information.
- **Audit logs**: These logs monitor and record user activity. Audit logs are a detective control and can be used to track compliance with security policy.
- **Security logs**: These logs track events that correlate directly or indirectly with security. Security logs record information such as user access, user-privileged operations, firewall issues, and intrusion detection system/intrusion prevention system (IDS/IPS) alerts.
- **Access logs**: These logs record information pertaining to access activity. Access logs should be copied to centralized servers and protected from unauthorized access and modification.
- **Application**: These logs are event logs that record software incidents.

Log files often require a great deal of storage as they are generated automatically during software and computer operations. Log files can be generated by web servers, computing devices, and applications. It is important to define log management policies for various sources and types of log files.

Note

One critical factor to consider with logs is time synchronization. If the time is off on just a few systems, log management review can be difficult or even impossible. One of the most common means to manage this issue is by using Network Time Protocol (NTP), which is the industry standard for synchronizing computer clocks between network devices.

An important standard for log management is National Institute of Standards and Technology (NIST) SP 800-92. This document provides a high-level overview and guidance for the planning, development, and implementation of an effective security log management strategy. NIST SP 800-92 defines a log management infrastructure as having four major functions:

- **General**: Log parsing, event filtering, and event aggregation
- **Log storage**: Rotation, archival, compression, reduction, normalization, and integrity checking
- **Log analysis**: Event correlation, viewing, and reporting
- **Disposal**: Data clearing

NIST SP 800-92 addresses the following security log management challenges:

- Log volume exceeding the rate of analysis
- Immutability during storage and transmission
- Inconsistent vendor log formats
- The importance of a consistent review schedule
- Retention issues involving purging, long-term storage, and cost

NIST SP 800-92 makes the following recommendations for security log management:

- Establish policies and procedures for log management.
- Prioritize log management appropriately throughout the organization.
- Create and maintain a log management infrastructure.
- Provide proper support for all staff with log management responsibilities.
- Establish standard log management operational processes.

Log management and reviews should be key components of compliance initiatives. Only with centralized logs in place can you monitor, audit, and report on file access, unauthorized activity by users, policy changes, and other critical activities performed in your organization. Many organizations have moved toward information security continuous monitoring (ISCM). This approach features ongoing awareness of information security in an organization, including, threats, vulnerabilities, and risk management. NIST 800-137 breaks ISCM into four phases:

1. Implement an ISCM program.
2. Analyze data and report findings.

3. Respond to findings.
4. Review and update the ISCM strategy and program.

Note

NIST 800-37 covers the Risk Management Framework (RMF) for information systems. The goal of the RMF is to transform the traditional certification and accreditation process into a structured six-step process.

Network Scanning

Network scanning is a procedure for identifying active devices on a network by using ICMP pings or port scanning. A basic *network discovery scan* can be performed with a ping sweep across the network range. The idea is to ping each device and see if a reply is returned. The following is an example of a ping:

```
C:\Users\admin>ping 192.168.1.253
Pinging 192.168.1.253 with 32 bytes of data:
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.1.253:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Although a ping sweep of a network can be fast, it provides little detail. It simply lets you know whether the system responds. A more in-depth scan would involve performing a port scan of some or all of the TCP and UDP ports, using a tool such as Nmap. Regardless of the technique used, a network discovery scan does not probe systems for vulnerabilities but provides a report showing the systems detected on a network and a list of the ports exposed.

Scans can also be focused on web applications. Automated tools can scan web applications from the outside and search for security vulnerabilities such as cross-site scripting (XSS), Structured Query Language (SQL) injection, poor input validation/sanitization, path traversal, and command injection. The Open Web Application Security Project (OWASP) is an entity that focuses on these activities. Web application scanning should be performed at several crucial points:

- During development
- When new applications are moved into production

- Before code changes go to production
- On a recurring periodic basis

There are many software tools available for web application scanning, including Nessus, Acunetix, Nikto, Wapiti, and Burp Suite.

Vulnerability Scans and Assessments

Vulnerability scans are used to review all potential points on a computer or network that could be used to exploit the system, and *vulnerability assessments* are used to identify all potential vulnerabilities that could be exploited in an environment. Vulnerability assessment tools are software packages used to scan for known vulnerabilities.

Much has changed in the way the IT industry views vulnerability assessments since the first software program was created for this purpose in the early 1990s. At that time, two well-known security professionals, Dan Farmer and Wietse Venema, wrote a landmark paper titled “Improving the Security of Your Site by Breaking Into It.” They went on to develop SATAN (System Administrator Tool for Analyzing Networks), the first vulnerability assessment program used to scan for problems. Sun Microsystems actually fired Dan Farmer for releasing the program. At the time, the tool was seen as something that could be dual-use—for good and bad—and some people were also uncomfortable with the name.

Today, organizations around the world use vulnerability assessment tools to scan their networks for software problems, misconfigurations, and security vulnerabilities. A vulnerability scanner can be run against a single address or a range of addresses and can also test the effectiveness of layered security measures.

Many vulnerability assessment tools are now available. Vulnerability assessment software can be used to scan systems, compiled software, or even source code. Nessus is a good example of a system-level vulnerability scanner. Even though vulnerability assessment software tools are important controls that increase security, they cannot test for every conceivable vulnerability and might cause systems to crash. A vulnerability assessment tool is just one of many items that help provide for defense in depth. Recall that defense in depth means using multiple layers—such as vulnerability assessment software, audits, penetration testing, and antivirus—to ensure security.

Vulnerability assessment software is not a substitute for more thorough tests and examinations, but penetration testing can help fill the gap.

Penetration Testing

Penetration testing is the process of evaluating an organization's security controls. Penetration tests can be performed in a number of ways, including the following:

- **Whitebox testing**: With this type of testing, the test team knows everything about the network. The team of testers has been provided network maps, diagrams, and documents specifying all the details of the organization's network.
- **Blackbox testing**: With this type of testing, the test team has no details of the organization's network. For example, last year my company did a blackbox test for an organization and was provided only the IP address range. The client wanted us to ascertain all other details during the penetration test.
- **Graybox testing**: This type of test examines what is possible with insider access.

Penetration testing can be performed using a manual process or via automated software packages, such as Core Impact and Metasploit. Penetration tests can take a number of forms:

- **Outsider testing**: This type of testing examines what threat actors or other outsiders can access or do.
- **Physical security testing**: This form of penetration testing involves using physical access to see what can be accomplished. Some would argue that if physical barriers can be bypassed, there is no security at all.
- **Wireless network testing**: This form of testing is done to verify the organization's wireless access policies and to ensure that no misconfigured devices have been introduced that may cause additional security exposures. Such testing might include Bluetooth and RFID testing of devices on premises.
- **Application security testing**: Many organizations offer access to core business functionality through web-based applications. Static testing, dynamic testing, and fuzz testing are different approaches to verifying that the controls over an application and its process flow are adequately designed.
- **Denial of service (DoS), or stress, testing**: The goal of this type of testing is to evaluate the network's susceptibility to DoS attacks and heavy loads.
- **War dialing**: War dialing is an attempt to systematically call a range of telephone numbers and identify modems, remote access devices, and maintenance connections of computers that could exist on an

organization's network. While this method is considered dated today it continues to be used. One example is to target Zoom and other online meeting tools. See https://krebsonsecurity.com/2020/04/war-dialing-tool-exposes-zooms-password-problems/.

- **Social engineering testing**: This form of penetration testing involves using social interaction techniques with an organization's employees, suppliers, and contractors to gather information and penetrate the organization's systems.

> **Caution**
>
> Penetration testing can be performed with the full knowledge of the security staff, as a blind test, or as a double-blind test. A blind test is one in which only publicly available information is used. A double-blind test is one in which only publicly available information is used and security staff are not notified of the event. A double-blind test allows the organization to observe the reactions of the security staff.

In addition to determining the mode of a test, you need to consider the network infrastructure. Figure 7.1 illustrates a layered security infrastructure.

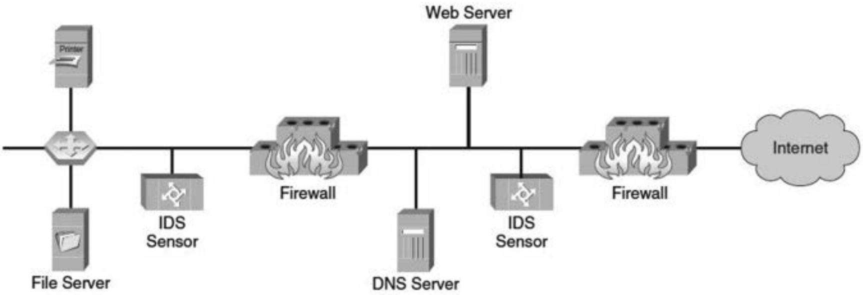


FIGURE 7.1 **Network Infrastructure**

Security tests of any type are a large undertaking. An organization needs a team to carry out these duties. This team is responsible for determining the weaknesses, technical flaws, and vulnerabilities of the organization. This team is known as a penetration test team or, informally, a red team, and the individuals on it are known as ethical hackers or white hat hackers. (Black hat hackers are threat actors, and gray hat hackers are in between, sometimes doing both helpful and harmful activities.) Ethical hackers perform the same activities as threat actors, but they do so with the approval of the organization and without causing damage.

The goal of penetration testing is to test the network in much the same way a threat actor would. Because of the global nature of the Internet and the increased emphasis on networking, these types of activities have gained increased prominence in the past several years.

Regardless of what it knows about the network, the penetration test team typically starts with basic user access. Its goal is to advance to root access or administrator access and to try to control the network. The most critical factor distinguishing threat actors from ethical hackers is obtaining corporate approval. Without the signed consent of the organization's owner or upper management, a penetration test team could very well be breaking the law.

Penetration testing typically involves the following phases:

1. **Discovery or reconnaissance**: The team identifies and documents information about the targeted organization.
2. **Enumeration**: The team uses intrusive methods and techniques to gain more information about the targeted organization (for example, using software tools to scan for live machines).
3. **Mapping the attack surface**: The team conducts vulnerability mapping to discover the correlation between the findings from enumeration and known and potential vulnerabilities that could be used to gain access.
4. **Exploitation**: The team attempts to gain user and privileged access by launching attacks against known vulnerabilities, performing lateral movement, and pivoting from one compromised host to another.
5. **Reporting to management**: The team prepares a report of the findings of the penetration test and details the issues that need to be addressed, along with their priority.

Penetration testing methodologies can be broken into two broad categories:

- **Proprietary Vendors**: Examples of organizations that provide proprietary penetration testing methodologies are IBM, ISS, McAfee/Foundstone, and the EC-Council.
- **Open-source Frameworks**: Open-source penetration testing methodologies are available from OSSTMM, ISSAF, OWASP, and NIST.

Each of these methodologies offers guidance on performing tests and identifying key areas of concern.

Note

To address advanced persistent threats and block lateral movement, many organizations have moved to microsegmentation and zero trust infrastructure.

NIST provides documents that are helpful for organizations planning penetration testing. For example, NIST 800-115, which includes recommendations for tools intended for self-evaluation, addresses the following areas:

- Risk analysis
- Certification
- Accreditation
- Policy development

NIST divides penetration testing into four primary stages:

1. **Planning**: As the saying goes, success is 90% preparation and 10% perspiration. Good planning is the key to success. You need to know where you are going, what your goals are, what the time frame is, and what the limits and boundaries are.
2. **Discovery**: This stage consists of two distinct phases:
   - **Passive**: During this phase, information is gathered in a very covert manner. Examples of passive information gathering include surfing the organization's website to mine valuable information and review job openings to gain a better understanding of the technologies and equipment used by the organization. This stage is deemed passive because the penetration test team is not port scanning or launching attack tools; it is only gathering information from available data sources.
   - **Active**: This phase of the test is split between network scanning and host scanning. As individual networks are enumerated, they are further probed to discover all hosts, determine their open ports, and attempt to pinpoint their OS. Nmap and Zenmap (which is a GUI-based Nmap tool) are popular scanning programs.
3. **Attack**: During this stage, the ethical hacker attempts to gain access, escalate privilege, browse the system, and expand influence.
4. **Reporting**: Although this stage is listed last, reporting and documentation should be conducted throughout each stage of the process. Documentation created throughout a test should be used to compile the final report, and the report should serve as the basis for corrective action. Corrective action can range from nothing more than enforcing existing policies to closing unneeded ports and adding patches and service packs.

At the completion of a penetration test, the results are delivered in a comprehensive report to management. Security of the report is an important issue, and distribution and storage are also crucial.

NIST 800-115 recommends making network security a routine feature of every network and using caution when testing. Things can go wrong! Employees should be trained in security testing so that when negative events occur, the organization has people already trained.

Although these are good guidelines, it's also important to understand the limitations of security testing activities. Penetration testing cannot cure every conceivable problem. You need to build on vulnerability management by patching and updating systems regularly, implementing and following good policies, and training employees.

Table 7.1 provides some sample intervals for common security review functions.

TABLE 7.1 **Security Review Intervals**

Technique	Daily	Weekly	Monthly	Biannually	Annually
Antivirus	✓	–	–	–	–
Log reviews	✓	✓	✓	–	–
Audits	–	–	–	✓	–
Vulnerability assessments	–	✓	–	–	–
Penetration testing	–	–	–	–	✓

Test Techniques and Methods

A variety of test techniques and methods can be used to test software, systems, and networks. Regardless of the methodology chosen, it is important to build security into a product. This concept of "baking in security" is the foundation of the secure software development lifecycle (SSDLC). Every phase of the SSDLC stresses the importance of incorporating security into the process:

- Requirements gathering
  - Security requirements
  - Assessment of risk
- Design
  - Design requirements identification from a security perspective
  - Design and architecture review
  - Threat modeling

- Coding
    - Coding best practices
    - Static analysis review
- Testing
    - Vulnerability assessment
    - Fuzzing
- Deployment
    - Server, network, and platform configuration review

For example, code review and testing might focus on which programming language was used and which functions were implemented. The C language, for instance, has some functions that can be exploited (because they do not check for proper buffer size), including `strcat()`, `strcpy()`, `sprintf()`, `vsprintf()`, `bcopy()`, `scanf()`, and `gets()`.

Applications continue to be one of the most targeted portions of an organization's IT infrastructure. Several approaches to deal with non-secure code include static testing of code, dynamic testing, and runtime protections. Static application security testing (SAST) might be performed to verify that security best practices have been built in. SAST is a manual review that is carried out without running the application; it involves analyzing the source code or the compiled application.

Interactive application security testing (IAST) is a post-build analysis tool that scans an application's source code. While the application is running, testing is ongoing. IAST is typically performed in a QA or test/dev environment and requires an agent be installed. The goal is to identify any problematic code, note it, and request the developer remediate.

Both SAST and IAST look directly at code; IAST does so only in a post-build environment. IAST is highly scalable and can be performed by a human tester or automated.

Dynamic application security testing (DAST), in contrast, is conducted in a runtime environment where testers typically do not have access to underlying source code and is considered a blackbox testing technique.

Runtime application self-protection (RASP) is capable of controlling the application during runtime and execution. RASP can detect and prevent attacks on applications in real time. RASP analyzes the context of suspected malicious behavior and monitors its own behavior to automatically detect and mitigate attacks. RASP is useful protection against a range of threats including cross-site scripting (XSS), SQL injection, and data exfiltration. However, it can impact application performance. DAST works from the outside in.

Conducting *synthetic transactions*, referred to as synthetic monitoring, involves building scripts or tools that simulate processes typically performed by an application. These are real-time transactions that are performed on monitored objects. Synthetic transactions can be used to measure the performance of a monitored object and to see how it reacts when it is stressed. For example, you might configure a synthetic transaction on a web server that simulates a user browsing website pages and performing common activities. Synthetic transactions can be used to see whether monitoring settings, such as alerts and notifications, perform as expected.

Fuzz testing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. It can be used in two different ways: With generation fuzzing, the software generates input values randomly from the specification, and with mutation fuzzing, you analyze real input and modify those real values. Regardless of the approach used, the program is monitored for exceptions such as potential memory leaks, application crashes, or failing built-in code assertions.

Fuzz testing is closely associated with *misuse case testing*. Think of this as a negative scenario: testing for things that should not happen. For example, if you enter a negative quantity in a field that requires a positive value, will the web application actually accept it? It shouldn't!

During a source code review, a Fagan inspection might be performed. A *Fagan inspection* is a process that defines a particular activity with prespecified entry and exit criteria. It is typically used with software to search for defects during various phases of the software development process to prevent issues and outages before the software is placed in production. The steps in this process include planning, overview, preparation, meeting, rework, and follow-up. During the rework phase, the code review may transition to the inspection, follow-up, or planning phases. During the overview phase, the code review may transition to the planning or preparation phases. During the inspection phase, the code review may transition to the rework or preparation phases. Transitioning from the rework phase to the preparation phase is not acceptable during a code review.

Another type of testing examines *integer overflow*, which occurs when a program or an application attempts to store a number in a variable that is larger than that variable's type can handle. Consider a situation where an allocated buffer can hold a value up to 65,535. If someone can exceed this value and tries to store a value in an unsigned integer type that is larger than the maximum value, only the modulus might remain; for example, 65,535 + 1 might become 0. Figure 7.2 shows an example.

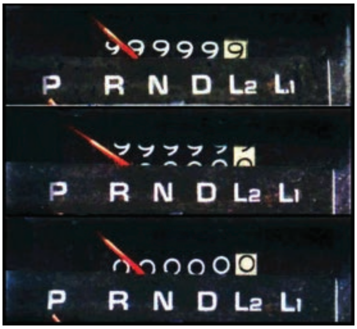


FIGURE 7.2 **Integer Overflow**

Source: https://en.wikipedia.org/wiki/Integer_overflow#/media/File:Odometer_rollover.jpg

Testing should focus on more than just input and output data. It should also look at how an application passes data from system to system, subsystem to subsystem, or variable to variable. This is where interface testing comes in. This type of testing is used to verify whether all the interactions between various modules and components are working properly and whether errors are handled properly.

Note

Attackers are always trying to tamper with data. One way they do so is with data diddling attacks. This type of attack works by changing data as it is keyed in or processed by a computer. It can be done to cancel debts without proper authority or assign a large hourly pay increase to an individual. Trying to track down the problem is difficult, and it could be months before such an attack is uncovered. However, regular testing can help bring such attacks to light.

Security Threats and Vulnerabilities

Now that we have examined some of the types of tests that an organization can perform, let's turn our attention to some of the threats and vulnerabilities an organization might face. Knowing what threats and vulnerabilities exist allows an organization to build controls to address these specific issues. It is much cheaper to be proactive and build in good controls than it is to be reactive and figure out how to respond after an attack has occurred.

Threat Actors

The people who threaten the security of your network can be divided into two main groups:

- **Insiders (often disgruntled employees)**: These are individuals who either currently work for the organization or have been fired or quit yet still have access. Insiders could be disgruntled employees or current or former contractors.
- **Outsiders**: These individuals have never worked for you—and you are probably lucky they haven't. Outsiders can be segregated into several subgroups:
  - **Script kiddies**: These individuals cause harm with scripts, tools, and rootkits written by other, more skilled, individuals. Often, they don't understand how the exploits they are using work.
  - **Hacktivists**: These hackers have an agenda in that their attacks are driven by the need to protest or make a statement. Hactivist groups, such as LulzSec and Anonymous, might use distributed denial of service (DDoS) tools or search for and publish private or identifying information about a target; this is known as *doxing*. Hacktivist is a combination of the words *hack* and *activist*. Hacktivists like to refer to themselves as protesters in cyberspace.
  - **Corporate spies**: These individuals work for rival firms. Their goal is to steal your proprietary information or open-source intelligence for competitive advantage.
  - **Skilled hackers**: Although they're not driven by corporate greed or the desire to advance agendas (as are hacktivists), these individuals do have motives. Maybe they are looking for ways to proclaim their advanced hacking skills, or they might be at odds with a stand or position your organization has taken.
  - **Hacker researchers**: These individuals may accidentally (or intentionally) discover vulnerabilities in a product or infrastructure and then attempt to communicate the issue to the responsible parties.
  - **Organized crime**: The primary motivation of organized crime is to make money. Organized crime activities might include creating and renting botnets, monetizing personally identifiable information (PII), and generating revenue from exploit kits aka crimeware kits and ransomware.

- **Foreign government agents**: These individuals seek ways to advance the interests of their country, and your data might be the target. These agents may spend months or years crafting highly customized attacks to achieve their objectives.

Note

Being a hacker researcher is not without risk. A hacker known as Weev was part of a group that exposed a flaw in AT&T security, which allowed the email addresses of 114,000 iPad users, including those of celebrities, to be revealed. Weev was charged and found guilty of identity fraud and conspiracy to access a computer without authorization. While the original conviction was later overturned, Weev did serve more than a year of his original sentence.

So, which group represents the biggest threat? The distinction between insiders and outsiders isn't always useful. Security professionals should not really trust anyone. This has advanced a security concept known as *zero trust*, which means that nothing is trusted by default. This concept is discussed in NIST 800-207.

Insiders typically have the means, access, and opportunity to commit crimes. All they may lack is motive. Outsiders, on the other hand, are not trusted with access, and being outside the organization's structure could leave them with little opportunity or means to launch an attack. However, outsiders can be driven by motivations like money, prestige, or national interests. Figure 7.3 shows examples of threat actors and sample attacks.

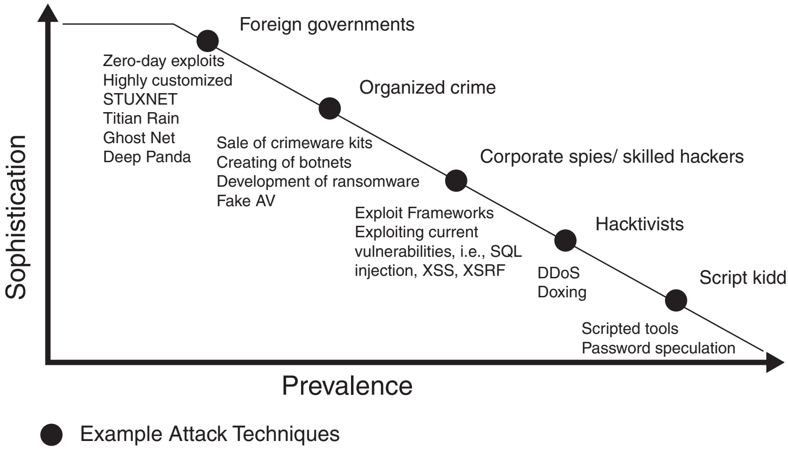


FIGURE 7.3 **Threat Actors and Attacks**

Note

Early hackers, known as *phreakers*, focused on analog phone and telecommunication attacks in the 1980s. Some of these individuals would reverse engineer the specific tones used by telecommunications systems to route long-distance/international calls for free.

Attack Methodologies

Attacks typically target one or more items that are tied to the security triad: confidentiality, integrity, or availability. Whereas confidentiality and integrity attacks actually give the attacker access to your data, availability attacks do not. Availability attacks usually result in denial of service.

Hackers target a variety of devices, but their modus operandi remain fairly constant. Their methodology of attack generally proceeds as follows:

1. **Footprinting**: The attackers identify potential targets, looking for information in places such as the organization's website, public databases, WHOIS, NSLOOKUP, Google groups, and EDGAR financial records.

2. **Scanning**: The attackers move beyond passive information gathering and use a variety of tools to scan for open ports and processes.

3. **Enumeration**: Somewhat similar to scanning, this step involves obtaining more detailed information about target devices, such as operating system identification. Attackers are likely to probe for poorly protected network shares and weak passwords during this phase.

4. **Penetration**: What makes this phase different from the previous one is that the hacker is attacking the network with the goal of gaining access. If access is not possible, the attacker might decide to launch a DoS attack.

5. **Escalation**: Many times the initial level of access gained by an attacker is not root or administrator. During the escalation phase, a hacker attempts to escalate privilege, pilfer data, and gain access to restricted information.

6. **Expanding access**: The attacker does not stop with access to just one system. Typically, attackers attempt lateral movement to expand their reach.

7. **Covering tracks**: When they're in control of the system, most hackers seek to destroy evidence of their activities. They are likely to attempt to plant tools and rootkits on the compromised system to further extend their stay. Rootkits typically serve the purpose of leaving backdoors so the attackers can come and go as they please.

Note

Escalation of privilege is required because some computer operations require special privileges to complete their tasks or can be run only from root, system, or administrative accounts. With horizontal privilege escalation, an attacker moves from one user account to another user account that has the same level of access. Vertical privilege escalation occurs when an attacker moves from an account with lower privileges to one with higher privileges.

Network Security Threats and Attack Techniques

Many threats to network security exist. Many attackers are opportunistic and typically take the path of least resistance, choosing the most convenient route and exploiting the most well-known flaws. Others, such as government spies and corporate hackers, might go to great lengths to gain access to the data or information they desire. In these instances, the attackers or advanced persistent threats (APTs) may spend large amounts of time and money to gain access to resources they covet. As discussed in the following sections, threats to network security can include session hijacking, sniffing, wiretapping, DoS and DDoS attacks, and botnets.

Session Hijacking

A session hijacking attack allows an attacker to take over an existing connection between two hosts that are communicating. It is an effective type of attack because most TCP services perform authentication only at the beginning of the session. In such a case, the attacker simply waits until authentication is complete and then jumps in and takes control of the session. Session hijacking can be performed at the host-to-host layer or the application layer. Protocols like FTP and Telnet can be targeted through prediction of sequence and acknowledgment numbers, and applications can be targeted at the application layer. You may have noticed that some sites log you in using HTTPS, but they use HTTP for the remainder of the connection. In such situations, the session ID and variable are passed via a plaintext cookie over port 80 instead of port 433.

Preventive measures include limiting incoming connections and using encryption provided by tools like Kerberos or IPsec. Plaintext protocols like FTP and Telnet are very vulnerable to session hijacking because all communication is sent in plaintext. Secure Shell (SSH) is a good alternative. SSH establishes an encrypted channel between the local and remote hosts.

Detection can be improved by using IDSs or IPSs. You can make session hijacking more difficult for an attacker by using switches, protocols like SSH, and software that uses more random initial sequence numbers (ISNs).

Sniffing

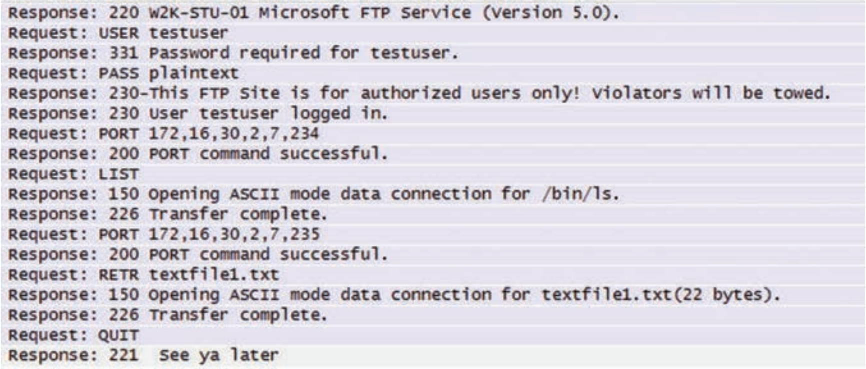
A *sniffer* is a packet-capturing program that captures network traffic and can decode the captured frames. Sniffers work by placing the hosting system's network card in *promiscuous mode*, which means the network card can receive all the data it can see and not just packets addressed to it.

When sniffing is performed on a switched network, it is known as *active sniffing*. There can be exceptions to this rule, however, because some switches can have one port configured to receive copies of all the packets in the broadcast domain. In such a case, passive sniffing can be performed.

When attackers do not have physical access to a switch, they might use techniques like Address Resolutions Protocol (ARP) poisoning and Media Access Control (MAC) address flooding to bypass the functionality of a switch.

Sniffers operate at the data link layer (Layer 2) of the OSI model. Sniffers can intercept whatever they see on the wire and record it for later review. They allow the user or attacker to see all the data contained in a packet—even information that should remain hidden. For sniffers to be successfully used by an attacker, the attacker must be on your local network or on a prominent intermediary point, such as a border router through which traffic passes.

Plaintext protocols are particularly at risk to sniffing. Figure 7.4 shows an example of a plaintext FTP session, which an attacker could use to steal password information. To reduce the threat of sniffing, you should use protocols like IPsec, SSL, and SSHv2 to pass usernames, passwords, and data.



```
Response: 220 W2K-STU-01 Microsoft FTP Service (Version 5.0).
Request: USER testuser
Response: 331 Password required for testuser.
Request: PASS plaintext
Response: 230-This FTP Site is for authorized users only! Violators will be towed.
Response: 230 User testuser logged in.
Request: PORT 172,16,30,2,7,234
Response: 200 PORT command successful.
Request: LIST
Response: 150 Opening ASCII mode data connection for /bin/ls.
Response: 226 Transfer complete.
Request: PORT 172,16,30,2,7,235
Response: 200 PORT command successful.
Request: RETR textfile1.txt
Response: 150 Opening ASCII mode data connection for textfile1.txt(22 bytes).
Response: 226 Transfer complete.
Request: QUIT
Response: 221  See ya later
```

FIGURE 7.4 Sniffing Plaintext Passwords

Wiretapping

Wiretapping traditionally involved connecting to telephone wires, but today it can involve network sniffing, VoIP sniffing, and radio frequency sniffing (for 802.11 networking, cellular traffic, Bluetooth, and so on). If an organization does not encrypt communication before transmission takes place over public networks, attackers can passively or actively eavesdrop on that communication.

In the United States, the Communications Assistance for Law Enforcement Act (CALEA) requires that all telecommunication providers, regardless of the technologies involved, must make it possible to eavesdrop on all forms of communication so that law enforcement can collect information when a proper search warrant is issued. Some of the techniques used to intercept traffic include intercept access points, mediation devices, and programs installed at the ISP that perform the collection function. Although you might not be too concerned about the government intercepting data, you should be concerned about the fact that an attacker could also attempt to use techniques like these to intercept your sensitive and private information.

DoS and DDoS Attacks

The goal of DoS and DDoS attacks is to destroy the availability of information or information systems. Malicious users often attempt these attacks to bring down a network, extort money, or hold the network hostage—sometimes as a last-ditch effort (that is, “If I can’t get in, I’ll make sure no one else does either”). Today, DoS attacks often take a hostage-type ransom approach and are designed to make money for the attackers or to disrupt network communications.

A DDoS attack is an amplified DoS attack. As with a DoS attack, the goal of a DDoS attack is disruption of service. However, a DDoS attack is more powerful in that it uses a large number of previously compromised systems to direct a coordinated attack against the target. These systems, known as *zombies*, wait until the attacker signals the attack. Botnets, discussed in the next section, are used to facilitate DDoS attacks. A DDoS attack can be devastating because of the tremendous amount of traffic generated.

Note

In 2007, a large-scale DDoS attack was launched against a nation for the first time. This attack against Estonia caused severe outages and was blamed on Russian attackers.

Note

Booters are websites that offer DDoS services. These sites are operated by cybercrime groups that provide paying customers with DDoS attack capabilities on demand. These services can hide behind multiple layers of IP addresses and can be very difficult to take down.

Botnets

Attackers are no longer content with just making a name for themselves. Today's attacks are often about making money. Attackers might be out-of-work Eastern European and Russian computer engineers or others working all over the globe. Attacks might be performed for extortion or to generate revenue. These attacks often depend on *botnets*, which were first seen around the year 2001. A botnet is a massive collection of computers that have been compromised or infected and become bots, or zombies (see Figure 7.5). Botnets are used to distribute spam, steal passwords used at banking and shopping websites, launch DoS attacks for extortion, and spread infections to other computer systems. They are not showing any signs of going away. In February 2020, Amazon Web Services (AWS) reportedly defended against a 2.3 Tbps DDoS attack staged by an army of bots.

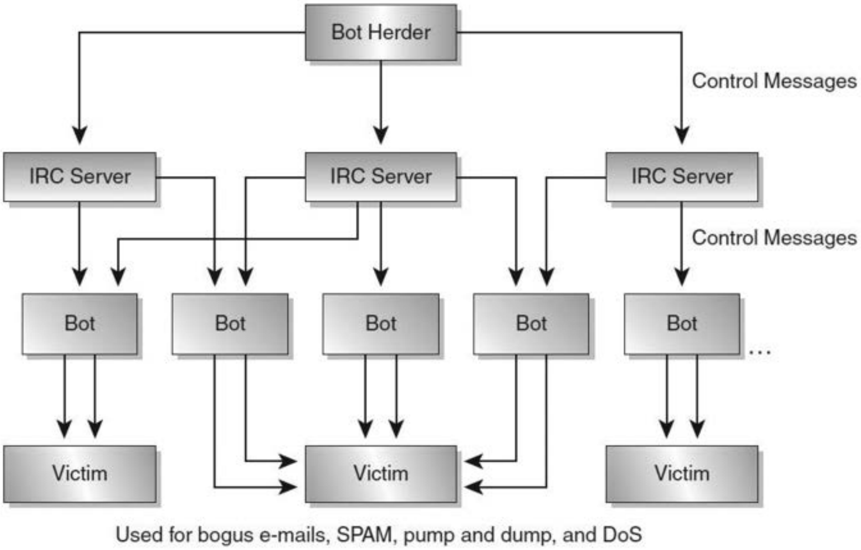


FIGURE 7.5 **Botnet Example**

Note

In 2010, a large group of hacktivists was able to organize a large-scale opt-in botnet attack. The attack, which was organized by the group Anonymous, targeted sites like MasterCard and Visa. These attacks used the application Low Orbit Ion Cannon (LOIC) to flood these sites and disrupt communication.

A botnet attack starts when the controller (called a *bot herder*) seeks to bypass the access control of third-party computers. These computers can be broadband users, home users, or even poorly configured corporate systems.

Bot herders can use a variety of techniques to avoid detection. For example, a fast-flux botnet has numerous IP addresses mapped to one domain name, which means an attacker can swap out IP addresses at an extremely high frequency to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts that act as proxies. Figure 7.6 shows an example.

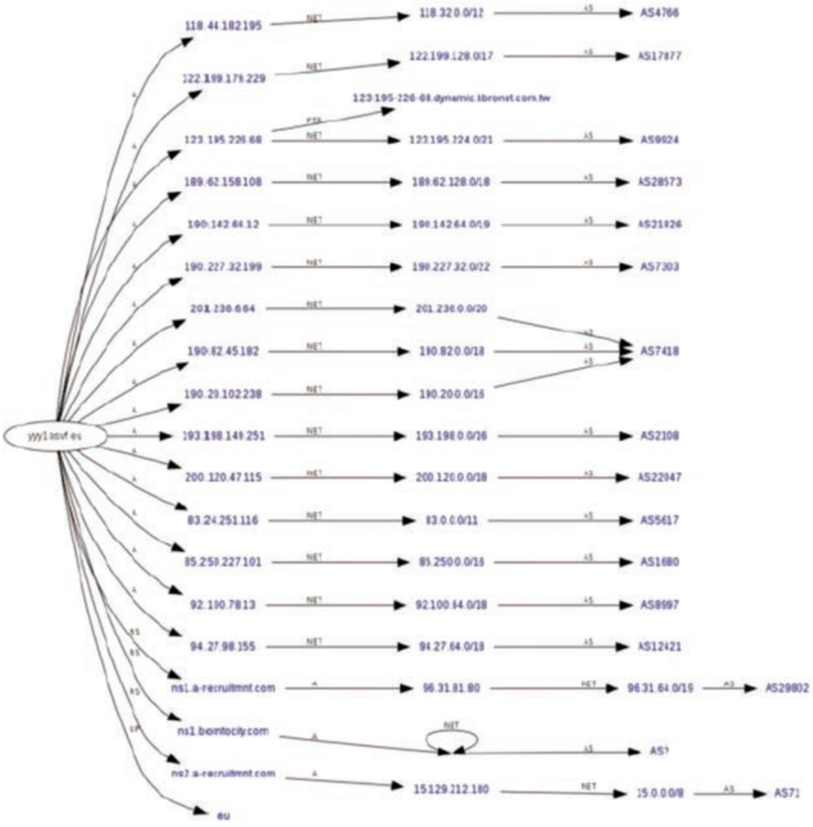


FIGURE 7.6 **Fast-Flux Botnet**

The evolution of botnets has now progressed to the point that they are packaged into *exploit kits*. These prepackaged botnets offer attackers everything they need and typically include detailed instructions.

Note

Botnets have evolved into a multi-million-dollar industry. In October 2020, Microsoft announced legal action seeking to disrupt a botnet cybercrime operation that uses more than 1 million zombie computers to loot bank accounts and spread ransomware (see https://apnews.com/article/technology-malware-elections-crime-cybercrime-913ee5d56affa97fc5d9c639c4a284ab).

Botnets pose a real threat to computer operations, and an organization needs multiple layers of defense to counter this threat. Defenses include the following:

- Patched and hardened computers
- Web security appliances
- Updated antivirus software to identify known threats
- Firewalled networks and the use of intrusion detection and prevention (IDP) systems to monitor traffic
- Routers configured to block spoofed traffic from within a network
- User training to guard against APTs and to adopt safer computing practices

Although these techniques might not prevent all attacks, they are a good starting point. Organizations must develop better security practices to deal with the threat of botnets.

Other Network Attack Techniques

In addition to the attack techniques already discussed, hackers might attempt the following techniques to violate network security:

- **ARP poisoning**: This type of attack is usually attempted to redirect traffic on a switch during the resolution of IP addresses to MAC addresses. An attacker may attempt a series of attacks, including sniffing, session hijacking, and interception of confidential information. Tools such as Bettercap and Ettercap are available to help attackers perform ARP poisoning.

- **Database attack**: This type of attack targets an organization's databases. SQL injection is one common attack vector. Although the techniques vary, the results are the same: Malicious users can run their code on the victim's database server or steal information from the server. This can present a serious threat to the integrity or confidentiality of the organization.

- **DNS spoofing**: Much like ARP poisoning, this type of attack attempts to poison the DNS process while addresses are being resolved from FQDNs to IP addresses. Individuals who succeed have their fake DNS entry placed into the victim's DNS cache or anywhere else the address resolution is taking place, such as on a cooperating DNS server. Victims can then be redirected to the wrong Internet sites or to a rogue server infected with malware, sitting in someone's basement and collecting your private information.

- **Email bombing**: This type of attack is used to target a victim with a large amount of bogus email. The attacker attempts to send so much email that the user's email account becomes completely full.

- **Pharming attack**: This is another type of attack that misuses DNS. Normally DNS is responsible for translating web addresses into IP addresses. Pharming attacks hijack the DNS server and force it to redirect your browser to another site, allowing fake software updates to install malware.

- **Traffic analysis**: This type of attack involves sniffing encrypted traffic to deduce information. Even with encrypted data, inferences can be made; for example, frequent communications can signal that planning is occurring.

- **War driving**: This type of attack involves driving, flying, boating, or walking around an area to find wireless access points. Many individuals who perform this activity look specifically for unsecured wireless networks to exploit. The primary threat is that these individuals might then have a direct connection to your internal network or unrestricted Internet access. This access can then be used to conduct attacks on other Internet sites, send spam, promote pump-and-dump financial schemes, or sell counterfeit goods.

- **Zero-day exploits**: A zero-day exploit can target corruption, modification, release, or interruption of data. This attack takes advantage of an exploit that might not be known to the vendor and for which there is no patch available.

Access Control Threats and Attack Techniques

Access control is probably one of the most targeted security mechanisms. After all, its job is to keep out unauthorized individuals. To try to bypass or subvert access control, attackers can use a variety of tools and techniques, such as unauthorized access, access aggregation, password attacks, spoofing/masquerading, sniffers, eavesdropping, shoulder surfing, and wiretapping. The following sections discuss a number of access control threats and attack methods.

Unauthorized Access

Information needs to be properly protected from unauthorized access, modification, disclosure, and destruction. To protect data, you need to select the best method of authentication for the situation. One important step to help determine what authentication should be used is to perform an asset valuation, which means assigning the dollar and non-dollar values to an asset. When the value of an asset is known, you can determine the appropriate access controls to prevent unauthorized access.

Caution

You can use threat modeling to examine the security risks of an application, including the problem of unauthorized access. A threat model details potential attacks, targets, and any vulnerabilities of an application. In part, threat modeling can help determine the types of access control mechanisms that are needed to prevent attack.

To learn more about threat modeling, review the information on Microsoft's Threat Modeling tool at https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling.

Access Aggregation

Access aggregation, or privilege creep, involves collection of access permissions in one or more systems. For example, say that Grace starts as a help desk employee, and in six months she moves to tech support. If those in charge of access permissions are not paying attention, Grace gains access to the rights and permissions of a technical support representative while maintaining her help desk rights and privileges. Access aggregation can cause employees to potentially end up with a greater level of access than they should have. This is a big problem for many organizations, and it violates the security principle of least privilege. I have witnessed access aggregation at almost every organization I have worked at, but it can be managed with regular user audits and a good policy based on the principle of least privilege.

Password Attacks

Do you think your passwords are secure? In 2019, a breach at Evite exposed records including 100 million passwords, and a breach at Canva exposed details of 137 million user accounts.

Many individuals don't practice good password security and reuse passwords. This can lead to problems such as *credential stuffing*, which is a cyberattack in which credentials obtained from a data breach on one service are used to attempt to log in to another unrelated service. Password hashes can be recovered in several different ways, as discussed in the following sections.

Dictionary Cracking

Dictionary cracking involves using a predefined dictionary to look for a match between an encrypted password and an encrypted dictionary word. Many dictionary files are available, ranging from files for Klingon to popular movies, sports, and the MBA. Many times, these cracks can be performed in just a few minutes because individuals tend to use easily remembered passwords. If passwords are well-known dictionary-based words, dictionary tools can crack them quickly.

Just how do dictionary cracking programs recover passwords? Passwords are commonly stored in a hashed format, and most password-cracking programs use a technique called *comparative analysis* (see Figure 7.7):

1. The hashed password must be recovered.
2. The recovered password and the dictionary list are loaded into the cracking program.
3. Each potential password found in a dictionary list is hashed and compared to the encrypted password.
4. If a match is obtained, the password has been discovered. If not, the program continues to the next word, computes its hashed value, and compares that to the hashed password.

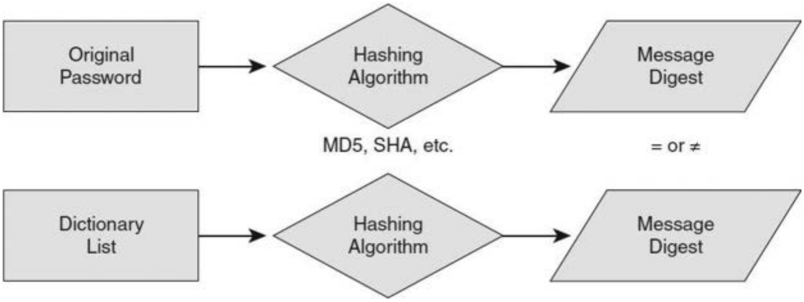


FIGURE 7.7 **Dictionary Cracking**

Dictionary cracking programs are comparatively smart because they can manipulate a word and use its variations. For example, a dictionary-cracking program would process the word *password* as *Password*, *password*, *PASSWORD*, *PassWord*, *PaSSword*, and using all other common permutations of the word.

Caution

Never store passwords as plaintext, don't write them on sticky notes attached to your computer, don't share them with others. Passwords should always be created and stored by means of a one-way hashing process.

If a dictionary attack does not recover a password, the attacker can also try simple modifications of each dictionary word. Those modifications might include adding common prefixes, suffixes, and extended characters to try to crack the password. This is called a *hybrid attack*. Using the previous example, these attempts could include *123password*, *abcpassword*, *drowssap*, *p@ssword*, *pa44w0rd*, and so on. These various approaches increase the odds of successfully cracking an ordinary word or any common variation of it.

Caution

Don't make passwords public. Only use passwords once and don't use the same password for multiple sites. Once passwords are breached it is easy for hackers to find them. The www.hackersforcharity.org/ghdb/ website provides resources that can highlight how big this password exposure problem is. At the site you will find various search strings to search for exposed passwords and other sensitive data.

Brute-Force Cracking

Attackers don’t tend to give up easily. A *brute-force crack* is a type of password assault (usually associated with encryption, though it doesn’t have to be) and can take hours, days, months, or years, depending on the complexity of the password and the key combinations used. The attacker attempts every possible combination of letters, numbers, and characters, and with enough time, recovery is possible. The speed of this type of password cracking depends on the power of the CPU being used to carry out the attack. For example, password crackers have been developed to recover weak passwords quickly. There are also many online sites that can be used for cracking or to test password strength.

Rainbow Tables

What if you do not have a week to crack passwords? An alternative to traditional brute-force password cracking is to use a rainbow table. Whereas traditional password cracking encrypts each potential password and looks for a match, the rainbow table technique precomputes all possible passwords in their *hashed value* in advance and stores them in a table. This is considered a time/space/memory trade-off technique. Precomputing the hashes requires the creation of massive databases of hashed values for every potential password, from single characters on up, using all keyboard characters. Creating hashes for the character set ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~’[]{}|\:;”’<>,.?/ would require about 64 GB and a considerable amount of time. When this process is complete, the passwords and their corresponding encrypted values are stored in a file called a *rainbow table*. An encrypted password can be quickly compared to the values stored in the table and cracked within a few seconds. For those who do not have the time or want to build their own, rainbow tables are available via BitTorrent and online.

> **Caution**
>
> Rainbow tables currently exist for Windows LAN Manager passwords up to 14 characters in length. These precomputed hashes have been demonstrated to attack and crack passwords with a 99% success rate in less than three hours. This means that if an attacker can recover a basic LAN Manager password, the encrypted password can most likely be cracked!

To protect your organization from these password attacks, you can implement two-factor authentication and lockout thresholds, monitor access to electronic password files, and enforce a strong password policy using as many different types of characters as possible, including lowercase and uppercase letters, numbers, and symbols. Users should change their passwords frequently, never reuse previous passwords, and not use the same password for more than one account.

Caution

Some organizations and government agencies require passwords to be longer than 15 characters. Having a longer password makes cracking it via brute force more difficult and requires the hacker to use additional time and resources to discover the password. NIST 800-63C provides guidelines on passwords and their complexity.

Spoofing

Spoofing, which is pretending to be something other than what you are on a network, can take place at different layers of the OSI model as it can be used on protocols, processes, services, and humans. *User spoofing*, which occurs when one user pretends to be another user, can involve changing usernames, IP addresses, or even MAC addresses. *Process spoofing* occurs when a process pretends to be a valid process when in fact it is not. An example of process spoofing involves use of a fake login screen (either inside an organization or on the Web). When a victim attempts to log in, the first attempt to the fake login screen is unsuccessful, and the victim, who thinks he simply mistyped the password the first time, is redirected to the real login page for a second attempt. However, the attacker used the attempt at the fake login screen to gather the credentials and store them for later use at the actual site.

Eavesdropping and Shoulder Surfing

Securing voice communication is a critical component of good security. There are plenty of opportunities to eavesdrop on or intercept phone calls and conversations. For example, during a recent trip, I had an interesting breakfast at the hotel: Someone a few tables away gave out their username and password to someone on the phone who needed assistance. *Eavesdropping* is the act of overhearing sensitive information or data, either on purpose or by accident. Eavesdropping can occur with telephone, network, email, or instant messaging traffic. *Shoulder surfing* is a related activity in which someone glances over your shoulder while you enter a password or username. Employees should be trained in how to avoid such potential problems. To combat shoulder surfing, for example, users may use monitor mirrors to see if anyone is looking over their shoulder or privacy screens to make it impossible for anyone who is not right in front of the screen to read it.

Identity Theft

Identity theft involves obtaining key pieces of information about an individual. Most attacks in the past were launched for notoriety and fame. Today's attackers seek money and access to valuable resources. Identity thieves may dig through the trash looking for information, or they may attempt to trick users into providing the information they need. Identity theft is big business. According to the FBI, 157,688 credit card fraud reports were filed in the United States in 2018, and about $1.48 billion was lost due to identity theft.

Social-Based Threats and Attack Techniques

Social engineering attacks use a variety of techniques and can be launched in person, remotely via phone, or via a computer. The target of such an attack may be known or unknown. Social engineering attacks take many forms.

Think of *phishing* as throwing out a broad net to all users (for example, emails from a person in Nigeria offering to give you $1 million). Some phishing scams work by sending the victim an email from what appears to be an official site, such as a bank or credit card company. The email usually contains a link the user can click to update, change, or modify her account information. The real purpose of the email and link is to steal the victim's username, PIN, account number, or password. Employees should be trained to always be wary of links obtained in emails, be alert to messages that request password verification or resetting, be skeptical of emails requesting information, and verify that the correct URL is listed in the address bar. To see what PayPal has to say about phishing, see www.paypal.com/us/webapps/mpp/security/suspicious-activity.

Spear phishing is targeted phishing. For example, a phishing email might be sent only to people who use a particular service. *Whaling* is an attempt to capture an important user, such as an executive or a CEO. Some social engineering attacks make use of the SMS messaging service used on mobile phone devices; this is known as *smishing*.

Another social engineering attack vector is *pretexting*, the practice of obtaining personal information about an individual under false pretenses. Pretexting is usually done to gather more information about a certain individual in order to sue him, to steal his assets, obtain credit in his name, or gain access to resources at his place of employment. Pretexters use a variety of techniques, all of which are simple variations of social engineering techniques. A pretexter might, for example, call your cell phone provider and ask for a reprint of a bill or call and say they lost their checkbook or even contact your credit card provider. In most cases, pretexting is illegal, and there are laws against pretending to be someone else to gain personal information.

Regardless of how the victim is targeted, social engineering attacks are designed to lure victims into disclosing confidential information, passwords, or other sensitive data. Social engineering is not new; in fact, it predates the computer era. Social engineering is much like an old-fashioned con game in that the attacker uses the art of manipulation to trick a victim. Social engineering attacks are often combined with technical attacks. For example, you might find a thumb drive that is labeled "spring break photos" in a parking lot. If you insert the thumb drive into a computer, you will unleash remote control software, such as Trojans, designed to infect your computer.

Table 7.2 lists some social engineering techniques.

TABLE 7.2 **Social Engineering Techniques**

Technique	Description
Impersonation	Pretending to be someone or something else
Spoofing	Using someone else's IP address, domain name, or MAC address
Shoulder surfing	Looking over someone's shoulder to view sensitive information
Virus hoax	Sending a pretend virus to elicit a specific response
Tailgating and piggybacking	Driving or walking behind someone at a checkpoint
Dumpster diving	Digging through trash to look for items of value, such as passwords, manuals, and account names

The best defense against social engineering is to educate users and staff never to give out passwords and user IDs over the phone, via email, or to anyone who isn't positively identified. Users should be leery of links and login pages that don't look right. Training can go a long way toward teaching employees how to spot social engineering.

Malicious Software Threats and Attack Techniques

During the 1970s, when mainframes were prominent, the phrase *computer virus* did not exist. Fred Cowen is credited with coining the term in 1983. Early computer crimes included malware, such as the Brain (1986), which was written by two Pakistani brothers who said they were just out to make a name for themselves. Even the 1988 Morris worm was said to have been an accident. As described in the following sections, today's malicious software is much more advanced than the simple viruses and worms from years ago.

Tip

Can a 75-cent error lead to the discovery of foreign government hackers? It did for Cliff Stoll. He used the accounting error to track down and find KGB hackers. The FBI initially refused to take him seriously as his focus was in astrophysics, but he persisted. You can read more about it in his book *The Cuckoo's Egg*.

Viruses

Virus propagation requires human activity, such as booting a computer or opening an email attachment. The following are some of the basic techniques used to propagate viruses:

- **Master boot record infection**: In this original method of attack (which is now obsolete), a virus attacked the master boot record of a floppy disk or hard drive.
- **File infection**: This slightly newer technique relies on the user to execute the file. Extensions like `.com` and `.exe` are typically used. Usually, some form of social engineering is used to get the user to execute the program. Techniques include renaming the program or changing the `.exe` extension to make the file appear to be a graphic or document.
- **Macro infection**: Macro viruses exploit scripting services installed on a computer. The I Love You virus is a prime example of a macro infector. Macro viruses infect applications like Word or Excel by attaching themselves to the application's initialization sequence or automated tasks within the application. These tasks run without user intervention, and when the application is started, the virus's instructions execute before control is given to the application. Then the virus replicates itself, infecting additional parts of the computer.
- **Fileless infection**: This modern type of infection started gaining prominence around 2017. With fileless infection, no files are written to the infected system's hard drive; fileless malware infection exists exclusively in computer memory. Virus and malware creators use fileless infections to trade persistence for stealth. Keeping the malware infection concealed while it triggers the intended action is the goal.

As virus writers change their approaches, antivirus companies have to develop better ways of detecting viruses, such as using artificial intelligence (AI). To keep pace, malware authors get clever and try to postpone detection by security vendors as long as possible. Another technique that virus developers have attempted is to make viruses polymorphic (from the Greek *poly*, meaning "many," and *morph*, meaning "shape"). A polymorphic virus can make copies of itself and change its signature every time it replicates and infects a new file. Fuzzy hashing is a technique that can be used against polymorphic viruses and malware. The concept is to execute a type of compression function to calculate and flag similar digital files. Fuzzy hashing helps automate the process of grouping and identifying similar malware.

Worms

Worms are unlike viruses in that they can self-replicate, whereas viruses require user interaction. True worms require no intervention and are hard to create. A worm does not attach to a host file but is self-contained and propagates across networks automatically. The first worm released on the Internet was the 1988 Morris worm. Robert Tappan Morris developed the worm as only a proof of concept. The Morris worm targeted aspects of `sendmail`, `finger`, and weak passwords, disabling roughly 6,000 computers connected to the Internet. Its accidental release was a rude awakening to the fact that worms can do massive damage to the Internet. The cost of the damage from the worm was estimated to be between $10 million and $100 million. Many other worms have been created since then. A relatively recent well-known worm is Stuxnet.

Worms, like viruses, are becoming less commonplace as malware creators focus their time on ventures that will generate revenue. For the CISSP exam, keep in mind that today's malware is sophisticated and can actually perform the tasks of both viruses and worms.

Note

Spam is one of the techniques used to spread viruses and worms. While much of the spam of the past was simply junk mail, more and more of it today is malicious in nature.

Logic Bombs

Logic bombs are somewhat different from viruses and worms as they are hidden in code. The malicious programming code is placed within an application's code and set to execute under given circumstances, such as after a certain amount of time has elapsed or when a specific event occurs.

Note

Logic bombs and other kinds of malware can be used to launch salami attacks. This financial crime works by taking small amounts of money from accounts over an extended period. For the attackers to be successful, they must remove an amount so small that it will go unnoticed. The 1999 movie *Office Space* offers a good example of this type of attack.

Backdoors and Trojans

Trojans get their name from Homer's epic tale *The Iliad*. To defeat their enemy, the Greeks built a giant wooden horse with a hollow belly and tricked the Trojans into bringing it into the fortified city of Troy. Unbeknown to the Trojans, Greek soldiers were stowed in the belly of the horse, and they crawled out, under the cover of darkness, opened the city's gate, and allowed the waiting Greek soldiers in; the complete fall and destruction of the city ensued.

In computer security terms, Trojans are programs that seem to do something you want but actually perform another, malicious, act. Before a Trojan program can act, it must trick the user into downloading it or performing some other type of action.

Consider a home user who sees nothing wrong with illegally downloading a movie from the Internet. After it has been downloaded, however, the user finds that the movie will not play and receives a message about a missing driver or codec. The user is prompted to go to a site that has a movie player with the right codec installed. The user does as instructed and, sure enough, everything works. It seems like a movie without any cost, but at the time the user installed the movie player, he also installed a remote-access Trojan (RAT) that was actually part of the player.

A Trojan may be configured to do many things, such as log keystrokes, add the user's system to a botnet, or give the attacker full access to the victim's computer. A user might think that a Trojan masquerading as a Word doc, a PDF, an image, or some other file looks harmless and is safe to run but, once executed, it delivers its malicious payload.

You might be wondering at this point how users get infected with Trojans. Often, the infection results from a combination of factors that includes social engineering. Email, social media, instant messaging (IM), and Internet Relay

Chat (IRC) can be used to spread malware. You might, for example, get an email that appears to be from HR but that is actually spoofed and has an attachment named “pending fall layoffs.” It would be tempting to open it; you want to see attachments that are important or that you believe are sent by friends or coworkers. Again, this is an area where education is essential.

Wrappers, Packers, and Crypters

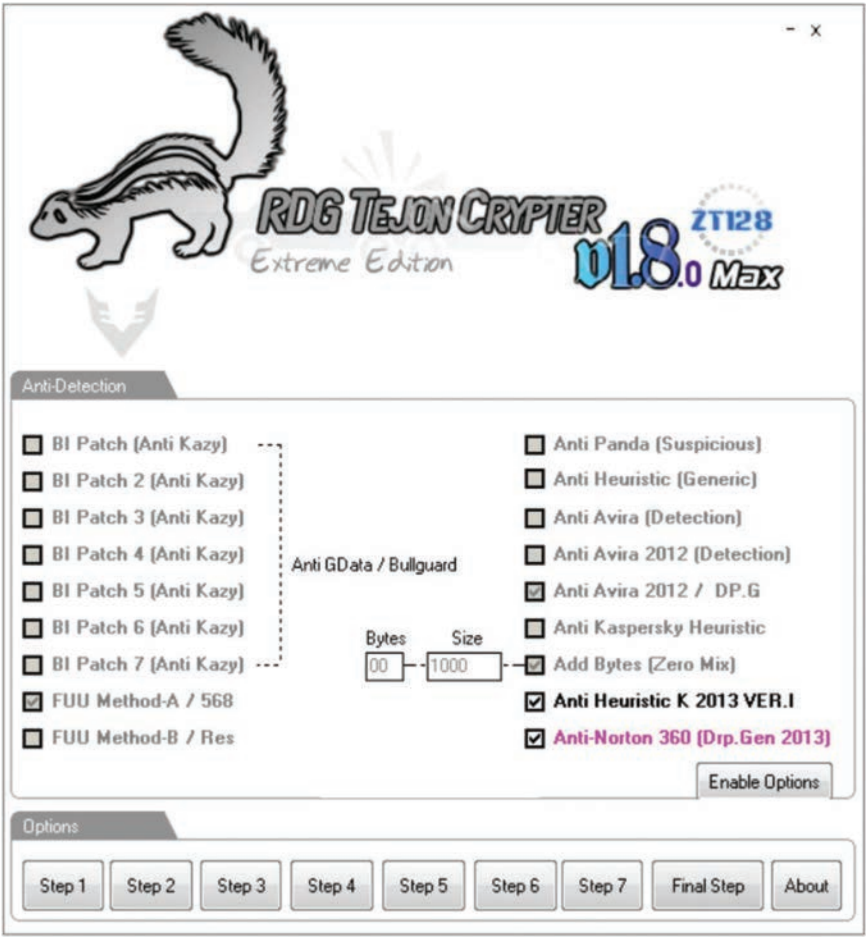
Distributing Trojans or any malware is no easy task. Users are more alert, less willing to click email attachments, and more likely to be running antivirus or other antimalware tools than in the past.

Today, it is not uncommon for attackers to use multiple layers of techniques to obfuscate code—such as making hostile code undetectable by antivirus programs and using techniques to prevent others from examining the code. These layers improve the attacker’s chances of controlling a computer infected by Trojans or other malware and using it for many types of illegal purposes. Techniques to be aware of are wrappers, packers, and crypters.

Wrappers provide hackers a method to slip past a user’s normal defenses. A *wrapper* is a program used to combine two or more executables into a single packaged program, essentially creating a new executable file. Some wrappers only allow two programs to be joined; others allow three, four, five, or more programs to be bound together. Basically, these programs perform like installation builders and setup programs. Wrappers also add additional layers of obfuscation and encryption around the target file. Wrappers are commonly made to seem like graphic files, music files, and non-executables.

Packers work much like programs such as WinZip, Rar, and Tar, in that they compress and/or encrypt files. Whereas compression programs do this to save space, packers do it to obfuscate the activity of the malware. The idea is to prevent anyone from viewing the malware’s code until it is placed in memory. Packers serve a second valuable purpose for an attacker: They bypass network security protection mechanisms, such as intrusion detection systems. It is not until the malware packer decompresses the program in memory that the program’s original code is revealed.

Crypters function to encrypt, manipulate, or obscure code. Some crypters obscure the contents of a Trojan, for example, by applying an encryption algorithm. Crypters can use any encryption scheme, from AES or RSA to Blowfish, or they might use more basic obfuscation techniques, such as XOR obfuscation, Base64 encoding, or ROT 13. These techniques are used to conceal the contents of the executable program, making it undetectable by antivirus software and resistant to reverse-engineering efforts. Figure 7.8 shows Tejon Crypter, a tool used to wrap malware to avoid detection.



□ BI Patch (Anti Kazy)
□ BI Patch 2 (Anti Kazy)
□ BI Patch 3 (Anti Kazy)
□ BI Patch 4 (Anti Kazy)
□ BI Patch 5 (Anti Kazy)
□ BI Patch 6 (Anti Kazy)
□ BI Patch 7 (Anti Kazy)
☑ FUU Method-A / 568
□ FUU Method-B / Res

Anti GData / Bullguard

Bytes: 00
Size: 1000

□ Anti Panda (Suspicious)
□ Anti Heuristic (Generic)
□ Anti Avira (Detection)
□ Anti Avira 2012 (Detection)
☑ Anti Avira 2012 / DP.G
□ Anti Kaspersky Heuristic
☑ Add Bytes (Zero Mix)
☑ Anti Heuristic K 2013 VER.I
☑ Anti-Norton 360 (Drp.Gen 2013)

FIGURE 7.8 **Tejon Crypter**

Rootkits

A rootkit is a collection of tools that allows an attacker to take control of a system. Although the use of rootkits is widespread, many security professionals still don't know much about them.

Once installed, a rootkit can be used to hide evidence of an attacker's presence and provide backdoor access to the system. A rootkit can contain log cleaners that attempt to remove all traces of the attacker's presence from the log files. Even if you can detect and clean a system that has a rootkit installed, you are unlikely to find the attacker. The fact is that a majority of individuals who attack systems go unpunished.

Rootkits can be divided into several different types, including applications, kernel modules, hardware, firmware, and bootloaders. For example, a loadable kernel module (LKM) rootkit is loaded as a driver or kernel extension. Because LKM rootkits corrupt the kernel, they can do almost anything, and they are by far the most dangerous rootkits.

Rootkits can avoid detection by many software methods, but there are means to detect them. Tools like MD5sum, Tripwire, and GMER can be a big help in uncovering some types of rootkits.

Exploit Kits

Exploit kits offer someone with no or little programming experience the ability to create, customize, and distribute malware. A large proportion of exploit kits are sold by hackers from Eastern Europe and Russia.

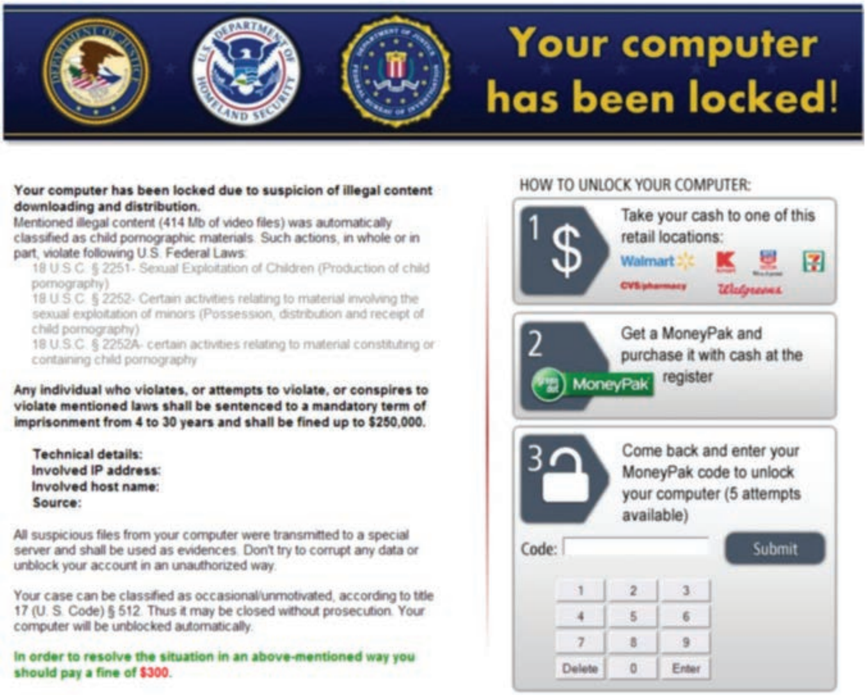
Some exploit kits also offer *bulletproof hosting*, which protects malware-infected websites from being shut down by their service providers. In the United States, when a website is found to contain malware, there are legal ways to take the site offline and prevent it from being used to infect other websites. However, in some countries such as in Russia, infected websites are often bulletproof: They are protected from being taken down, and cybercriminals have safe platforms for hosting their malware and infecting U.S. consumers and businesses.

Advanced Persistent Threats (APTs)

An advanced persistent threat (APT) is a highly sophisticated and well-organized group, government, or organization that has the capability and determination to target a very specific victim organization for an extended period of time with the goal of a *success attack*. Such attackers might use sophisticated malware, zero-day exploits, and other techniques to exploit vulnerabilities in targeted systems. Stuxnet is an example of an APT.

Ransomware

Imagine that you come in to work one day, boot up your laptop, and find a warning message on your screen like the one shown in Figure 7.9. Sometimes these types of messages claim to be from the FBI or an international law enforcement agency, and sometimes they accuse users of illegal activity, such as visiting illegal or inappropriate websites. This type of message is a sign that a hacker has taken over your computer and wants money before he or she will give it back. This is *ransomware*, a type of malware that hackers install on your computer so they can lock it from a remote location and then demand money. Ransomware forces victims to experience financial damage either by paying the ransom or by absorbing the cost of recovering from the attack. Ransomware has become a widely used instrument in the toolkit of cybercriminals.



Your computer has been locked!

Your computer has been locked due to suspicion of illegal content downloading and distribution.
Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)
18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to $250,000.

Technical details:
Involved IP address:
Involved host name:
Source:

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.

Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of $300.

HOW TO UNLOCK YOUR COMPUTER:

1 Take your cash to one of this retail locations:

2 Get a MoneyPak and purchase it with cash at the register

3 Come back and enter your MoneyPak code to unlock your computer (5 attempts available)

Code:

FIGURE 7.9 Ransomware

If a computer gets infected with ransomware, it may difficult or impossible to open the files on that machine. This is one of the reasons it's so important to constantly back up your data and encrypt it yourself; then, in the event that it is stolen, you can tell the threat actors to keep your encrypted data because it is useless to them, and you can just restore your backup. There are many ways to back up either locally or to a cloud-based provider. It is important to be prepared for a disaster like this.

Closely related to ransomware is *rogue security software*. This fake antivirus software attempts to convince users that their computer is infected and manipulates them into buying and downloading the fake software. However, the link takes the user to malware that infects the computer.

Investigating Computer Crime

Security incidents can come in many forms. They can result from honest mistakes by employees who thought they were helping, or they may result from intentional attacks by insiders or outsiders. One of the basic tests to help identify or eliminate potential suspects is *means*, *opportunity*, *and motive* (MOM), also known as *the crime triangle* (see Figure 7.10). MOM demonstrates why insiders pose a greater threat to security than outsiders: Insiders possess the means and opportunity to launch an attack, whereas outsiders might have only a motive.

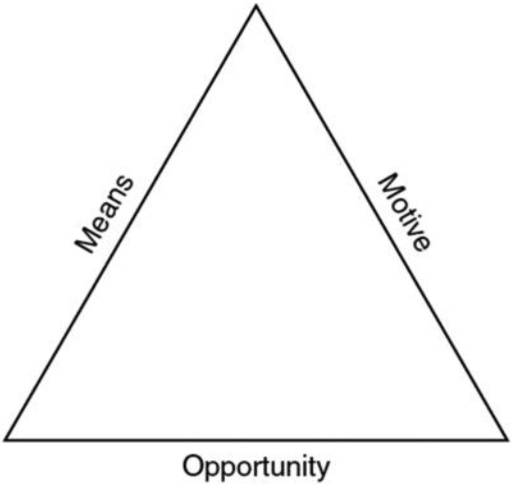


FIGURE 7.10 Crime Triangle

Whatever the motive or reason, the response to a security incident should always be the same: It should be investigated in a structured, methodical manner. Most organizations would not operate a business without training their employees to properly respond to fires, but many organizations do not build good incident response and investigation procedures for cybercrime.

Computer Crime Jurisdiction

The unpleasant truth is that tracking and prosecuting hackers can be a difficult job because international law is often ill-suited to deal with these problems. Unlike a conventional crime that occurs in one location, a hacking crime might originate in India, use a compromised computer network located in Singapore, and target a computer network located in Canada. Different countries' conflicting views on what constitutes cybercrime and disagreements on how—or even if—the hackers should be punished can cause legal nightmares. It is hard to apply national borders to a medium like the Internet that is essentially borderless. The United States has proposed legislation to claim jurisdiction over any criminal activity that travels through a U.S.-controlled portion of the Internet, regardless of the starting or destination country.

Incident Response

The Defense Advanced Research Projects Agency (DARPA) formed an early emergency response team in 1988. Many people attribute the founding of its Computer Emergency Response Team (CERT) to the Morris worm, which occurred earlier that year. The "Information Superhighway" was little more than a dirt road in 1988, so the delayed response wasn't fatal. Few of us today have the luxury of waiting until after an attack to form an incident response plan. To reduce the amount of damage that attackers can cause, organizations need to have incident response and handling policies in place. These policies should dictate how the organization responds to various types of incidents. Most organizations set up a *computer security incident response team* (*CSIRT*) or *computer incident response team* (*CIRT*) because CERT is now a registered trademark of Carnegie Mellon University. A CSIRT or CIRT is responsible for the following:

- Analyzing an event notification
- Responding to an incident if the analysis warrants it
- Conducting escalation path procedures
- Resolving, conducting post-incident follow-up, and reporting to the appropriate individuals
- Deterring future attacks

An *event* is a noticeable occurrence. For example, say that an IDS alert is tripped. This requires investigation because you must determine whether the event is an *incident*—that is, an adverse event or series of events that violates law, policy, or procedure. The individuals investigating the incident need a variety of skills, including the following:

- Recognition skills and abilities
- Technical skills and abilities
- Investigative and response skills

The individuals in charge of handling an incident must be able to recognize that something has happened. In the example of the IDS alert, recognition is not enough because those responsible must also have the ability to look at logs and event records and perform incident analysis. They also need to have the skills to properly investigate the incident and understand concepts such as chain of custody.

The Incident Response Team

Incident response team members need to have diverse skill sets. Internal teams should include representation from various departments, including the following:

- Information security
- Legal
- Human resources
- Public relations
- Physical security
- Network and system administration
- Internal auditing
- Information technology help desk

Many people need to be involved in an incident if the attack came from inside the organization. Legal, HR, and others must determine what will be done. Incidents traced to outside the organization must also have many groups involved. Will management want to involve the police? If so, someone will need to act as an organizational spokesperson. Roles must be clearly defined, as must the process for escalating incidents to the proper authority.

The Incident Response Process

The incident response process spells out the specific steps an organization will carry out when an incident takes place. Good incident response procedures give an organization an effective and efficient means of dealing with an incident in a manner that reduces the potential impact. These procedures should also provide management with sufficient information to decide on an appropriate course of action. By having these procedures in place, an organization can maintain or restore business continuity, defend against future attacks, and prosecute violators to deter further attacks.

The primary goals of incident response are to contain the damage, find out what happened, recover from the incident, get systems back online, and prevent such an event from reoccurring. The following are the basic steps of incident response (see Figure 7.11):

1. **Planning and preparation**: The organization must establish policies and procedures to address the potential for security incidents.
2. **Identification and evaluation**: Automated systems should be used to determine whether an event occurred. There must be a means to verify that an event was real and not a false positive. Tools used for identification include IDSs, IPSs, firewalls, audits, logging, and observation.

> **Note**
>
> An *event* is a noticeable occurrence, whereas an *incident* is a violation of policy or law.

3. **Containment and mitigation**: Preplanning, training, and the use of predeveloped procedures are key to this step in the process. The incident response plan should dictate what action needs to be taken. The incident response team requires training to the desired level of proficiency to properly handle the response. This team also needs to know how to contain the damage and determine how to proceed.

> **Note**
>
> Management needs to make a decision about whether law enforcement should be called in during a security breach. There are reasons both for and against notifying law enforcement.

4. **Eradication and recovery**: Containing a problem is not enough. It must also be removed, and steps need to be taken to return to normal business processes.
5. **Investigation and closure**: When the investigation is complete, a report, either formal or informal, must be prepared. The report should be used to evaluate any needed changes to incident response policies.
6. **Lessons learned**: At this final step, all those involved in the incident response need to review what happened and why. Most importantly, what changes must be put in place to prevent future problems? Learning from what happened is the only way to prevent it from happening again.

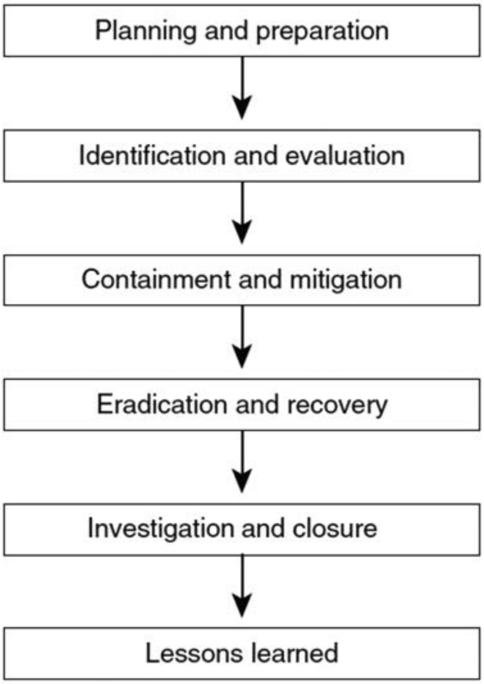

Planning and preparation
Identification and evaluation
Containment and mitigation
Eradication and recovery
Investigation and closure
Lessons learned

FIGURE 7.11 **Incident Response Steps**

There are several specialized incident response methodologies available, such as the MITRE ATT&CK six-stage framework and the Lockheed Martin seven-stage Cyber Kill Chain framework. Both of these methodologies describe the structure and lifecycle of a cyberattack.

Incident Response and Results

Incident response procedures must be of such detail that they specify unique types of incidents and provide advice on what the proper response would be. Documentation that addresses potential incidents is critical because investigating computer crime is complex and involved. Missteps can render evidence useless and unusable in a court of law. Members of the incident response team must be knowledgeable of the proper procedures and must be trained in how to secure and isolate the scene to prevent contamination. Table 7.3 outlines some sample response strategies.

TABLE 7.3 **Sample Incident Response Strategies**

Incident	Response Strategy
Possible data theft	Contact legal department, make forensic image, secure evidence
External hacker attack	Capture logs, monitor activities, gather evidence, contact management
Unauthorized use of computer resources	Gather evidence, make forensic image, analyze data, review corporate policy

In the end, incident response is about learning. The results of the team's findings should be fed back into the system to make changes or improve the environment so that the same incident isn't repeated. Tasks you might end up doing as a result of an attack include the following:

- Figuring out how the attack occurred and looking for ways to prevent it from happening again.
- Upgrading tools or software in response to finding out what the team lacked that prevented effective response to the incident.
- Finding things that went wrong and making changes to the incident response plan to improve operations during the next incident.

Note

The massive SolarWinds breach in 2021 is a good case study in incident response and how attackers have changed the way they operate. Modern attacks are much more sophisticated than attacks in the past. One common tactic today is the use of lateral movement. In the SolarWinds attack, a software update process in a network management tool was compromised, and threat actors were able to gain deep access into targeted networks. The attackers were able to easily pivot from one system to another, gaining access and data as they moved. See https://www.cisecurity.org/solarwinds/ for more information.

Although no one ever wants to end up in court or to take incident response to the next level, sometimes those steps are inevitable. An organization must handle incident response meticulously in order to be prepared for whatever unfolds in an investigation.

Note

Ultimately, incident response is about learning. These are the questions that should be answered: What happened? How did it happen? Can we prevent it from happening again? How can we better prepare and respond for the next time? What did we learn?

Disaster Recovery and Business Continuity

Disaster recovery and business continuity deserve mention because the threats discussed in this chapter can disrupt mission-critical operations. Disaster recovery is a subset of business continuity activities. Imagine your organization being hit with a ransomware attack that encrypts all data in your data center. Mission-critical operations would not be able to continue, and business continuity could not be maintained. *Mission-critical operations* are operations that are required to keep your business going. Most organizations cannot afford to be without operations for very long. When a disaster occurs, operations halt, and business continuity has failed. Business continuity is about keeping critical process up and running. Anyone can trigger an alert in an emergency situation. However, only the business continuity plan (BCP) coordinator or the appointed person can declare the situation a disaster and trigger the fallover to another site, cloud provider, facility, and so on.

Disaster recovery is a subset of the BCP effort that is more closely focused on restoring systems after an outage or event. Disaster recovery focuses on the immediate measures to restore operations and is concluded when the organization is back to normal operations.

Tip

It is important to validate backups before they are needed. This activity should be built in to your normal processes. Two common means of validation are restoring a file from a random date and restoring a server or the entire service from backup. Assume during the recovery that you will start with nothing.

An organization needs to perform test and discovery drills at least once a year. While there are multiple ways to test a business continuity plan, it is most important to understand that you should have no confidence in the plan until it has been tested. As part of testing, you should look at your backup solutions such as uninterruptible power supplies (UPS) and generators. While generators can be used for longer-term outages, UPSs are typically for short-term outages and graceful shutdown of systems.

Note

When testing business continuity and disaster recovery plans, there are two main objectives: validate that the plan functions properly and identify updates to the plan that are needed due to technology/business process changes.

Investigations

An *investigation* is typically a probe or an inquiry into questionable activities and can occur after an incident response or in conjunction with forensic activities. IT professionals do not have the same investigative abilities as law enforcement professionals. The following sections cover some areas of concern in investigations.

Search, Seizure, and Surveillance

In the workplace, surveillance can be broken down into two categories:

- **Physical**: Examples of physical surveillance include closed-circuit television (CCTV) cameras, observation, and security guards.
- **Logical**: Examples of logical surveillance include system monitoring, keystroke logging, and network sniffers.

Caution

Before you attempt any type of monitoring, be sure to check with your organization's legal department. Laws at both the state and federal levels require notification as to the expectation of privacy that someone has while using computer resources. You need to know the laws to avoid breaking them.

Interviews and Interrogations

At some time during an investigation, it might be determined that interviews and interrogations need to be conducted. Areas of concern include the possibility that disclosing the investigation might tip off the suspect to halt his or her activities. The suspect might also flee to avoid prosecution. Some suspects might try to deceive the investigator to prevent further action. Many individuals will lie or misrepresent the truth to avoid being fired or facing legal action.

Investigators must be properly trained to carry out interviews and interrogations. For example, investigators must understand the difference between enticement and entrapment. *Enticement* is legal and ethical. For example, a honeypot is a form of enticement and is legal. *Entrapment*, on the other hand, is illegal. For example, sending someone a phishing email to lure him in your network and then accusing him of breaking in, is illegal.

Exam Prep Questions

1. IP spoofing is commonly used for which of the following types of attacks?
   - ❍ **A.** Salami
   - ❍ **B.** Keystroke logging
   - ❍ **C.** DoS
   - ❍ **D.** Data diddling

2. Which of the following best describes session hijacking?
   - ❍ **A.** Session hijacking works by subverting the DNS process. If this is successful, an attacker can use an already established TCP connection.
   - ❍ **B.** Session hijacking subverts UDP and allows an attacker to use an already established connection.
   - ❍ **C.** Session hijacking targets the TCP connection between a client and a server. An attacker who learns the initial sequence might be able to hijack a connection.
   - ❍ **D.** Session hijacking works by subverting the DNS process. If this is successful, an attacker can use an already established UDP connection.

3. Several of your organization’s employees have been hit with email scams over the past several weeks. One of these attacks successfully tricked an employee into revealing his username and password. Management has asked you to look for possible solutions to these attacks. Which of the following is the best solution?
   - ❍ **A.** Implement a new, more robust password policy that requires complex passwords.
   - ❍ **B.** Start a training and awareness program.
   - ❍ **C.** Increase the organization’s email-filtering ability.
   - ❍ **D.** Develop a policy that restricts email to official use only.

4. You have been asked to manually review audit logs to detect malicious activity. Which statement is correct?
   - ❍ **A.** The audit logs are a compensating control for the detection of malicious activity.
   - ❍ **B.** The manual review is a compensating control for the audit logs.
   - ❍ **C.** The manual review is a technical control that supplements automated processes.
   - ❍ **D.** The audit logs, when combined with review processes, are a detective control.

5. Which of the following groups presents the largest threat to an organization?

❍ **A.** Insiders

❍ **B.** Corporate spies

❍ **C.** Government spies

❍ **D.** Script kiddies

6. Which of the following documents would you reference to determine the frequency for monitoring a control when implementing an information security continuous monitoring system?

❍ **A.** ITIL

❍ **B.** NIST 800-137

❍ **C.** NIST 800-92

❍ **D.** NIST 800-115

7. Which type of SOC report is typically shared with the general public?

❍ **A.** SOC 2

❍ **B.** SOC 1

❍ **C.** SOC 4

❍ **D.** SOC 3

8. Which of the following individuals in an organization can declare a disaster?

❍ **A.** Owner/CEO

❍ **B.** Disaster recovery and business continuity planning personnel

❍ **C.** Anyone

❍ **D.** Business continuity planning coordinator

9. Which of the following is the best solution for a graceful shutdown during a disaster?

❍ **A.** Generator

❍ **B.** UPS

❍ **C.** Redundant power supply

❍ **D.** Dual power feeds

10. In which of the following ways are ethical hackers different from threat actors?

❍ **A.** They have permission to destroy a network.

❍ **B.** Their goal is to do no harm.

❍ **C.** They cannot be held liable for any damage.

❍ **D.** They cannot be prosecuted or jailed for their actions.

11. Which of the following describes actions run against a monitored system to see how it responds?

❍ **A.** Fagan inspection

❍ **B.** Static code testing

❍ **C.** Synthetic transactions

❍ **D.** Fuzzing

12. Which of the following best describes SATAN?

❍ **A.** It is used for password cracking.

❍ **B.** It is used for reviewing audit logs.

❍ **C.** It is used to exploit systems.

❍ **D.** It is used to find vulnerabilities.

13. Which of the following is a powerful way to test how an application reacts to various inputs?

❍ **A.** Synthetic transactions

❍ **B.** Fuzzing

❍ **C.** Dynamic code analysis

❍ **D.** Static code analysis

14. What type of penetration test examines what insiders can access?

❍ **A.** Whitebox

❍ **B.** Graybox

❍ **C.** Blackbox

❍ **D.** Bluebox

15. Which of the following individuals are known for their attacks on analog phone and telecommunication systems?

❍ **A.** Script kiddies

❍ **B.** Phreakers

❍ **C.** Crackers

❍ **D.** Hackers

Answers to Exam Prep Questions

1. **C.** IP spoofing is a common practice when DoS tools are used to help an attacker mask his identity. Salami attacks, data diddling, and keystroke logging do not typically spoof IP addresses, so answers A, B, and D are incorrect.
2. **C.** This more advanced spoofing attack works by subverting the TCP connection between a client and a server. If it is successful, the attacker has a valid connection to the victim's network and is authenticated with his credentials. This type of attack is very hard to do with modern operating systems but is trivial with older operating systems. Answer A is incorrect because session hijacking does not involve DNS; it functions by manipulating the TCP sequence number. Answer B is incorrect because session hijacking does not use UDP; UDP is used for stateless connections. Answer D is incorrect because, again, session hijacking is not based on DNS and UDP. These two technologies are unrelated to TCP sequence numbers.
3. **B.** The best defense against social engineering is to educate users and staff. Training can go a long way toward teaching employees how to spot scams. Although the other answers are not bad ideas, they will not prevent social engineering, so answers A, C, and D are incorrect.
4. **D.** Audits are a detective control. Answers A, B, and C are incorrect because they are not detective or compensating controls.
5. **A.** Insiders are the biggest threat to an organization because they possess two of the three things needed to attempt malicious activity: means and opportunity. Answers B, C, and D are incorrect because although outsiders might have a motive, they typically lack the means or opportunity to attack an organization.
6. **B.** NIST 800-137 defines ISCM. Answers A, C, and D are incorrect. NIST 800-92 addresses log management, NIST 800-115 deals with penetration testing, and ITIL is a framework of best practices for delivery of IT services.
7. **D.** SOC 3 for Service Organizations reports are general use reports that can be freely distributed. Answers A, B, and C are incorrect because SOC 1 reports are for evaluating the effect of controls at the service organization on users' financial statements. SOC 2 reports provide detailed information about how a service organization handles users' data and the confidentiality and privacy of the information processed by these systems. There is no SOC 4 designation.
8. **D.** While anyone can declare an emergency, only a business continuity planning coordinator can declare a disaster. Therefore, answers, A, B, and C are incorrect.
9. **B.** A UPS is best option for a graceful shutdown. Answer A is incorrect because a generator is for long-term recovery. Answers C and D are incorrect because redundant power supplies and dual power feeds are not short-term solutions.
10. **B.** Ethical hackers use the same methods as crackers and black hat hackers, but they report the problems they find instead of taking advantage of them. Ethical hacking has other names, such as *penetration testing*, *intrusion testing*, and *red-teaming*. Answer A is incorrect because ethical hackers do not have

permission to destroy networks. Answer C is incorrect because ethical hackers can be held liable. Answer D is incorrect because ethical hackers can be jailed if they break the law or exceed the terms of their contract.

11. **C.** Synthetic reactions are run against a monitored system to see how it responds. Answer A is incorrect because Fagen inspections are carried out during code development. Answer B is incorrect because static code analysis is a type of manual review. Answer D is incorrect because fuzzing uses random variables as inputs to evaluate the output.
12. **D.** SATAN, the first vulnerability assessment program, was designed to find vulnerabilities in a network. Programs like Retina and Nessus are also used for vulnerability assessment. SATAN is not used for password cracking (answer A) or auditing logs (answer B), and it is not used to exploit systems (answer C).
13. **B.** There are two types of fuzzing: generation based and mutation based. Answer A is not correct because synthetic transactions are real-time transactions that are performed on monitored objects. Answer C is incorrect because dynamic code analysis is designed to test a running application for potentially exploitable vulnerabilities. Answer D is incorrect because static code analysis is a method of debugging that involves examining source code before a program is run.
14. **B.** Graybox testing aims to determine what type of activities can be performed. Answer A is incorrect because with whitebox testing, everything is known about the network. Answer C is incorrect because with blackbox testing, nothing is known about the network. Answer D is incorrect because blueboxing is a term used by phreakers to make free phone calls via a mechanical device.
15. **B.** Phreakers are individuals who are known for their attacks on analog phone and telecommunications equipment. Answers C and D are incorrect because hackers and crackers are both types of computer criminals. Answer A is incorrect because script kiddies are junior hackers who rely on using others' processes and programs to attack computers.

Need to Know More?

RFC 1087: www.faqs.org/rfcs/rfc1087.html

NIST 800-137: https://csrc.nist.gov/publications/detail/sp/800-137/final

COBIT versus ISO 27001: https://advisera.com/27001academy/blog/2019/05/06/cobit-vs-iso-27001-how-much-do-they-differ/

DOJ site on cybercrime: www.cybercrime.gov

Fagan inspection: http://www.osel.co.uk/presentations/fitsbnwtf.pdf

Log management (NIST 800-92): https://csrc.nist.gov/publications/detail/sp/800-92/final

Synthetic transactions: www.logicmonitor.com/blog/an-introduction-to-executing-synthetic-transactions-with-logicmonitor/

Misuse case testing: https://sqa.stackexchange.com/questions/1804/abuse-cases-and-misuse-cases

Detecting vulnerabilities with SCAP and OVAL: https://www.integrigy.com/security-resources/stigs-scap-oval-oracle-databases-and-erp-security

EU privacy laws: en.wikipedia.org/wiki/Data_Protection_Directive

Generation and mutation fuzzing: www.f-secure.com/us-en/consulting/our-thinking/15-minute-guide-to-fuzzing

Federal rules of evidence: www.law.cornell.edu/rules/fre/

CVEs and CVSS defined: www.imperva.com/learn/application-security/cve-cvss-vulnerability/

Passive vulnerability monitoring: www.honeynet.org

Hearsay defined: https://en.wikipedia.org/wiki/Hearsay

Best practices for log review: www.computerweekly.com/tip/Best-practices-for-audit-log-review-for-IT-security-investigations

CHAPTER 8
Security Operations

Terms you'll need to understand:

- Redundant array of inexpensive disks (RAID)
- Clustering
- Distributed computing
- Cloud computing
- Media management
- Least privilege
- Mandatory vacations
- Due care
- Due diligence
- Privileged entities
- Clipping level
- Resource protection

Topics you'll need to master:

- Disaster recovery processes and plans
- How to understand and support investigations
- Foundational security concepts
- Different types of RAID
- How to implement disaster recovery strategies and recovery strategies
- How to participate in business continuity planning and exercises
- Perimeter and internal physical controls
- How to implement disaster recovery processes
- Auditing and monitoring

Introduction

When preparing for the (ISC)^2 CISSP exam or reviewing the Security Operations domain, you need to understand what resources should be protected and be familiar with principles of best practices; methods to restrict access, protect resources, and monitor activity; and how to respond to incidents.

The Security Operations domain covers a wide range of topics involving operational security best practices. Security professionals apply operational controls to daily activities to keep systems running smoothly and facilities secure. This chapter reviews those controls and shows how their application to day-to-day activities can prevent or mitigate attacks.

The process starts before an employee is hired. Employers should perform background checks, reference checks, criminal history reports, and educational verification. Among many other onboarding tasks, a new employee must be trained on corporate policies.

Controls need to be put in place to limit the ability and access an employee has. Access is a major control that should be limited to just what is needed to complete required tasks; this limit is referred to as *least privilege*. Job rotation, dual control, and mandatory vacations are also several examples of these types of controls.

Controls are not just about people. Controls are also needed to deal with system failure. Disaster recovery and business continuity planning and exercises are key controls in this area.

Many of the controls discussed in this chapter are technical in nature. These controls include intrusion prevention, network access control, anti-malware, RAID and security information, and event management. Each of these controls is used in a unique way to prevent, detect, and recover from security incidents and exposures. Keep in mind that violations to operational security aren't always malicious; sometimes things break or accidents happen. Operational security must be prepared to deal with such unintended occurrences by building in system resilience and fault tolerance.

Foundational Security Operations Concepts

Ask any seasoned security professional what it takes to secure its networks, systems, applications, and data, and the answer will most likely involve a combination of operational, technical, and physical controls. This process starts before you ever hire your first employee. Employees need to know what is expected of them. Accounts need to be configured, users need to have the appropriate level of access approved, and monitoring must be implemented. The following sections discuss these topics.

Managing Users and Accounts

One foundational way to increase accountability is to enforce specific roles and responsibilities in an organization. Most organizations have clearly defined controls that specify what each job role is responsible for. The following are some common roles in organizations:

- **Systems administrator**: This role is responsible for the operation and maintenance of the LAN and associated components, such as Windows Server 2019, Linux, and possibly mainframes. A small organization might have only one systems administrator, and a larger one might have many.
- **Quality assurance specialist**: This role can focus on either quality assurance or quality control. Quality assurance employees make sure programs and documentation adhere to standards; quality control employees perform tests at various stages of product development to make sure the products are free of defects.
- **Database administrator**: This role is responsible for the organization's data and maintains the data structure. The database administrator has control over all the data; therefore, detective controls and supervision of duties must be closely observed. This role is usually filled by a senior information systems employee because these employees have control over the physical data database, implementation of data definition controls, and definition and initiation of backup and recovery.
- **Systems analyst**: This role is involved in the software development lifecycle (SDLC) process and is responsible for determining the needs of users and developing the requirements and specifications for the design of needed software.
- **Network administrator**: This role is responsible for maintenance and configuration of network equipment, such as routers, switches, firewalls, wireless access points, and so on.
- **Security architect**: This role is responsible for examining the security infrastructure of the organization's network.

Job titles can be confusing because different organizations tend to use different titles for identical positions. In addition, smaller organizations tend to combine duties under one position or title. For example, some network architects are called network *engineers*. The critical concept for a security professional is to understand that, to avoid conflicts of interest, certain roles should not be combined. Table 8.1 lists some examples of role combinations and whether it's okay to combine them.

TABLE 8.1 **Separation of Duties**

First Job Role	Can Be Combined With?	Second Job Role
Systems analyst	No	Security administrator
Application programmer	Yes	Systems analyst
Help desk	No	Network administrator
Data entry	Yes	Quality assurance
Computer operator	No	Systems programmer
Database administrator	Yes	Systems analyst
Systems administrator	No	Database administrator
Security administrator	No	Application programmer
Systems programmer	No	Security administrator

The titles and descriptions in Table 8.1 are just examples, and many organizations might describe them differently or assign more or less responsibility to particular job roles. To better understand the effect of role combinations that can conflict, consider a small company that employs one person as both the network administrator and the security administrator. This represents a real weakness because of the conflict of interest in the range of duties that a security administrator and a network administrator must perform: Whereas a network administrator is tasked with keeping the system up and running and keeping services available, a security administrator is tasked with turning services off, blocking them, and denying user access. A security professional should be aware of such incompatibilities and be concerned about the risks that can arise when certain roles are combined. Finally, any employee of the organization who has elevated access requires careful supervision. Such individuals should be considered privileged entities.

Privileged Entities

A *privileged entity* is anyone who has a higher level of access than a typical user. Privileged entities can include mainframe operators, security administrators, network administrators, power users, and anyone with higher-than-typical levels of access. It important that sufficient controls be placed on these entities so that misuse of their access is deterred or, if their access is misused, it can be detected and corrected.

Controlling Access

Before hiring employees, you must make sure that you have the right person for the right job. Items such as background checks, reference checks, education/certification checks, and Internet or social media checks might be run before new-hire orientation ever occurs. New employees might be asked to sign *nondisclosure agreements* (*NDAs*), agree to good security practices, and agree to *acceptable use policies* (*AUPs*).

When employees are onboarded, a number of controls can be used to control access and privilege. First, s*eparation of duties* describes the process of dividing duties so that more than one person is required to complete a particular task. *Job rotation* can be used to maintain redundancy, back up key personnel, and help identify fraudulent activities. The *principle of least privilege* is another important concept that can help an organization achieve its operational security goals. According to this principle, individuals should have only enough resources to accomplish their required tasks.

Controls such as mandatory vacations provide time for audits and for examining user activity for illicit activities. Controls need to be backed up by policies, procedures, and training. Keep in mind that organizations benefit when each employee actively participates in the security of the organization.

Clipping Levels

No one has the time to investigate every event or anomaly that occurs, but an organization must have systems in place to log and monitor activities. An organization can set a *clipping level* to identify an acceptable threshold for the normal mistakes a user might commit. Then, events that occur with a frequency in excess of the clipping level can trigger administrative notification and investigation.

A clipping level allows users to occasionally make mistakes, but if the established level is exceeded, violations are recorded or some type of response occurs. A network administrator might, for example, allow users to attempt to log in three times. If a user can't get the password right by the third try, the account is locked, and the user is forced to call the help desk for support. If an administrator or a help desk staffer is contacted to reset a password, a second type of authentication should be required to protect against social engineering attacks. Chapter 7, "Security Assessment and Testing," covers social engineering in detail.

Tip

To prevent social engineering attacks, when individuals need to have their passwords reset by automated means, they should be required to authenticate by providing information such as user ID, PIN, or two or more cognitive passwords. For systems with higher security, physical retrieval or in-person verification should be required for password recovery.

Resource Protection

When you think of resource protection, you might think of servers or other tangible assets. But resources can be both tangible and intangible. Tangible assets include equipment and buildings, and intangible assets can include such things as patents, trademarks, copyrights, and brand recognition. Loss of a trade secret to a competitor can be just as devastating as employee theft of a laptop. An organization must take reasonable care to protect all items of value.

Due Care and Due Diligence

Due care is focused on taking reasonable ongoing care to protect the assets of an organization. *Due diligence* is the background research. For example, before accepting credit cards, you might want to research the laws that govern their use, storage, and handling. In this case, due diligence would be associated with reviewing the controls highlighted in PCI-DSS.

Note

Due diligence was first used as a result of the U.S. Securities Act of 1933.

Organizations and their senior management are increasingly being held to higher levels of due care and due diligence. Depending on the law, senior management who are found negligent can be held responsible for criminal and/or financial damages. The Sarbanes-Oxley Act of 2002 and the Federal Information Security Modernization Act have increased an organization's liability for maintaining industry compliance. For example, U.S. federal sentencing guidelines allow for fines in excess of $200 million.

When an organization's due diligence is challenged, the court system looks at what a "prudent person" would have done; this is referred to as the *reasonably prudent person rule*. For example, a prudent person would implement PCI-DSS controls for credit card transactions for a retail store using a point of sale (POS) device with more than 80,000 transactions a year. The reasonably prudent person is a legal abstraction; in the context of cybersecurity, it would be a professional, well trained, certified, educated individual with common sense in cyberdefense.

Note

While PCI is a major standard for control of financial information, the Group of Eight (G8) started as a forum for the governments of eight of the world's largest economies to discuss issues related to commerce. Today, it has grown to 20 members.

Asset Management

Asset management is the process of identifying all the hardware and software assets in an organization, including the organization's employees. There is no way to assess risk or to consider what proper operational controls are without good asset management. Asset management not only helps an organization gain control of its software and hardware assets but also increases the organization's accountability. Consider the process of hardening, patching, and updating. This process cannot be effectively managed without knowing what operating systems and/or software an organization owns and on what systems those products are installed.

System Hardening

Once we know what assets we have, *system hardening* is used to eliminate all applications, processes, and services that are not required for the business to function. When attackers attempt to gain access to a system, they typically look for systems that are highly vulnerable or where there is "low-hanging fruit." This phrase describes services and applications that are easily exploitable, often because they are unnecessary and unmanaged. The purpose of system hardening is to reduce the attack surface by removing anything that is not needed or at least to isolate vulnerable services away from sensitive systems. After a system has been reduced to its bare essentials, there are fewer avenues for a potential attacker to exploit.

Hardening should also be considered from a hardware perspective. Hardware components such as DVD drives and USB ports should be disabled or removed. Also, hardening can be extended to the physical premises. Wiring closets should be locked, data centers should permit limited access, and network equipment such as switches, routers, and wireless access points should be physically secured.

> **Note**
>
> After performing many security assessments, one of the first things I now look for when I enter a facility is a lack of physical controls on assets such as wireless access points, telecommunication equipment, servers, and riser rooms. If an asset is physically accessible to an intruder, it is insecure.

Once a system has been hardened and approved for release, a baseline needs to be approved. *Baselining* is simply capturing a configuration or an image at a point in time and understanding the current system security configuration.

All your work up to this point would do little good if the systems were not maintained in a secure state. This is where change management comes into play.

Change and Configuration Management

Organizations put a lot of effort into securing assets and hardening systems. To manage required system changes, controls must be put in place to make sure all changes are documented and approved. This is accomplished through the *change management* process. Any time a change is to be made, it is important to verify what is being requested, how it will affect the systems, and what unexpected actions might occur. Most organizations do not directly deploy a patch without first testing it to see what changes will occur after the patch has been installed. It is important to ensure that changes do not somehow diminish or reduce the security of a system. Configuration management should also provide a means to roll back or undo any applied changes in the event that negative effects occur because of the change. Although change management processes can be implemented slightly differently in various organizations, the following is a generic process:

1. Request a change.
2. Approve the change.
3. Catalog the change.

4. Schedule the change.
5. Prepare a means to roll back the change, if needed.
6. Implement the change.
7. Test or confirm the change.
8. Report the completion of the change to the appropriate individuals/groups.

> **Tip**
>
> While some might question the need to have a rollback plan, things can go wrong. For example, in December 2020, Microsoft's Windows 10 update conflicted with CORSAIR Utility Engine software and caused Windows to crash.

Despite the fact that different organizations might implement change management in different ways, there can be no argument over the value of using comprehensive change management. The primary benefits of change management include the following:

- Verification that change is implemented in an orderly manner through formalized testing
- Verification that the user base is informed of impending/completed changes
- Review of the effects of changes on the system after implementation to create lessons learned for the next change
- Mitigation of any adverse impact that changes might have had on services, systems, or resources

Change management can also be used to demonstrate due care and due diligence.

Trusted Recovery

Any failure that endangers the security of a system must be understood and investigated. It is critical that an organization's environment be protected during recovery. Consider a server running Windows 2019 Server. Have you ever noticed that when you shut down such a server, you are asked why you are shutting it down? The screen that asks this question is an example of an operational control.

To protect the environment during the reboot/restart process, access to the server must be limited. You want to prevent opportunities for people to disrupt the process.

Some examples of recovery limits include the following:

- Preventing a system from being booted from the network, DVD, or USB
- Logging restarts so that auditing can be performed
- Blocking complementary metal-oxide semiconductor (CMOS) changes to prevent tampering
- Denying forced shutdowns

Remote Access

As transportation, utilities, and other associated costs associated with traditional 9-to-5 employees and global changes like the COVID-19 pandemic alter the way business is conducted, organizations are increasingly permitting employees to telecommute, access resources remotely, and use cloud computing. Organizations are therefore being required to enable remote access to their networks. However, remote access offers attackers a potential means of gaining access to the protected network. Therefore, organizations need to implement good remote access practices to mitigate risk. Some basic remote access controls include the following:

- Implementing caller ID
- Using a callback system
- Disabling unused authentication protocols
- Using strong authentication, including MFA
- Implementing remote and centralized logging
- Using VPNs and encryption

Media Management, Retention, and Destruction

Resource protection techniques go beyond when the resource is being used and also include disposal. If data is held on hard drives, magnetic media, or thumb drives, those devices must eventually be sanitized. *Sanitization* is the process of clearing all identified content such that no data remnants can be recovered. When sanitization is performed, none of the original information can be recovered. The following are some of the methods used for sanitization:

- **Drive wiping**: This method involves overwriting all information on a drive. It allows the drive to be reused.
- **Zeroization**: This involves overwriting the data with zeros. Zeroization is defined in ANSI X9.17.
- **Degaussing**: This method is used to permanently destroy the contents of a hard drive or magnetic media. With degaussing, a powerful magnet is used to penetrate the media and polarize the magnetic particles on the tape or hard disk platters. Degaussed media cannot be reused.
- **Physical destruction**: This may be required to sanitize newer solid-state drives.

Telecommunication Controls

Guglielmo Marconi probably had no idea that his contributions to the field of radio would lead to all the telecommunications systems available today. A security professional is not going to be tasked with building the first ship-to-shore radio system, like Marconi did, but she must be aware of current telecommunication systems and understand their usage and potential vulnerabilities. Concepts related to these systems that you must be aware of include cloud computing, email systems, fax machines, public branch exchanges (PBXs), whitelisting, sandboxing, and anti-malware.

Cloud Computing

Cloud computing refers to using Internet-based systems to perform on-demand computing. Users only have to pay for the services and computing resources they require and can increase usage when more computing resources are needed or reduce usage when the services are not needed. The following are some of the most common cloud computing models:

- **Monitoring-as-a-service (MaaS)**: MaaS allows IT and other organizations to remotely monitor and manage networks, applications, and services.
- **Communication-as-a-service (CaaS)**: With CaaS, the service provider seamlessly integrates multiple communication devices or channels for voice, video, IM, and email as a single solution.

- **Infrastructure-as-a-service (IaaS)**: IaaS enables organizations to rent storage and computing resources, such as servers, networking technology storage, and data center space.
- **Platform-as-a-service (PaaS)**: PaaS provides access to platforms that let organizations develop, test, and deploy applications. It is a cloud computing service delivery model that delivers a set of software. In PaaS, the user's application resides entirely on the cloud, from development to delivery.
- **Software-as-a-service (SaaS)**: SaaS enables an organization to use applications that are running in the service provider's environment. It is a cloud service model that delivers prebuilt applications over the Internet on an on-demand basis. SaaS can use a multi-tenant architecture to deliver a single application to multiple customers within an organization.

Cloud computing models generally fall into the following categories:

- **Private**: The entire cloud and all its components are managed by a single organization.
- **Community**: Cloud components are shared by multiple organizations and managed by one of them or by a third party.
- **Public**: The cloud is open for any organization or user to use, is public, and is managed by a third-party provider.
- **Hybrid**: This service model has components of more than one of the private, community, and public service models.

ExamAlert

For the CISSP exam, you need to know not just cloud computing models like SaaS and MaaS but also the categories private, community, public, and hybrid.

Email

Email enables individuals to communicate electronically over the Internet or a data communications network. Email is the most commonly used Internet application. Email is subject to some security concerns. Email was designed in a different era and, by default, sends information in plaintext. Anyone who is able to sniff plaintext traffic can read it. Email can be easily spoofed so that the true identity of the sender is masked. Email is also a major conduit for spam, phishing, and viruses.

Email functions by means of several underlying services, including the following:

- **Simple Mail Transfer Protocol (SMTP)**: SMTP is used to send mail and to relay mail to other SMTP mail servers. SMTP uses TCP port 25. A message sent through SMTP has two parts: an address header and message text. All types of computers can exchange messages by using SMTP.
- **Post Office Protocol (POP)**: POP is currently at version 3 (POP3) and is one of the protocols that can be used to retrieve messages from a mail server. POP3 performs authentication in plaintext on TCP port 110. An alternative to POP3 is IMAP.
- **Internet Message Access Protocol (IMAP)**: IMAP, which is used as a replacement for POP, operates on TCP port 143 and is designed to retrieve messages from an SMTP server. IMAP4, which is the current version, offers several advantages over POP. IMAP makes it possible to work with email remotely. Many of today's email users need to access email from different locations and devices, such as smartphones, laptops, and desktops. IMAP makes it possible for multiple clients to access the email server and leave the email there until it's deleted.

Tip

An updated version of POP that provides authentication is known as Authenticated Post Office Protocol (APOP).

With basic email operation, SMTP is used to send messages to the email server. To retrieve email, a client application, such as Outlook, might use POP or IMAP, as illustrated in Figure 8.1.

Anyone who uses email needs to be aware of the security risks. Spam is an ongoing problem, and techniques like graylisting can be used to deal with it. The sending of sensitive information in plaintext is another area of concern. If an organization has policies that allow email to be used for sensitive information, encryption should be mandatory. An organization needs to evaluate its needs related to email. Several solutions can make email more secure, including Pretty Good Privacy (PGP) and link encryption or secure email standards, such as Secure Multipurpose Internet Mail Extensions (S/MIME) and Privacy Enhanced Mail (PEM).

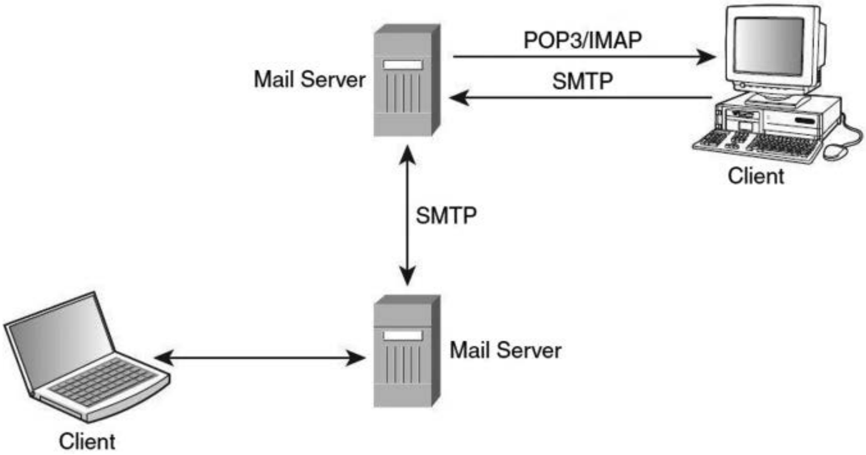


FIGURE 8.1 **Email Configuration**

Whitelisting, Blacklisting, and Graylisting

Whitelisting, blacklisting, and graylisting are technical controls.

A whitelist is used to determine what is allowed access or what can be performed. Anything that is not included on the whitelist is prohibited.

Blacklists operate in the opposite way, banning or denying particular users, types of access, or resources. The problem with blacklisting is that as the list continues to grow, it requires more ongoing maintenance and oversight.

Many email administrators use graylists to deal with spam. A graylist rejects any email sender that is unknown. Mail that is from a legitimate email server is retransmitted after a period of time, and the graylisted email is moved off the graylist and onto the whitelist, at which point it is delivered to the inbox of the receiving account. Email is not necessarily blacklisted or deleted until the user evaluates the decision and makes a human decision to reject or accept the sender.

A related technique is *sandboxing*. A sandbox is often used when untested code or untrusted programs from third-party sources are being used.

ExamAlert

For the CISSP exam, you should understand blacklists, graylists, and whitelists.

Firewalls

The CISSP exam might test you on the advantages and disadvantages of different types of firewalls and their design. A packet filter, which is the most basic form of firewall, operates at the network layer of the OSI model. This type of firewall filters traffic by using an access control list (ACL). The ACL determines what packets can be accepted and what packets should be denied access.

Another type of firewall, a proxy firewall, can be an application-level proxy, a circuit-level proxy, or a kernel-level proxy. A kernel-level proxy is the most advanced and operates at the application layer of the OSI model. A kernel-level proxy firewall works faster than all the application-level firewalls because activity is centered in the kernel. When a packet ingresses a kernel proxy firewall, a new virtual stack is created that has only the protocol proxies needed to examine that specific packet.

Firewalls can be designed in three main ways:

- **Single-homed**: With a single-homed firewall, one packet-filtering router is installed between the trusted and untrusted networks (which are usually the Internet and the organization's network).
- **Dual-homed**: A dual-homed gateway offers an improvement over a basic packet-filtering router because it comprises a bastion host that has two network interfaces. One important factor with a dual-homed gateway is that IP forwarding is disabled on the host. Additional protection can be provided by adding a packet-filtering router in front of a dual-homed host.
- **Demilitarized (DMZ)**: A DMZ (or screened subnet) is a subnet that is in between firewalls or off one leg of a firewall (see Figure 8.2). Because the DMZ sits in between the public Internet and private networks, it keeps the internal, private network isolated from the external network and provides an area of middle ground where you can host web, mail, and authentication servers.

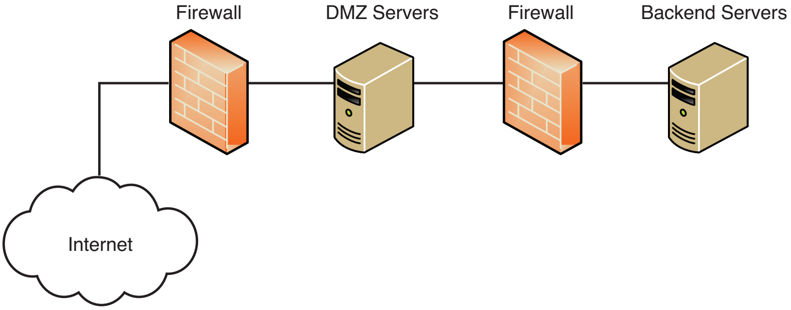


FIGURE 8.2 **Screened Host**

Phone, Fax, and PBX

Three techniques attackers can use to target phone users are *phone hijacking*, *slamming*, and *cramming*. Phone hijacking occurs when hackers use personal information to deceive a phone company's customer service representatives into transferring your phone number to them. Slamming refers to switching users' long-distance phone carriers without their knowledge. Cramming relates to unauthorized phone charges. One cramming technique is to send a fake SMS message that, when clicked on, authorizes the attacker to bill the victim a small amount each month.

Fax machines can present some security problems if they are being used to transmit sensitive information. Fax systems can be secured by using fax servers, encryption, and activity logs.

Caution

Although fax servers have solved many security problems, they have their own challenges. Many of them use hard drives where organizations store large numbers of commonly used administrative documents and forms. Others allow HTTP and/or FTP access to the print queue, where someone can capture the files. These issues must be addressed before effective security can be achieved.

Private organizations use PBX systems, which permit users to connect to a public switched telephone network (PSTN). A PBX can be used to assign extensions, provide voicemail, and enable special services for internal users and customers. Like other organizational resources, a PBX can be a potential target. If hacked, the PBX can be used to allow callers to call out and make free long-distance phone calls that are charged to the organization. PBX hacking is not as prevalent today as it was in the past, but a PBX can still pose a threat to operational security. Individuals who target PBX and phone systems are known as *phreakers*. *Phreaking* is the art of hacking phone systems. Although this might sound like a rather complicated affair, back in the early 1970s, it was discovered that free phone calls could be made by playing a 2600 Hz tone into a phone. This tone allowed the phreaker to bypass the normal billing process. The first device tailored to this purpose was known as a *blue box*. These boxes were invented in the 1970s and used until the early 1990s.

Although these tools are primarily historical, phreakers can still carry out activities like caller ID spoofing, SIM swapping attacks and they might even target VoIP phone systems for DoS attacks or sniffing attacks.

Anti-malware

Malware is a problem that computer users are faced with daily. Training users in safe computing practices is a good start, but anti-malware tools are still needed to protect an organization's computers. When you find suspected malware, there are generally two ways to examine it: using static analysis or active analysis. Whereas static analysis requires you to decompile or disassemble the code, active analysis requires the suspected malware to be executed. Because executing malware on a live production environment can be dangerous, it is typically done on a standalone system or virtual machine referred to as a *sandbox*. The sandbox allows you to safely view or execute the suspected malware or any untrusted code while keeping it contained.

> **Caution**
>
> Keep in mind that even when malware is run in a sandbox, there is always some possibility that it may escape and infect other systems.

Anti-malware is software that helps you prevent malware from executing on your systems. Anti-malware software should be installed on servers, workstations, and even portable devices. It can use one or more techniques to check files and applications for viruses and other types of common malware. These techniques include the following:

- **Signature scanning**: In a similar fashion to intrusion detection system (IDS) pattern-matching systems, signature scanning looks at the beginning and end of an executable file for known virus signatures. Virus creators attempt to circumvent the signature scanning process by making viruses polymorphic.
- **Heuristic scanning**: Heuristic scanning examines computer files for irregular or unusual instructions. For example, think of your word processing program. It probably creates, opens, and updates text files.
- **Integrity checking**: An integrity checker works by building a database of checksums or hashed values. Periodically, new scans are performed, and the results are compared to the stored results. Although integrity checking is not always effective for data files, this technique is useful for executables because their contents rarely change. For example, the md5sum hashed value of the Linux bootable OS Kali Linux is a66bf35409f4458ee7f35a77891951eb. Any change to the Kali.iso would result in a change in the hashed value, and an integrity checker would easily detect the change.

- **Activity blockers**: An activity blocker intercepts a virus when it starts to execute and blocks it from infecting other programs or data. Activity blockers are usually designed to start at bootup and continue until the computer shuts down.

Honeypots and Honeynets

Honeypots and honeynets are much like IDSs in that they are tools for detecting intrusion attempts.

A *honeypot* is really a tool of deception. Its purpose is to fool an intruder into believing that the honeypot is a vulnerable computer. Honeypots are used for diversion and analysis of an attacker's tactics, tools, and methods. Honeypots are simply fake systems or networks. Honeypots contain files, services, and databases that have no real value to an organization if compromised but are generally attractive to a hacker. Honeypots are effective because they can appear attractive without putting sensitive information at risk. To be effective, a honeypot must adequately persuade hackers that they have discovered a real system.

Some honeypot vendors sell products that can simulate an entire network, including routers and hosts, that are actually located on a single workstation; these are called *honeynets*. A honeynet can be deployed so that it is a separate server that is not being used in production.

Real servers can generate tons of traffic, which can make it hard to detect malicious activity. Because nothing is running on a honeypot or honeynet, any activity can easily be detected as a potential intrusion.

Honeypots can be configured for low interaction or high interaction. Low-interaction honeypots simulate only some parts of a service. For example, using a tool like `netcat` as a low-interaction honeypot, you can set a listener on a common port as shown here:

```
nc -v -n -l -p 80
```

This would show the port as open but would not return a banner.

In contrast, a high-interaction honeypot would show the port as open and could also return the proper banner, as shown here:

```
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Wed, 18 Jul 2012 18:08:25 GMT
Content-Type: text/html
Content-Length: 87
```

Honeypots can be configured in such a way that administrators will be alerted to their use so they have time to plan a defense for or guard the real network. However, honeypots do have downsides. Just like any other security system on a network, a honeypot requires time and configuration effort. In addition, a honeypot, by design, attracts a malicious element into your domain. Also, administrators must spend time monitoring these systems. Another downside is that, if an attacker can successfully compromise a honeypot, he now has a base of attack from which to launch further attacks.

Honeypots were originally designed for researching attack styles and designing improved architectures and anti-malware. More and more agencies are deploying honeypots to act as decoys, divert attackers from real systems, and provide early warning. It is important to understand that it is considered legal to entice someone, but it is not legal to entrap someone. The fuzzy distinction between enticement and entrapment can lead to interesting court cases.

Caution

A key issue with honeypots is to avoid entrapment, which is illegal. Using warning banners can help you avoid claims of entrapment by clearly noting that those who use or abuse the system will be monitored and potentially prosecuted.

Patch Management

Patch management is critical in helping to resolve software flaws and getting them updated in an expedient manner to reduce overall risk of system compromise. Patch management is key to keeping applications and operating systems secure. An organization should have a well-developed patch management testing and deployment system in place. The most recent security patches should be tested and installed on host systems as soon as possible. The only exception is when an immediate installation would interfere with business requirements.

Before a patch can be deployed, it must be verified. Typical forms of verification include digital signatures, digital certificates, and some checksums and integrity verification mechanisms. Verification is a critical step that must be performed before testing and deployment to make sure a patch has not been maliciously or accidentally altered. When testing is complete, deployment can begin. Change management protocols should be followed throughout this process.

System Resilience, Fault Tolerance, and Recovery Controls

Things will surely go wrong; it is just a matter of when. Understanding how to react and recover from errors and failures is an important part of operational security.

Good operational security practices require security planners to perform *contingency planning*, which involves developing plans and procedures that can be implemented when things go wrong. Contingency planning should occur after you've identified operational risks and performed a risk analysis to determine the extent of the impact of possible adverse events.

Recovery Controls

Recovery controls are controls that are applied after an adverse event occurs. They are administrative in nature and are useful for contingency planning and disaster recovery. Most of us do *contingency planning* in our personal lives. For example, while writing this book, I had a hard drive failure. I was lucky to have backed up the data, and I needed to find a way to finish the chapter and get it emailed by the deadline. My contingency plan was to use my laptop until I could get the desktop system back up and running. Most major organizations need much more detailed contingency plans than this.

The process of *recovery* requires having a mechanism to restore lost services after a disruptive event. To ensure that recovery goes smoothly, an organization must eliminate single points of failure and consider mean time between failures (MTBF) and mean time to repair (MTTR).

MTBF is the average time until something fails. Engineers often discuss MTBF in terms of the bathtub curve, which is illustrated in Figure 8.3. This graphic example of average time before failure looks at the average rate of failure of a population of devices. Some devices will fail early, but are engineered to operate until their designed end of service.

Devices that survive until their end of life will start to fail at an increasing rate as they wear out. Good operational control practices dictate that an organization should have some idea how long a device is calculated to last. This helps the organization plan for replacement before outages occur and services are disrupted.

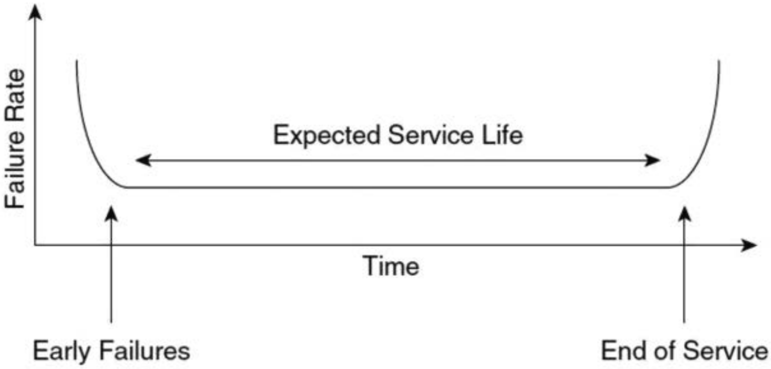


FIGURE 8.3 **MTBF and the Bathtub Curve**

For items that fail before the expected end of service, a second important variable is MTTR. The MTTR is the amount of time it will take to get the item back online. One of the major ways that organizations deal with such unknowns is to use service-level agreements (SLAs).

Monitoring and Auditing Controls

Computer resources are a limited commodity provided by an organization to help meet its overall goals.

Accountability must be maintained for network access, software usage, and data access. In a high-security environment, the level of accountability should be substantial, and users should be held responsible by logging and auditing their activities.

Good practice dictates that audit logs be transmitted to a remote centralized site. Centralized logging makes it easier for the person assigned the auditing task to review the data. Exporting the logs to a remote site also makes it harder for hackers to erase the logs and cover their activity. If there is a downside to all the logging that occurs, it is that all the information must be recorded and reviewed. A balance must be found between collecting audit data and maintaining a manageable log size. Reviewing logs can be expedited by using *audit reduction and correlation tools*, such as security information and event management (SIEM) tools. These tools parse the data and eliminate unneeded information. Another useful tool is a variance detection tool, which looks for trends that fall outside the realm of normal activity. For example, if an employee normally enters the building around 7 a.m. and leaves around 4 p.m. but is seen entering at 3 a.m., a variance detection tool would detect this abnormality.

Auditing and monitoring require *accountability* because if you don't have accountability, you cannot perform an effective audit. True security relies on the capability to verify that individual users perform specific actions. Without the capability to hold individuals accountable, organizations can't enforce security policies. Some of the primary ways to establish accountability are as follows:

- Auditing user activity
- Monitoring application controls
- Using SIEM tools
- Ensuring emanation security
- Implementing network access control
- Tracking the movement of individuals throughout the organization's physical premises

Auditing User Activity

Auditing produces audit trails, which can be used to re-create events and verify whether security policies have been violated. The biggest disadvantage of the audit process is that it is detective in nature, and audit trails are usually examined after an event. Some might think of audit trails as only corresponding to logical access, but auditing can also be applied to physical access. Audit tools can be used to monitor who entered a facility and what time certain areas were accessed. A security professional has plenty of tools available to help isolate activities of individual users.

Many organizations monitor network traffic to look for suspicious activity and anomalies. Some monitoring tools enable administrators to examine just packet headers, whereas others can capture all network traffic. Snort, Wireshark, and tcpdump are several such tools. Regardless of the tools used to capture and analyze traffic, administrators need to make sure that policies detail how such uncovered activities will be handled. Warning banners and AUPs go a long way toward making sure users are adequately informed of what to expect when using organization resources.

ExamAlert

For the CISSP exam, you should understand the importance of monitoring employees and keep in mind that tools that examine activity are detective in nature.

Tip

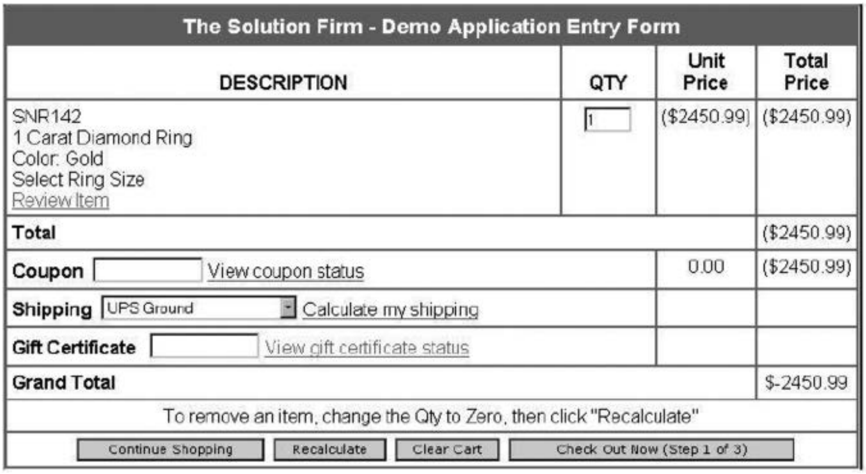
A *warning banner* is the verbiage a user sees at the point of entry into a system. Its purpose is to identify the expectations that users accessing those systems will be subjected to. These banners also aid in attempts to prosecute those who violate the AUPs. A sample AUP is shown here:

WARNING: Unauthorized access to this system is forbidden and will be prosecuted by law. By accessing this system, you agree that your actions may be monitored if unauthorized use is suspected.

Monitoring Application Transactions

Good security is about more than people. A big part of a security professional's day is spent monitoring controls to ensure that people are working according to policy. Much of today's computing activity occurs on servers that are connected to the Internet, and these systems must be monitored.

All input, processed, and output data should be monitored. Inputs must be validated. Consider the example of a dishonest individual browsing an e-commerce website and entering a quantity of –1 for an item that is worth $2,450.99. Hopefully, the application has been written in such a way as to not accept a negative quantity for any items advertised. Figure 8.4 shows an example of an application that lacks this control.



The Solution Firm - Demo Application Entry Form

DESCRIPTION	QTY	Unit Price	Total Price
SNR142 1 Carat Diamond Ring Color: Gold Select Ring Size Review Item	1	($2450.99)	($2450.99)
Total			($2450.99)
Coupon View coupon status		0.00	($2450.99)
Shipping UPS Ground Calculate my shipping			
Gift Certificate View gift certificate status			
Grand Total			$-2450.99

To remove an item, change the Qty to Zero, then click "Recalculate"

FIGURE 8.4 **Shopping Cart with Altered Values**

Note

One good example of an output control can be seen in many modern printer configurations. For example, some employee evaluation reviews might be configured so that they can be printed only to the supervisor's printer. Another example can be seen in products such as Adobe's Acrobat, which can limit printing of PDFs or embed password controls to limit who can open or edit PDFs.

Security Information and Event Management (SIEM)

Security information and event management (SIEM) is a relatively new set of tools and services that is used to collect and analyze auditable events. SIEM is the combination of the two separate services: security information management (SIM) and security event management (SEM). SIM is used to process and handle the long-term storage of audit and event data, whereas SEM is used for real-time reporting of events. Combining these two technologies provides users with the ability to alert, capture, aggregate, and review log information from many different systems and sources. Vendors that offer SIEM tools include Splunk, LogRhythm, and Sentinel.

SIEM allows for centralized logging and log analysis and can work with a variety of log data, such as NetFlow, sFlow, jFlow, and syslog. Most SIEM products support controls for confidentiality, integrity, and availability of log data. SIEM products provide four functions: aggregation, normalization, correlation, and reporting. SIEM can be used to detect misconfigured systems, unresponsive servers, malfunctioning controls, and failed applications. SIEM is typically used for ingress and egress monitoring:

- **Ingress**: The SIEM tools monitor data traffic that originates from outside the trusted network.
- **Egress**: The SIEM tools are used to monitor data that is leaving a trusted network.

While SIEM can be used to spot attacks and security incidents, it can also be used for the day-to-day operational concerns of a network. SIEM can also handle the storage of log data by disregarding data fields that are not significant to computer security, thereby reducing network bandwidth and data storage. Most SIEM products support two ways of collecting logs from log generators:

- **Agentless**: The SIEM server receives data from the hosts without needing to have any special software (agents) installed on those hosts.
- **Agent based**: An agent program is installed on the hosts and may be used to generate log input such as syslog and SNMP.

Although technologies such as SIEM are a great addition to a security professional's toolkit, keep in mind that you should strive for defense in depth. For example, SIEM is typically used with a variety of other technologies. Data loss prevention (DLP) solutions are often used to help protect sensitive data as it moves around the network and makes its way to endpoint devices. Identity and access management (IAM) solutions complement DLP by connecting disparate authentication services together; therefore, when users need to access systems or applications, they can make requests through a single service. Combining these technologies with a SIEM provides much greater protection than using any one technology by itself.

Network Access Control

Network access control (*NAC*), which has grown out of the trusted computing movement, has the goal of unified security. NAC offers administrators a way to verify that devices meet certain health standards before allowing them to connect to the network. Laptops, desktop computers, and other devices that don't comply with predefined requirements can be prevented from joining the network or can even be relegated to a controlled network where access is restricted until they are brought up to the required security standards.

Keystroke Monitoring

Keystroke monitoring, which can be accomplished with hardware or software devices, is used to monitor activity—for both legal and illegal purposes. As a compliance tool, a keystroke logger allows management to monitor a user's activity and verify compliance. The primary issue of concern is the user's expectation of privacy. Policies and procedures should be in place to inform the user that such technologies can be used to monitor compliance. The following is an example of an AUP that addresses keystroke monitoring:

> This acceptable use policy defines the boundaries of the acceptable use of this organization's systems and resources. Access to any organizational system or resources is a privilege that may be wholly or partially

> restricted without prior notice and without consent of the user. In cases of suspected violations or during the process of periodic review, employees can have activities monitored. Monitoring may involve a complete keystroke log of an entire session or sessions as needed to vary compliance with organizational policies and usage agreements.

Unfortunately, keystroke monitoring is not just for good guys. Hackers can use the same tools to monitor and record an individual's activities. Although an outsider to an organization might have some trouble getting one of these devices installed, an insider is in a prime position to plant a keystroke logger. Keystroke loggers can be hardware or software based.

Keystroke Logging and the Law

The U.S. Department of Justice has noted that administrators should protect themselves by giving notice to users if keystroke monitoring has been implemented. This notification can be by means of organizational policy or a warning banner. Administrators who fail to implement operational policies that specify how keystroke monitoring will be used could be subject to criminal and civil charges.

Emanation Security

The U.S. government was concerned enough about the possibility of emanations that the Department of Defense started a program to study them. Research actually began in the 1950s, based on the fear that attackers might try to sniff the stray electrical signals that emanate from electronic devices. TEMPEST technology resulted from this research. (Eavesdropping on the contents of a CRT by emanation leakage is referred to as *Van Eck phreaking*.) Devices that have been built to TEMPEST standards, such as cathode ray tube (CRT) monitors, have had TEMPEST-grade copper mesh, known as a *Faraday cage*, embedded in the case to prevent signal leakage. This costly technology is found only in very high-security environments.

TEMPEST is now considered somewhat dated; newer technologies such as white noise and control zones are now used to provide emanation security. White noise involves using special devices that send out streams of frequencies that make it impossible for an attacker to distinguish the real information. *Control zones* are facilities, walls, floors, and ceilings designed to block electrical signals from leaving the zones.

Perimeter Security Controls and Risks

Threats to physical security have existed for as long as humans have inhabited Earth. Consider the Incan city of Machu Picchu, built high on a mountain more than 7,000 feet above sea level. This ancient city was surrounded by thick stone walls and many natural exterior defenses that made it difficult to attack. Careful, ingenious planning is evident in the design of this city's defense.

In the modern world, multinational organizations might not be headquartered on remote mountain peaks, but security is still evident to deal with a variety of threats to physical security. These threats can be divided into broad categories, such as natural disasters, human-caused threats, and technical problems. The sections that follow delve into these threats in greater detail.

Natural Disasters

Natural disasters come in many forms. Although it is impossible to prevent natural disasters, it is possible to create a disaster recovery plan to mitigate the impact of such an event. You can create and implement a recovery and corrective plan for facilities, information, and information systems that could be affected; in it, you can detail how you will respond when confronted with disasters. For example, organizations planning to establish a facility in New Orleans, Louisiana, might have minimal earthquake concerns; however, hurricanes would be considered an imminent threat. Understanding a region and its associated weather-related issues is important in planning physical security.

Natural disasters that organizations should consider include the following:

- **Hurricanes, typhoons, and tropical cyclones**: These natural products of the tropical ocean and atmosphere are powered by heat from the sea. They grow in strength and velocity as they progress across the ocean and spawn tornadoes and cause high winds and floods when they come ashore.
- **Tidal waves/tsunamis**: The word *tsunami* is based on a Japanese word meaning "harbor wave." This natural phenomenon consists of a series of huge and widely dispersed waves that cause massive damage when they crash on shore.
- **Floods**: Floods can result when the soil has poor retention properties or when the amount of rainfall exceeds the ground's capability to absorb water. Floods are also caused when creeks and rivers overflow their banks.

- **Earthquakes**: Earthquakes occur because of movement of the earth along fault lines. For example, the Nepal earthquake of 2015 killed more than 8,000 people and injured more than 21,000. Some areas of the United States, such as California and Alaska, are especially vulnerable to earthquakes because they are on top of major active fault lines.
- **Tornadoes**: Tornadoes are storms that descend to the ground as violent rotating columns of air. A tornado leaves a path of destruction that may be quite narrow or extremely broad (up to about a mile wide).
- **Fire**: Fire, which can be caused by humans (intentionally or accidentally) or nature, is the most common cause of damage to property and loss of life. According to statistics at fema.gov, some 3,655 deaths were due to fire in the United States in 2018. That's a great loss of life. Wildfires can also cause massive damage.

Human-Caused Threats

Human-caused threats are a major concern when planning an organization's physical security. Whereas natural threats such as floods, hurricanes, and tornadoes cannot be prevented, human-caused threats can be mitigated by controls that minimize (or eliminate) opportunity of occurrence and provide for quick response in the event of any occurrence.

The following are examples of human-caused threats:

- **Terrorism**: As demonstrated in events such as the Sri Lanka terrorist suicide attacks in April 2019 that killed more 250 people, and as painfully understood by victims worldwide, terrorists act with calculated inhumane tactics to force their goals on society. Through risk analysis and threat modeling, organizations can determine what aspects of their businesses make them possible targets for terrorism (that is, "soft" targets). The answers could drive the need for physical security controls.
- **Vandalism**: Since the Vandals sacked Rome in 455 BCE, the term *vandalism* has been synonymous with the willful destruction of another's property.
- **Theft**: Theft of organizational assets can range from annoyance to legal liability. An organization's laptop, tablet, or smartphone can likely be replaced, but what about the data on the device?
- **Destruction**: Physical and logical assets are vulnerable to destruction by current employees, former employees, and/or outsiders. The Shamoon malware is believed to have destroyed 30,000 Saudi Aramco workstations in 2012.

- **Criminal activities**: This category is a catchall for other malicious behaviors that threaten an organization's employees or infrastructure.

Technical Problems

Unlike natural disasters or human-caused threats, technical problems are events that just seem to happen, often at highly inopportune times. These events can range from inconvenient glitches to potentially large-scale disasters.

Technical problems can include the following:

- **Communication loss**: Voice and data communication systems play a critical role in today's organizations. Communication loss can refer to outage of voice communication systems or data networks. As more organizations use convergence technologies such as network-controlled door locks, Internet Protocol (IP) video cameras, and VoIP (voice over IP), network failure means failure of data connection as well as voice communication.
- **Utility loss**: Utilities include water, gas, communication systems, and electrical power. The loss of utilities can bring business to a standstill. Generators and backups can be used to prevent these problems.
- **Equipment failure**: Equipment fails over time. This is why maintenance is so important. With insufficient planning, you might experience a business outage. A Fortune 1000 study found that 65% of all businesses that fail to resume operations within one week never recover at all and permanently cease operation.

> **Caution**
>
> Using service-level agreements (SLAs) is one good way to plan for equipment failure. In an SLA, a vendor agrees to repair or replace the covered equipment within a given time. Just keep in mind that while an SLA covers replacement of materials or repair time, it doesn't cover costs related to the downtime or loss of credibility.

Facility Concerns and Requirements

Whether you are charged with assessing an existing facility, moving into a new facility, or planning to construct a new facility, physical security must be a high priority. It's important to consider all the threats that have been discussed so far, as well as additional threats that might be unique to your operations. You don't want to build a facility in an area where your employees fear for their personal safety. You also don't want a facility to feel like a bank vault or be designed like a prison. You need a facility in which employees can be comfortable and productive, and where they can feel safe.

CPTED

A key component of achieving a balance between comfort and safety is Crime Prevention Through Environmental Design (CPTED). The benefits of CPTED include the following:

- Natural access control
- Natural surveillance
- Territorial reinforcement

CPTED is unique in that it considers the factors that facilitate crime and seeks to use proper facility design to reduce the fear and incidence of crime. At the core of CPTED is the belief that physical environments can be structured to reduce crime.

Let's look at a few examples of CPTED. Maybe you have noticed limited entrance and exit points into and out of mall parking lots. This is an example of *natural access control*. Or maybe you have seen an organization that has its employee parking lot in an area that is visible from the employee workspace. This enables employees to look out their windows in the office and see their parked cars. Even if this organization employs only a single guard, the facility's design allows increased surveillance by all the employees.

CPTED causes a criminal to feel an increase in the threat of being discovered and provides natural surveillance that can serve as a physical deterrent control. CPTED can also be applied to CCTV.

CCTV cameras should be mounted so that potential criminals can easily see the cameras and know they face a high risk of getting caught. A CCTV system can serve as a physical deterrent control and a detective control as well. Criminals may be deterred from entering property by the presence of a warning sign that alerts intruders that the property is under surveillance. Police can refer to video, along with log books and other technical logs, to make human judgments about who, how, when, and where a crime was committed; therefore, a CCTV system is a great physical detective control. CCTV is also a great tool for detecting and deterring insider threats.

Every facet of facility design should be reviewed with a focus on CPTED. Even items such as hedges are important in natural surveillance. They should not be higher than 2.5 feet as overgrown hedges obstruct visibility.

The third benefit of CPTED is territorial reinforcement. Walls, windows, fences, barriers, landscaping, and so on can be used strategically to define areas and create a sense of ownership with employees. It is typically best to use fences, lighting, sidewalks, and designated parking areas on the outside of a facility and move critical assets toward the center of the facility.

Area Concerns

Finding a good location is important when planning a new facility. Key points to consider include the following:

- **Accessibility**: An organization's facility needs to be in a location that people can access. Requirements will vary depending on business and individual needs, but aspects such as roads, freeways, local traffic patterns, public transportation, and convenience to regional airports need to be considered.
- **Climatology and natural disasters**: Mother Nature affects all of us. If you're building in Phoenix, Arizona, you will not have the same weather concerns as someone building a facility in Anchorage, Alaska. Events such as hurricanes, earthquakes, floods, snowstorms, dust storms, and tornadoes should be discussed and planned before starting construction.
- **Local considerations**: Issues such as freight lines, airline flight paths, toxic waste dumps, and insurance costs should be considered when determining where to build a facility. Although cheap land for a new facility might seem like a bargain, the discovery that it is next to a railway used to haul toxic chemicals could change your opinion.
- **Utilities**: You should check that water, gas, and electric lines are adequate for the organization's needs. This might seem like a nonissue, but California found out otherwise in the California energy crisis of 2019 and 2020, which left many without power and caused periods of rolling blackouts.
- **Visibility**: Area population, terrain, and types of neighbors are concerns. Depending on the type of business, you might want a facility that blends into the neighborhood. You might design individual buildings that cloak activities taking place there. Some organizations might even place an earthen dike or barrier around the facility grounds to obstruct the view of those who pass by.

Location

The location of a facility is an important issue. Before construction begins, an organization should consider how the location fits with the organization's overall tasks and goals. A good example is the NSA museum outside Baltimore. It's the kind of place every cryptographic geek dreams of going. It's actually behind the main NSA facility, in what used to be a hotel. (Rumor has it that the hotel was a favorite hangout of the KGB before the NSA bought it.) Although having facilities nearby for visitors and guests can be a good idea, the placement of the hotel so close to a critical agency might be a problem as it would allow for spying.

Keep in mind that the acquisition of a new corporate site involves more than just the cost of the property. Other factors are important as well. For example, if your organization manufactures rockets for satellites, you might want to be near fire stations and hospitals in case there's an accident.

Construction

After you have chosen a location, your next big task is to determine how the facility will be constructed. In many ways, this is driven by what the facility will be used for and by federal, state, and local laws. Buildings used to store grounds-keeping equipment have different requirements than those used as clean rooms for the manufacturer of microchips. In other words, you need to know how various parts of a facility will be used. Remember to make sure that the facility is built to support whatever equipment you plan to put in it.

Tip

The *load* refers to how much weight a facility's walls, floor, and ceiling are being asked to support.

Doors, Walls, Windows, and Ceilings

Have you ever wondered why most doors on homes open inward, whereas almost all doors on businesses open outward? This design is rooted in security. The door on your home is hinged to the inside to make it harder for thieves to remove your door to break in, and it also gives you an easy way to remove the door to bring in that big new leather couch. Years ago, the individuals who designed business facilities built them with the same type of doors. The problem is that open-in designs don't work well when people panic. It's a sad fact that the United States has a long and tragic history of workplace fires. In 1911, nearly 150 women and young girls died when they couldn't exit the Triangle Shirtwaist Factory they were working in when it caught fire. The emergency exit doors were locked! Because of this and other tragic losses of life, modern businesses are required to maintain exits that are accessible and unlocked and that open out. These doors are more expensive than open-in doors because they are harder to install and remove. Special care must be taken to protect the hinges so that they cannot be easily removed. Many doors include a panic bar that permits quick exit: Just push, and you're out. In emergencies or situations in which a crowd is exiting a building quickly, panic bars help keep people moving away from danger.

Maybe you have heard the phrase "security starts at the front door." It is of the utmost importance to keep unauthorized individuals out of a facility or areas where they do not belong. Doors must be as secure as the surrounding walls, floor, and ceiling. If a door is protecting a critical area such as a data center or an onsite server room, the door needs to have the hinges on the inside of the door so that hinge pins cannot be removed. The structural components around the door must also be strengthened. The lock, hinges, strike plate, and the door frame must all have enough strength to prevent someone from attempting to kick, pry, pick, or knock down the door.

The construction of doors varies. Critical infrastructure should be protected with solid core doors. The core material is the material within the door that is used to fill space, provide rigidity, and increase security. Hollow core doors simply contain a lattice or honeycomb made of corrugated cardboard or thin wooden slats. Unlike a hollow core door, a solid core door is hard to penetrate. Solid core doors consist of low-density particle board, rigid foam, solid hardwood, or even steel that completely fills the space within the door. Solid core flush doors have great strength. The outer portion of the door is the skin, which can be wood, steel, or another material, such as a polymer. Commercial steel doors are classified by ANSI/SDI A250.8-2014 into various categories that include standard duty, heavy duty, extra-heavy duty, and maximum duty. Selection of a steel door should be based on usage, degree of abuse, and required protection factor.

Many organizations use electrically powered doors to control access. For example, an employee might have to insert an ID card to gain access to a facility. The card reader would actuate an electric relay that allows the door to open. A security professional should know the state of these door relays in the event of a power loss. An unlocked (or disengaged) state allows employees to enter or exit and not be locked in. If a door lock defaults to open during a power disruption, this is referred to as *fail-safe*. If the lock defaults to locked during a power disruption, this is referred to as *fail-secure*; in this situation, a panic bar or release must be provided so employees are not trapped inside the facility. For high-security doors, it is also important to consider *delay alarms*, which are used to alert security that a security door has been open for a long time. A fail-safe option may be the best option and/or may be a regulatory requirement (depending on the local fire code) when there are people employed within the facility; the code may differ for an unstaffed data warehouse.

Caution

Fail-safe locks protect employees in the event of power loss because they allow employees to exit the facility.

ExamAlert

The terms *fail-safe* and *fail-secure* have very different meanings when discussed in physical security than they have in logical security. When you take the CISSP exam, read the questions carefully to determine the context in which these terms are being used.

Doors aren't the only factor you need to consider. For example, data centers typically should have raised floors, constructed in such a way that they are grounded against static electricity. Cables and wiring should be in conduit, not loose or above the raised floor such that a trip hazard exists. Walls must be designed to slow the spread of fires, and emergency lighting should be in place to light the way for anyone trying to escape in an emergency. Other considerations include the following:

- **Walls**: Walls need to extend from the floor to the ceiling in critical areas and where they separate key departments. Walls should have an adequate fire rating and should be reinforced to keep unauthorized personnel from accessing secure areas, such as data centers or server rooms. Anyone who works in a cubicle environment understands the deficiency of short walls. A loud noise leads employees to "prairie dog" and look over their cubicle walls to see what is happening.
- **Ceilings**: Ceilings need to be waterproof above the plenum space, have an adequate fire rating, and be reinforced to keep unauthorized personnel from accessing secure areas, such as server rooms.

- **Electrical and HVAC**: It is important to plan for adequate power. Rooms that contain servers or other heat-producing equipment need additional cooling to protect that equipment. Heating, ventilating, and air conditioning (HVAC) systems should be controllable by fire-suppression equipment; otherwise, these systems can inadvertently provide oxygen and help feed a fire.

Caution

Air intakes should be properly designed to protect people from breathing toxins or other substances that might cause harm. For example, in 2020, OSHA released new guidelines for ventilation systems to decrease the airborne spread of COVID-19 (see www.businessinsider.com/osha-releases-covid-19-ventilation-guide-for-workplaces-2020-11?op=1).

- **Windows**: Windows are a common point of entry for thieves, burglars, and others seeking access. Windows are usually designed with aesthetics, not security, in mind. Interior or exterior windows need to be fixed in place and should be shatterproof on at least the first and second floors. Windows can be standard glass, tempered, laminated, or acrylic, and they can be embedded with wire mesh to help prevent the glass from shattering. Alarms or sensors might also be needed.
- **Fire escapes**: Fire escapes are critical because they enable personnel to exit in the event of a fire. It is critical that fire drills be performed to practice evacuation plans and determine real exit times. After the first attack on the World Trade Center towers in 1993, it was discovered that it took people two to three times longer to exit the facility than had been planned. Increased drills would have reduced evacuation time.
- **Fire detectors**: Smoke detectors should be installed to warn employees of danger. Sprinklers and detectors should be used to reduce the spread of fire. Smoke detectors can be placed under raised floors, above suspended ceilings, in the plenum space, and within air ducts.

Asset Placement

Security management includes the appropriate placement of high-value assets, such as servers and data centers. Data centers should not be placed above the second floor of a facility because a fire might make them inaccessible. Likewise, you wouldn’t want a data center to be located in a basement because it could be at risk of flooding.

It's not a good idea to have a data center with uncontrolled access or in an area where people will congregate or mill around. Even placing a data center off a main hallway is not a good idea. I often tell students that the location of the server room should be like Talkeetna, Alaska: If you are going there, you cannot be going anywhere else because that is where the road ends.

A data center should have limited accessibility and typically no more than two doors. A first-floor interior room is a good location for a data center. The ceilings should extend all the way up past the drop ceiling, access to the room should be controlled, and doors should be solid core with hinges to the inside. The goal in your design should be to make it as hard as possible for unauthorized personnel to gain access to the data center. Server rooms should not have exterior windows or walls. Placing a server room inside a facility protects the servers against potential destruction from storms and makes it more difficult for thieves or vandals to target them. If individuals can gain physical access to your servers, you have no security.

Environmental Controls

Heat can be damaging to computer equipment, so most data centers are kept at temperatures of around 70°F. Higher and lower temperatures can reduce the useful life of electronic devices. But temperature should not be your only concern when designing a data center. High humidity can cause electronics to corrode, and low humidity increases the risk of static electricity. What might feel like only a small shock to a human can totally destroy electronic components. Grounding devices such as antistatic wrist bands and antistatic flooring can be used to reduce the possibility of damage due to static electricity.

Heating, Ventilating, and Air Conditioning

Do you know what can be hotter than Houston in the summer? A room full of computers without sufficient HVAC. Data centers and other areas that are full of computer or electrical equipment generate heat. Modern electronic equipment is very sensitive to heat and can tolerate temperatures of only 110°F to 115°F degrees before circuits are permanently damaged.

Data centers should have HVAC systems separate from the HVAC of the rest of the facility. The HVAC should maintain positive pressurization and ventilation to control contamination by pushing air outside. Pressurization and ventilation are especially important in case of fire because they ensure that smoke will be pushed out of the facility instead of being pulled in.

Security management should know who is in charge of the HVAC system and how they can be contacted. Intake vents should be protected so that contaminants cannot spread easily. These systems must be controlled to protect organizations and their occupants from chemical and biological threats. HVAC systems generate water in gas (affecting humidity) or liquid (encouraging growth of mold, structural damage, and decay) form. As mentioned earlier in this section, high humidity causes rust and corrosion, and low humidity can increase the risk of static electricity. The ideal humidity for a data center is between 40% and 60% rH to prevent ESD corrosion.

Note

The American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE) has expanded the allowable temperatures for data centers in an effort to promote green environmental practices and to provide a wider range of allowed temperatures.

The Importance of HVAC

HVAC is like any other critical system in an organization and needs to be protected. During a security assessment in 2017, I encountered a page at the client's website that requested authentication. What surprised me is that it appeared to be a control for HVAC. A quick review of the vendor's site provided me with a default username and password. Because I was approved to perform the assessment, I entered the username and password and was taken to a web page that had all the organization's HVAC controls online. My task was simply to report the problem. A malicious hacker might have applied a little heat to the CEO's office or played a game of freeze-out with accounting.

Electrical Power

Electrical power, like HVAC, is a resource that most of us take for granted. Residents of the United States are lucky, but large portions of the world live without dependable electrical power. Even areas that have dependable power can be subject to line noise or might suffer from *electromagnetic interference* (*EMI*). Electrical motors and other electronic devices can cause EMI. You might have noticed that fluorescent lights can also cause electrical problems; this phenomenon is known as *radio frequency interference* (*RFI*). Table 8.2 lists some other power anomalies.

TABLE 8.2 **Power Faults**

Fault	Description
Blackout	Prolonged loss of power
Brownout	Power degradation so that less power is available than normal
Sag	Momentary low voltage
Fault	Momentary loss of power
Spike	Momentary high voltage
Surge	Prolonged high voltage
Noise	Interference superimposed onto the power line
Transient	Electrical noise of a short duration
Inrush	Initial surge of power at startup

Luckily, power conditioners, surge protectors, and uninterruptible power supplies can provide clean power. Although most of the time we seek this clean power, there are times when we need to kill electricity quickly (such as when someone is electrocuted or when there is a danger of water coming into direct contact with a power source). National fire protection codes require that you have an *emergency power off* (*EPO*) switch located near server room exit doors to kill power quickly, if needed. These switches are typically big red buttons.

Caution

An EPO switch should have a plastic cover installed to prevent people from accidentally pressing it.

Uninterruptible Power Supplies (UPSs)

Because computers have become essential pieces of technology, downtime of any significant duration can be devastating to an organization. Power outages can happen, and businesses must be prepared to deal with them. Uninterruptible power supplies (UPSs) can help meet this challenge. Two categories of UPS exist:

- **Online system**: An online system uses AC power to charge a bank of DC batteries. These batteries are held in reserve until power fails. At that time, a power inverter converts the DC voltage back to AC for the computer systems to use. These systems are good for short-term power outages.

- **Standby system**: This type of system monitors a power line for a failure. When a failure is sensed, backup power is switched on. A standby system relies on generators or power subsystems to keep computers running during longer power outages. Most standby generators run on diesel fuel or natural gas:
  - **Diesel fuel**: An organization should maintain at least 12 hours' worth of fuel.
  - **Natural gas**: Gas is an option in areas that have a good supply of natural gas and are geologically stable.

Equipment Lifecycle

Even when you do all the right things—perform preventive maintenance, keep equipment at the right operating temperature, and use surge protectors—equipment eventually ceases to function. This is why many organizations choose to maintain service-level agreements (SLAs).

> ExamAlert
>
> An SLA is a contract with a hardware vendor that provides a certain level of protection. For a fee, the vendor agrees to repair or replace the equipment within the contracted time.

Fire Prevention, Detection, and Suppression

A fire needs three things: oxygen, heat, and fuel. When all three items are present, a fire can ignite and present a lethal threat, as illustrated in the fire tetrahedron in Figure 8.5. Fires can be devastating to people and facilities. Saving human lives should always be your first priority. As a CISSP candidate, it's important to understand that proper precautions, preparation, and training must be performed to help save lives and limit damage.

Fire prevention is a key to proactive defense against fires. A big part of prevention is making sure people are trained and know how to prevent potential fire hazards. Corporate policy must define how employees will be trained to deal with fires.

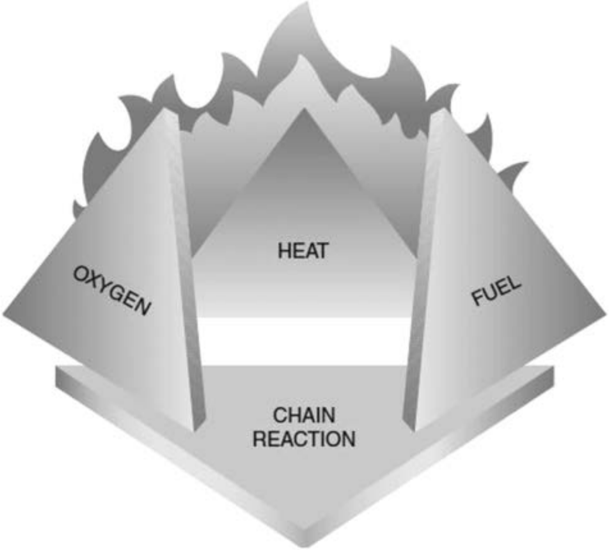


FIGURE 8.5 **Fire Tetrahedron**

Fire drills are another important part of building a good security policy. Fire drills should occur periodically but randomly. Employees should have a designated area to go to in a safe zone outside the facility. Supervisors or others should be in charge of the safe zone and responsible for performing employee head counts to ensure that everyone is present and accounted for. After a drill, employees should be required to use their IDs to reenter the facility to deter social engineering and piggybacking attacks.

Fire-Detection Equipment

Having plans and procedures to carry out in the event of a fire is only part of an overall fire-prevention program. Organizations should make sure they have appropriate and functioning fire-detection equipment so that employees can be alerted to possible danger. Fire detectors can work in different ways and can be activated by the following:

- **Heat**: A heat-activated sensor is triggered when a predetermined temperature is reached or when the temperature rises quickly in a specified time period. The rate-of-rise type of sensor produces more false positives than the predetermined temperature type.

- **Smoke**: A smoke-activated sensor can be powered by a photoelectric optical detector or by a radioactive smoke-detection device.
- **Flame**: A flame-activated sensor is the most expensive of the three types discussed. It functions by sensing either the infrared energy associated with flame or the pulsation of flame.

Fire Suppression

Just being alerted to a fire is not enough. Employees need to know what to do and how to handle different types of fires. A fire can be suppressed by removing heat, fuel, or oxygen. Fires are rated according to the types of materials burning. Although it might be acceptable to throw water on smoldering paper, it would not be a good idea to throw water on a combustible metal fire, which could actually cause the fire to spread. Table 8.3 lists fire classes and corresponding suppression methods.

TABLE 8.3 **Fire Classes and Suppression Methods**

Fire Class	Fire Type	Suppression Method
Class A	Paper or wood fires	Water or soda acid
Class B	Gasoline or oil fires	CO_2, soda acid, or halon
Class C	Electronic or computer fires	CO_2 or halon replacement, such as FM-200
Class D	Fires caused by combustible metals	Dry powder or special techniques
Class K	Commercial kitchen fires	Saponifying agents that blanket the fire

Tip

To remember the classes of fires, think of them in the order of frequency of occurrence: Paper (A) more than liquid (B), liquid more than electric (C), electric more than metal (D).

The two primary methods of corporate fire suppression are use of *water sprinklers* and *gas discharge systems*. Water is easy to work with, widely available, and nontoxic. Gas discharge systems are better suited for areas where humans are not present.

Water Sprinklers

Water sprinklers are an effective means of extinguishing Class A fires. The disadvantage of using sprinkler systems is that water is damaging to electronics. Four variants of sprinkler systems are available:

- **Dry pipe**: As the name implies, this type of sprinkler system contains no standing water. The line contains compressed air. When the system is triggered, the clapper valve opens, air flows out of the system, and water flows in (see Figure 8.6). The benefit of this type of system is that it reduces the risk of accidental flooding and provides some time to cover or turn off electrical equipment. These systems are also great for cold-weather areas, unstaffed warehouses, and other locations where low temperatures could freeze any water standing in the system.

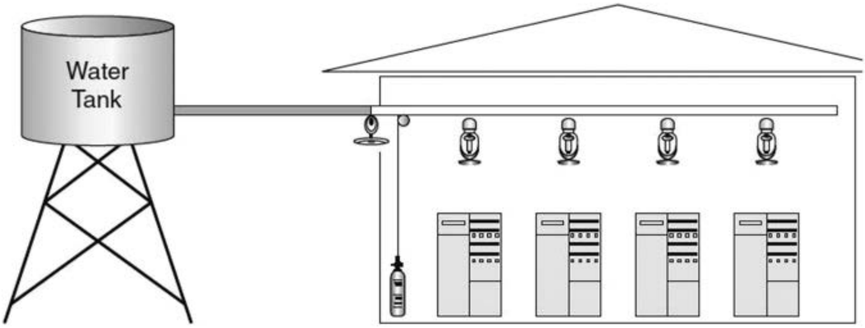


FIGURE 8.6 **Dry-Pipe Fire-Suppression System**

- **Wet pipe**: Wet-pipe systems are more widely used than dry-pipe systems, and they are ready for activation at all times. This type of system is charged and full of water. When triggered, only the affected sprinklers activate. Wet-pipe systems are not triggered by smoke, and they are prone to leaks and accidental discharge. The next time you are staying in a hotel, take a look around, and you'll probably see this type of system. Wet-pipe systems typically use some type of fusible link that allows discharge after a link breaks or melts.

- **Pre-action**: This is a combination system in which pipes are initially dry and do not fill with water until air pressure is reduced. Even then, the system does not activate until a secondary mechanism triggers. The secondary mechanism might be some type of fusible link similar to what is used in a wet-pipe system. The advantage of pre-action systems is that they provide an extra level of control and reduce the chance of accidental triggering.

- **Deluge**: This type of system is similar to a dry-pipe system, except that after the system is triggered, there is no holding back the water. A large volume of water covers a large area quickly. If your organization builds booster rockets for supplies being shuttled to the International Space Station, this might be your preferred suppression system.

Halon

Using halon is one of the oldest fire-suppression methods. It was considered the perfect fire-suppression method: Halon mixes easily with air, doesn't harm computer equipment, and, once dissipated, leaves no solid or liquid residue. Halon is unique in that it does not remove or reduce any of the three necessary components of a fire; instead, halon interferes with the fire's chemical reaction. There are two types of halon: halon 1211 and halon 1301.

The Montreal Protocol of 1987 designated halon as an ozone-depleting substance. Halon is 3 to 10 times more damaging to the ozone layer than CFCs. Other issues with halon exist. If it is deployed in concentrations greater than 10% and in temperatures of 900°F or more, it degrades into hydrogen fluoride, hydrogen bromide, and bromine—a toxic brew that people should not breathe.

If you currently have a halon fire-suppression system, you can leave it in place, but there are strict regulations on reporting discharges. Laws also govern the removal and disposal of halon fire-suppression systems. The EPA has approved some more ecological and less toxic replacements for halon, including the following:

- FM-200
- CEA-410
- NAF-S-III
- FE-13
- Argon
- Low-pressure water mist
- Argonite

Alarm Systems

A range of technical controls can be used to enhance physical security. Alarm systems are one such control.

An alarm system is made up of many components, including an intrusion detection system, a control panel, arming systems, and annunciators. Every time an alarm occurs, someone must respond and determine whether the event is real.

Intrusion Detection Systems (IDSs)

Physical intrusion detection systems (IDSs) are used for detecting unauthorized physical access. IDS sensors around windows or attached to doors can detect the breakage of glass or the opening of doors. These systems are typically effective in detecting changes in the environment. The following are some common types of IDS sensors:

- **Audio detection or acoustical detection sensors**: These sensors use microphones to listen for changes in the ambient noise level. They are susceptible to false positives.
- **Dry contact switches**: These sensors detect the opening of a door or window.
- **Electro-mechanical sensors**: These sensors trigger on a break in the circuit.
- **Motion detectors**: You have probably seen this type of sensor on one of the many security lights sold commercially. Motion detectors can be triggered by audio, radio wave pattern, or capacitance.
- **Vibration sensors**: These sensors use piezoelectric technology to detect vibration and trigger on movement.
- **Pressure-sensitive sensors**: These sensors are sensitive to weight and typically measure a change in resistance that triggers the device. Pressure mats are an example of this type of technology.
- **Photoelectric sensors**: These sensors use infrared light and are laid out as a grid over an area. If the grid is disturbed, the sensor detects a change.
- **Passive infrared sensors**: These sensors can sense changes in heat generated by humans.

ExamAlert

When you encounter intrusion detection questions on the CISSP exam, note whether the question is referencing a *physical* intrusion detection system or a *logical* intrusion detection system.

An organization may choose not to use IDS solutions because they can produce false positives. A false positive result indicates that a condition is present when it actually is not. Before IDSs are deployed, a risk assessment should be performed to determine the true value of these devices to the organization. IDS solutions often are a layer of security used for monitoring and alerting a security guard to do some human inspection to determine whether further preventive measures need to be taken.

Monitoring and Detection

Alarm systems must be monitored and controlled. Either an in-house guard or a third-party organization needs to be assigned the task of monitoring the alarm system. Alarm systems use one of four basic designs, as shown in Table 8.4.

TABLE 8.4 **Alarm Systems**

System Design	Description
Local alarm	The alarm triggers an audio and visual alert locally. A guard is required to respond.
Central station	This system is operated by private third-party organizations that can respond to the customer's premises within 10 to 15 minutes.
Proprietary system	This is an in-house system that is much like a central station except that it is owned and operated by the organization.
Auxiliary system	This is a subcategory of any of the preceding three systems that can dial the police or fire department when a triggering event occurs.

Although movies sometimes show criminals disconnecting alarm systems or cutting the red wire to disable them, in reality, this doesn't work. Alarm systems have built-in *tamper protection*. Any attempt to compromise detection devices, controllers, annunciators, or other alarm components initiates a tamper alarm. Even if power is cut, the alarm will still sound because modern alarm systems are backed up by battery power. Many systems also provide cellular phone backup. The National Fire Protection Association (NFPA) NFPA 72 standard specifies that a local alarm system must provide 60 hours of battery backup, and a central station signaling system must provide 24 hours of backup. In any situation in which the annunciator signals an alarm, NFPA 72 states that the audible alert should be at least 105 dB and have a visual component for those who are deaf or hearing impaired.

No monitoring plan is complete without controls that monitor physical access. Some common facility access controls include the following:

- **CCTV**: An organization can use CCTV to monitor who enters or leaves the facility. It can also correlate these logs with logical access policies for systems and facilities.
- **Card readers or biometric sensors**: An organization can use these devices on server room doors to maintain a log of who accesses the area.
- **Alarm sensors**: An organization can use these devices on doors and windows to detect possible security breaches.
- **Mantraps and gates**: An organization can use these devices to control traffic and log entry to secured areas. Remember that mantraps are double doors used to control the flow of employees and block unauthorized individuals.

ExamAlert

Make sure you know the difference between audit and accountability for the CISSP exam. Audit controls are detective controls, which are used after an event occurs and are usually implemented to detect fraud or other illegal activities. Accountability is the capability to track actions, transactions, changes, and resource usage to a specific user in a system. It is accomplished in part by having unique identification for each user, using strong authentication mechanisms, and logging events.

Intrusion Detection and Prevention Systems

Intrusion detection involves monitoring network traffic, detecting attempts to gain unauthorized access to a system or resource, and notifying the appropriate individuals so that counteractions can be taken. An IDS is designed to function as an access control monitor.

A huge problem with an IDS is that it is an after-the-fact device, used after an attack has already taken place. Other problems with IDSs are false positives and false negatives. A *false positive* occurs when an IDS triggers an alarm for normal traffic. A *false negative* is even worse: It occurs when a real attack occurs but the IDS does not pick it up. IDSs can be divided into two basic types: *network-based intrusion detection systems* (*NIDSs*) and *host-based intrusion detection systems* (*HIDSs*). A HIDS resides on a host computer.

Intrusion prevention systems (*IPSs*) build on the foundation of IDSs and attempt to take the technology a step further. IPSs can react automatically and actually prevent a security event from happening, sometimes even without user intervention. IPSs are considered the next generation of IDSs and can block attacks in real time. The National Institute of Standards and Technology (NIST) now uses the term IDP (intrusion detection and prevention system) to refer to modern devices that maintain the functionality of both IDS and IPS devices. These topics are covered in more detail in Chapter 9, "Software Development Security."

Investigations and Incidents

Many different types of incidents might trigger investigations, including anything from unauthorized disclosure, to theft of property, to outage due to DoS attack, to the detection of an intrusion. As a CISSP candidate, you must understand the following investigation types:

- **Criminal**: This type of investigation exists to preserve the public peace and protect the safety of people. Penalties can include fines and jail time.
- **Civil**: This type of investigation exists to govern matters concerning legal disputes between citizens and organizations. Penalties include fines but not jail.
- **Regulatory**: This type of investigation exists to ensure that administrative policies, procedures, and regulations are being observed. Penalties can include fines and jail time.

An organization needs to create a team to deal with an investigation. The team must understand legal issues and items such as e-discovery evidence collection and how to properly handle the crime scene. For example, the team needs to understand how to protect evidence and maintain it in the proper chain of custody. An organization also needs to establish specific roles and responsibilities within the team, including a team lead to be in charge of the response to any incident.

It is important to establish contacts within your organization with various departments such as HR. For example, if an employee is discovered to have been hacking, the supervisor may want to fire the employee but must first discuss the issue with human resources and the legal department. Even when an incident has been contained and is in the recovery phase, you need to think about what lessons can be learned and how you will report and document your findings. All this information must be included in an incident response policy.

Incident Response

The most important thing to understand when it comes to incident response is that every organization needs to have a plan in place before something unfortunate occurs. The basic stages of incident response are shown here:

1. **Preparation**: Create an incident response team to address incidents.
2. **Identification**: Determine what has occurred.
3. **Mitigation and containment**: Halt the effect of the incident and prevent it from spreading further.
4. **Investigation**: Determine what the problem is and who is responsible to mitigate.
5. **Eradication**: Eliminate the problem.
6. **Recovery**: Clean up any residual effects.
7. **Follow-up and resolution**: Improve security measures to prevent or reduce the impact of future occurrences.

Incident response and forensics are very similar, except that incident response is more focused on finding the problem and returning to normal activities, whereas forensics is more focused on legal aspects and potentially prosecuting the accused. Also, only some organizations can justify forensic investigation due to the potential cost.

Digital Forensics, Tools, Tactics, and Procedures

Governments, the military, and law enforcement have practiced forensics for many years, but forensics is a much younger science for private industry. Its growth in recent years is due to the increased role of computers in the workplace and the types of information and access these computers maintain. There are four types of digital forensics:

- **Software forensics**: This type of forensics includes analysis of malware and other types of malicious code, such as bots, viruses, worms, and Trojans. Organizations such as McAfee and Symantec perform such duties, and tools like decompilers and disassemblers are used.
- **Network forensics**: This type of forensics includes review of network traffic and communication. Tools used include sniffers like Wireshark and Snort.

- **Computer forensics**: This type of forensics includes review of hard drives, solid-state drives, and computer media, such as CDs, DVDs, and USB thumb drives. Tools used include hex editors, Encase, and FTK.
- **Hardware/embedded device forensics**: This type of forensics includes review of smartphones, tablets, routers, and other hardware devices.

Tip

Hardware forensics continues to grow in importance as our reliance on electronic devices increases. One report from a former Pentagon analyst alleges that a large amount of foreign-made Telco gear has built-in backdoors (see www.zdnet.com/former-pentagon-analyst-china-has-backdoors-to-80-of-telecoms-7000000908/).

Digital forensics is a complex field and includes the following stages:

1. Plan and prepare to be creating procedures and policies and conducting training.
2. Secure and isolate the scene to prevent contamination.
3. Record the scene by taking photographs and recording data in an investigator's notebook.
4. Interview suspects and witnesses.
5. Systematically search for other physical evidence.
6. Collect or seize the suspect system or media.
7. Package and transport evidence.
8. Submit evidence to a lab for analysis.

Before discussing the steps of digital forensics in more detail, let's examine the overall concepts and targets of forensic activities. *Digital forensics* defines a precise methodology to preserve, identify, recover, and document computer or electronic data. Growth in this field is directly related to the ever-growing popularity of electronics.

Computers are some of the most commonly targeted items, but they are not the only devices subject to forensic analysis. Smartphones, tablets, digital cameras, iPods, USB drives, and just about any other electronic device can also be analyzed. Attempted hacking attacks and allegations of employee computer misuse have added to the need for organizations to examine and analyze electronic devices. Mishandling concerns can cost organizations millions of dollars.

Organizations must handle each event in a legal and defensible manner. Digital forensics follows a distinct and measurable process that has been standardized.

Standardization of Forensic Procedures

In March 1998, the International Organization on Computer Evidence (IOCE; www.ioec.org) was appointed to draw up international principles for procedures related to digital evidence. The goal was to harmonize methods and practices among nations and guarantee the ability to use digital evidence collected by one country in the courts of another country. The IOCE has established the following six principles to govern these activities:

- When dealing with digital evidence, all generally accepted forensic and procedural principles must be applied.
- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person should be trained in the techniques to be used.
- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in his or her possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

Digital Forensics

Digital forensics can be subdivided into three stages:

1. **Acquisition**: Acquisition is usually performed by means of a *bit-level copy*. A bit-level copy is an exact duplicate of the original data, made using a write blocker, that allows an examiner to scrutinize the copy while leaving the original intact.
2. **Authentication**: An investigator must show that the original data is unchanged and has not been tampered with; the investigator must be able to prove that the bit-level copy is an exact copy. Authentication can be accomplished through the use of checksums and hashes, such as MD5 and SHA.

Tip

Message digests, such as MD5 and SHA, are used to ensure the integrity of files and data and to ensure that no changes have occurred.

3. **Analysis**: An investigator must be careful while examining the data and ensure that all actions are thoroughly documented. The investigator recovers evidence by examining files, state information, drive slack space, file slack space, free space, hidden files, swap data, Internet cache, and other locations, such as the Recycle Bin. Copies of the original disks, drives, or data are usually examined to protect the original evidence.

Acquisition

Acquisition refers to assuming possession of evidence or contracting to assume possession. In many instances, a forensic analyst is asked to acquire hard drives, computers, media, or other items on site. Just as with any other investigation, an analyst in a digital forensics case should make careful notes about what physical evidence is recovered and show the chain of custody for all evidence acquired. Physical evidence and digital forensics can help build a relationship between an incident scene, a victim, and a suspect (see Figure 8.7).

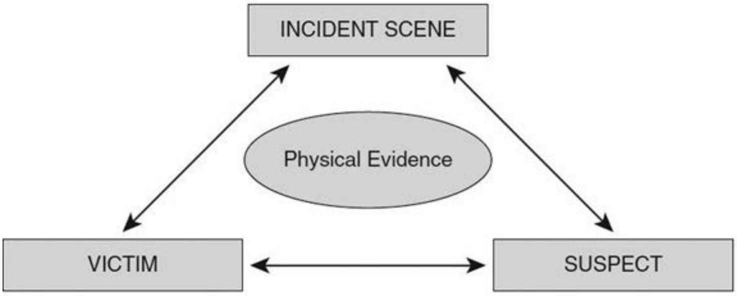


FIGURE 8.7 **Relationship of Evidence to Suspect**

During the acquisition stage, the following processes occur:

- Documentation and collection of the evidence
- Protection of the chain of custody
- Identification, transportation, and storage
- Approved duplication and copying

During collection and handling of evidence, it is important to record everything. You can use a digital camera to record the layout of the scene. You need to document the condition of the computer systems, attachments, cables, physical layout, and all electronic media. You can also use a camera to take pictures of any screen settings visible on a running system. You should also document internal storage devices and hardware configuration, including hard drive make, model, size, jumper settings, location, and drive interface as well as internal components such as the sound card, video card, and network card.

Tip

The handling of evidence is of special importance to a forensic investigator. This is addressed through the *chain of custody*, a process that helps protect the integrity and reliability of the evidence by providing an evidence log that shows every access to evidence, from collection to appearance in court.

A forensic analyst needs to keep adequate records and build a proper chain of custody. Although the chain of custody is something that those in law enforcement are familiar with, it might be new to many IT professionals but will surely be called into question for all digital evidence in the court of law as well. *Chain of custody* is used to address the reliability and creditability of evidence. Chain of custody is the process of documenting the journey of any and all evidence while keeping it under control. Chain of custody should be able to answer the following the questions:

- Who collected the evidence?
- Where was the evidence collected?
- When did possession of the evidence occur?
- How was the evidence stored and protected (that is, what software tool was used)? Is this a best practice tool used by the industry? Is the professional trained on use of the tool? How many times has the professional used the tool?
- If evidence was removed from storage, why, by whom, and for how long was it taken from storage?

Caution

Computer evidence is very volatile; it is therefore of utmost importance to protect the chain of custody throughout the entire evidence lifecycle.

Even though many forensic investigations might not lead to court cases or legal showdowns, some do, so you must always maintain the integrity of evidence. After collecting and recording evidence, it is likely that you have reached the point at which you might need hard drives or fixed disks for duplication. Any analysis needs to be performed on a copy of the evidence so that the original can remain safely stored away. The objective of disk imaging is to preserve the original copy in a pristine state and to provide the analyst with a copy to use for investigation. This process usually consists of three steps:

1. Remove the drive from the suspect's computer.
2. Connect the suspect's drive to a write blocker and fingerprint it using a message digest.
3. Use a clean wiped drive to make a copy of the suspect's computer or copy it to an image file.

The copy must be an exact copy of the original. This is known as a bit-level copy, or *physical copy*. A bit-level copy is a copy of everything, including all files, file slack, and drive slack or free space. A logical copy is not this type of copy.

Caution

Investigators must use caution when seizing computer systems because the equipment might be booby-trapped. That is, the device may be set up to act as a dead man's switch that will activate when a network connection is broken or when a computer case is opened. Such a switch can wipe all the information on the device, encrypt files, turn off a self-encrypted drive, or take other actions that make the data inaccessible.

It's critical that a hard drive used to receive a copy of the evidence not have any files, data, or information stored on it. Common practice is to wipe the drive before using it to receive the copy. *Drive wiping* is the process of overwriting all addressable locations on the disk. The U.S. Department of Defense (DoD) drive-wiping standard 5220-22M states, "All addressable locations must be overwritten with a character, its complement, then a random character and verify." Drive wiping is useful for forensic purposes, for organizations that want to dispose of hard drives, and for criminals who want to dispose of evidence. By making up to seven wiping passes over the media, an organization can further decrease the possibility of data recovery.

Authentication

Having an exact copy of the data in an investigation is just a start. You must also show that the copy and the original are exactly the same. This verification can be accomplished by means of hashing or other integrity algorithms that fingerprint the original drive and the forensically produced copy. Integrity checks ensure the veracity of the information and allow users of that information to have confidence in its correctness. There are many ways that data can become distorted, either accidentally or intentionally. A forensic analyst must protect against all distortion.

Integrity

Integrity can apply to paper documents as well as electronic ones. Forgers can copy and create fake paper documents, but it is not a skill easily learned. Integrity in electronic documents and data is much more difficult to protect. Forensic duplication and verification require cryptographic algorithms, which use one-way hashing algorithms. Rules of evidence generally require that when a duplicate of the original data is admitted as evidence, it must be an exact duplicate of the original. The hash values must match and be of sufficient strength to prove that tampering has not occurred. Not every investigation you become involved in will go to court, but ethics and good practice require that evidence be authenticated as unchanged from the moment of discovery to the point of disposal.

Tip

A *primary image* is the original image. It should be held in storage and kept unchanged. The *working image* is the image used for analysis purposes. Forensic examiners should work on the working image only.

Analysis

Analysis is the process of examining the evidence. Forensic analysts typically make two copies of the original drive and work with one of the copies. The following items are commonly analyzed in an investigation:

- Word documents, compressed files, and images
- Deleted items
- Files created/accessed/modified on suspect dates
- Email files (such as .PST files)
- Files stored in NTFS streams

Forensic investigators use many different programs to review the evidence. With *dead analysis*, a machine is turned off and the drive analyzed. Sometimes, a machine must be analyzed without being turned off; this is a *live analysis*. With live analysis, it is critical that evidence be examined from most volatile to least volatile.

Note

No single program will do everything you need to perform during an investigation. As an example, you may want to use hex editors to examine slack space and deleted items.

The Disaster Recovery Lifecycle

Disaster recovery is closely related to incident response and forensics. The purpose of disaster recovery is to get a damaged organization restarted so that critical business functions can resume. When a disaster occurs, the process of progressing back to normal operations includes the following stages:

1. Crisis management
2. Recovery
3. Reconstitution
4. Resumption

Federal and state government entities typically use a continuity of operations (COOP) site, which is designed to take on operational capabilities when the primary site is not functioning. The length of time that the COOP site is active and the criteria in which the COOP site is enabled depend on the business continuity and disaster recovery plans. Both government and nongovernment entities typically make use of a checklist to manage continuity of operations. Table 8.5 shows a sample disaster recovery checklist.

TABLE 8.5 **Disaster Recovery Checklist**

Time Frame	Activity
When disaster occurs	Notify disaster recovery manager and recovery coordinator
Within 2 hours	Assess damage, notify senior management, and determine immediate course of action
Within 4 hours	Contact offsite facility, recover backups, and replace equipment, as needed

Time Frame	Activity
Within 8 hours	Provide management with updated assessment and begin recovery at updated site
Within 36 hours	Reestablish full processing at alternate site and determine timeline for return to primary facility

ExamAlert

The disaster recovery manager should direct short-term recovery actions immediately following a disaster.

Individuals responsible for emergency management need to assess damage and perform triage. The areas impacted the most need attention first. Protection of life is a priority while working to mitigate damage. Recovery from a disaster requires that personnel be sent to the recovery site. When employees and materials are at the recovery site, interim functions can resume operations. This might entail installing software and hardware. Backups might need to be loaded, and systems might require configuration.

The recovery process does not necessarily occur as a series of steps. For example, while the recovery process is taking place, teams are also dispatched to the disaster site to start the cleanup, salvage, and repair process. When those processes are complete, normal operations can resume.

When operations are moved from the alternate operations site back to the restored site, the efficiency of the restored site must be tested. Processes should be sequentially returned, from least critical to most critical. In the event that a few glitches need to be worked out in the restored facility, you can be confident that your most critical processes are still in full operation at the alternate site.

Flat Tires Are a Fact of Life

When teaching the CISSP Security Operations domain in the classroom, one of the things I always try to impress on students is that the disaster recovery lifecycle is something that, in reality, they already really know. Consider this: While driving home from the airport, I had a flat tire. Here is what transpired, step by step:

- **Crisis management**: On realizing I had a flat, I pulled safely off the freeway.
- **Recovery**: Working quickly, I jacked up the car and replaced the flat tire with the emergency spare that GM generously provides.

- **Reconstitution**: Back on the freeway, I was able to limp along with my 50-mile-per-hour-rated spare until I could reach a tire repair shop.
- **Resumption**: As expected, the technician confirmed that the tire could not be fixed. But for only $149 plus a few fees, he could get me back on the road. I headed home with the new tire on the car and my wallet a little emptier.

Consider this story when you are trying to conceptualize disaster recovery and, hopefully, it will make the task a little easier.

Teams and Responsibilities

Individuals involved in disaster recovery must deal with many things; when called to action, their activities focus on emergency response, assessing the damage, recovery operations, and restoration. Figure 8.8 illustrates an example of disaster recovery activities.

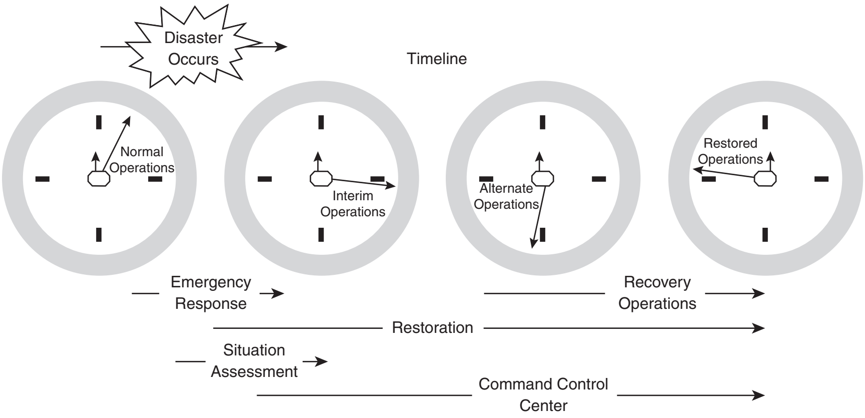


FIGURE 8.8 **Disaster Recovery Timeline**

The recovery team has the necessary authority and responsibility to get the alternate site up and running. This site is used as a stand-in for the original site until full operations can be restored.

Caution

Physical security is of great importance after a disaster. Precautions such as guards, temporary fencing, and barriers should be deployed to prevent looting and vandalism.

Recovery Strategy

When a disaster occurs, a recovery strategy is needed. A recovery strategy involves planning for failure by using methods of resiliency. Developing a successful recovery strategy requires the support of senior management. To judge the best strategy to recover from a given interruption, the team must evaluate and complete the following:

- Detailed documentation of all costs associated with each possible alternative
- Quoted cost estimates for any outside services that might be needed
- Written agreements with chosen vendors for all outside services
- Possible resumption strategies in the event of a complete loss of the facility
- Documentation of findings and conclusions as a report to management of chosen recovery strategy for feedback and approval

This information is used to determine the best course of action based on the analysis of data from the business impact analysis (BIA). With so much to consider, it is helpful to divide the organization's recovery into specific areas, functions, or categories, such as the following:

- Business process recovery
- Facility and supply recovery
- User recovery
- Operations recovery

Business Process Recovery

Business processes may be interrupted due to the loss of personnel, critical equipment, supplies, or office space; or from uprisings, such as strikes. Even if a facility is intact after a disaster, people are required and are an important part of the business process recovery.

Workflow diagrams and documents can assist with business process recovery by mapping relationships between critical functions to evaluate interdependencies. Often, a critical process cannot be done because a related process was left out of the workflow. For example, say that you bring in the hardware, software, electric supply, and a system engineer to restore a computerized business process; however, you do not have any network cables to connect the equipment. Now all the vendors are closed because of the storm, and no $5 networking cables are available. A process flow created before disaster strikes can identify what needs to be done and what parts and components will be needed. Building a workflow diagram allows an organization to examine the resources required for each step and the functions that are critical for continued business operations.

Facility and Supply Recovery

Facility and supply interruptions can be caused by fire, loss of inventory, transportation or telecommunications problems, or even heating, ventilating, and air conditioning (HVAC) problems. An emergency operations center (EOC) must be established, and redundant services must be enabled for rapid recovery from interruptions. Many options are available, from a dedicated offsite facility, to agreements with other organizations for shared space, to the option of putting up a prefab building and leaving it empty as a type of cold backup site. The following sections examine some of these options.

Subscription Services

Building and running data-processing facilities is expensive. Organizations typically opt instead to contract their EOC facility needs to a subscription service. The CISSP exam categorizes these subscription services as hot, warm, and cold sites.

A *hot site* is ready to be brought online quickly. It is fully configured and equipped with the same systems as the regular production site. It can be made operational within just a few hours. A hot site needs staff, data, and procedural documentation. Hot sites are a high-cost recovery option but can be justified when a short recovery time is required. A hot site subscription service involves a range of associated fees, including monthly cost, subscription fees, testing costs, and usage or activation fees. Contracts for hot sites need to be closely examined because some services charge extremely high activation fees to discourage subscribers from utilizing these facilities for anything less than a true disaster. To get an idea of the types of costs involved, www.drj.com reports that subscriptions for hot sites average 52 months in duration, and costs can be as high as $120,000 per month.

Caution

It’s possible that during a disaster, one backup site might not be available. Many organizations therefore have a backup to a backup site. Such a site is known as a *tertiary site*.

Regardless of the fees involved, a hot site needs to be periodically tested to evaluate processing abilities as well as security. The physical security of a hot site should be at least at the same level as the security of the primary site. Finally, it is important to remember that a hot site is intended for short-term use only. With a subscriber-based service, there might be others in line for the same resource once your contract ends. An organization should have a plan to recover primary services quickly or move to a secondary location.

Caution

To decrease risk of sabotage and other potential disruptions, hot sites should not be externally identifiable.

For organizations that lack the funds to spend on a hot site or in situations where a short-term outage is acceptable, a *warm site* might be acceptable. A warm site has data equipment and cables and is partially configured. It could be made operational within a few hours to a few days. The assumption with a warm site is that necessary computer equipment and software can be procured despite the disaster. Although a warm site might have some computer equipment installed, it is typically of lower processing power than at the primary site. The costs associated with a warm site are slightly lower than those of a hot site (see Figure 8.9).

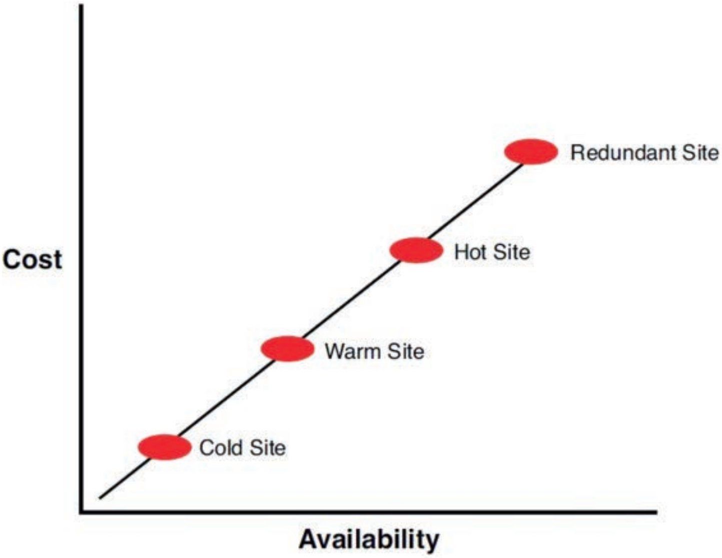


FIGURE 8.9 Recovery Site Availability Versus Cost

In situations where even longer outages are acceptable, a cold site might be the right choice. A cold site is basically an empty room with only rudimentary electrical power and computing capability. Although it might have a raised floor and some racks, it is nowhere near ready for use. It might take several weeks to a month to get the site operational. Cold sites are less ready than hot and warm sites, but the associated costs are also much lower than for hot or warm sites, averaging $2,000 per month or more.

Tip

Cold sites are a good choice for the recovery of noncritical services.

Redundant Sites

The CISSP exam considers redundant sites to be sites owned by the organization. Although these sites might be either partially or totally configured, the CISSP exam does not typically expect you to know that level of detail. A redundant site is capable of handling all operations if another site fails. Although a redundant site can be expensive, it offers an organization fault tolerance, which is necessary for an organization that cannot withstand any downtime. If redundant sites are geographically dispersed, the possibility of more than one being damaged is reduced. For low- to medium-priority services, a distance of 10 to 20 miles from the primary site is considered acceptable. If the loss of services, for even a very short time, could cost the organization millions of dollars, the redundant site should be farther away. Therefore, redundant sites that are meant to support highly critical services should not be in the same geographic region or subject to the same types of natural disasters as the primary site.

An organization that has multiple sites dispersed in different regions of the world might choose to use multiple processing centers. This way, a branch in one area can act as backup for a branch in another area.

Mobile Sites

Mobile sites are usually tractor-trailer rigs that have been converted into data-processing centers. These sites contain all the necessary equipment and are mobile, permitting transport to any business location quickly. Rigs can also be chained together to provide space for data processing and provide communication capabilities. Mobile units are a good choice for areas where no recovery facilities exist and are commonly used by the military and organizations such as large insurance agencies for immediate response during a disaster. They can get critical services up and running quickly and commonly provide tactical satellite services but do not work as a long-term solution.

> **Note**
>
> Mobile sites are a non-mainstream alternative to traditional recovery options. Mobile sites typically consist of fully contained tractor-trailer rigs that come with all the facilities needed for a data center. Units can be quickly moved to any site and are perfect for use after storms, whose boundaries are hard to predict.

Whatever recovery method is chosen, regular testing is important to verify that the redundant site meets the organization's needs and that the team can handle the workload to meet minimum processing requirements.

Reciprocal Agreements

In a reciprocal agreement, two organizations pledge to assist one another in the event of a disaster. The organizations would share space, computer facilities, and technology resources. On paper, this appears to be a cost-effective approach, but it has drawbacks. Each party to such an agreement must place its trust in the other organization to provide aid in the event of a disaster. However, the party that has not been affected by the disaster may be hesitant to follow through when a disaster actually occurs.

Also, confidentiality is an important issue with a reciprocal agreement. The damaged organization is in a vulnerable position and needs to trust the other party's housing of the victim's confidential information. Legal liability can also be a concern; for example, one organization might agree to help another and be hacked as a result. Finally, if the two parties to a reciprocal agreement are geographically near one another, there is a danger that disaster could strike both of them, thereby rendering the agreement useless.

The biggest drawbacks to reciprocal agreements are that they are hard to enforce and that, many times, incompatibilities in organization hardware, software, and even cultures are not discovered until after a disaster strikes.

User Recovery

User recovery focuses on what employees need in order to do their jobs. User recovery must address the following:

- Procedures, documents, and manuals
- Communication systems

- Means of mobility and transportation to and from work
- Workspace and equipment
- Alternate site facilities
- Basic human requirements, such as food and water, sanitation facilities, rest, money, and morale

An organization might be able to get employees to a backup facility after a disaster, but if there are no phones, desks, or computers, the employees' ability to work will be severely limited.

User recovery plans sometimes need to consider food. For example, my brother-in-law works for a large chemical company on the Texas Gulf Coast. During hurricanes and other disasters, he is required to stay at work as part of the emergency operations team. His job requires him to stay at the facility regardless of whether the disaster lasts two days or two weeks. During a simulation test several years ago, it was discovered that someone had forgotten to order food for the facility where the employees were to remain for the duration of the drill. Luckily, the 40 or so hungry employees were not really in a disaster and were able to have pizza delivered. Had it been a real disaster, however, no takeout would have been available.

Operations Recovery

Operations recovery addresses interruptions caused by equipment failure. Redundancy—redundant equipment, redundant arrays of inexpensive disks (RAID), backup power supplies (BPSs), and other redundant services—solves this potential loss of availability.

Hardware failures are some of the most common disruptions that can occur. Preventing this type of disruption is critical to operations. The best time to start planning hardware redundancy is when equipment is purchased. At purchase time, there are two important numbers that a buyer must investigate:

- **Mean time between failure (MTBF)**: Used to calculate the expected lifetime of a device. A higher MTBF number means the equipment should last longer.
- **Mean time to repair (MTTR)**: Used to estimate how long it would take to repair the equipment and get it back into production. Lower MTTR numbers mean the equipment requires less repair time and can be returned to service sooner.

You can use this formula to calculate availability of equipment:

MTBF / (MTBF + MTTR) = Availability

To maximize availability of critical equipment, an organization can consider obtaining an SLA. There are many kinds of SLAs, but an SLA for operations recovery is a contract between an organization and a hardware vendor, in which the vendor promises to provide a certain level of protection and support. For a fee, the vendor agrees to repair or replace the covered equipment within the contracted time.

Fault tolerance can be applied at the server or drive level. For servers, *clustering* is a technology that allows for high availability; clustering means grouping multiple servers together so that they are viewed logically as a single server. Users see a cluster as one unit. The advantage is that if one server in the cluster fails, the remaining active servers pick up the load and continue operation.

Fault tolerance at the drive level is achieved primarily with RAID, which provides hardware fault tolerance and/or performance improvements. This is accomplished by breaking up the data and writing it across one or more disks. To applications and other devices, RAID appears as a single drive. Most RAID systems have hot-swappable disks. This means that faulty drives can be removed and replaced without turning off the entire computer system. If a RAID system uses parity and is fault tolerant, the parity data can be used to reconstruct the newly replaced drive. The technique for writing the data across multiple drives is called *striping*. With striping, although write performance remains almost constant, read performance is drastically increased.

All hard drives and data storage systems fail. It's not a matter of if but when. There are many types of RAID; Table 8.6 lists and describes the nine most common types.

TABLE 8.6 **RAID Levels**

Level	Type	Description
RAID 0	Striped disk without fault tolerance	Provides data striping but no fault tolerance. If one drive fails, all data in the array is lost.
RAID 1	Mirroring and duplexing	Provides disk mirroring. Level 1 provides twice the read transaction rate of single disks and the same write transaction rate as single disks.
RAID 2	Error-correcting	Stripes data at the bit level rather than the block level. This level of RAID is rarely used.
RAID 3	Bit-interleaved parity	Offers byte-level striping with a dedicated parity disk.

Level	Type	Description
RAID 4	Dedicated parity drive	Provides block-level striping. If a data disk fails, the parity data is used to create a replacement disk.
RAID 5	Block-interleaved distributed parity	Provides data striping at the byte level, good performance, and good fault tolerance. It is also one of the most popular types of RAID.
RAID 6	Independent data disks with double parity	Provides block-level striping with parity across all disks.
RAID 10	A stripe of mirrors	Creates mirrors and a RAID 0 stripe. This is not one of the original RAID levels. Sometimes referred to as 0+1.
RAID 15	Mirrors and parity	Creates mirrors RAID 1 and RAID 5 distributed parity. This is not one of the original RAID levels.

It is worth mentioning that RAID Level 0 is used for performance only and not for redundancy.

The most expensive RAID solution to implement is RAID Level 1 because all the data on disk A is mirrored on disk B. However, mirroring has a disadvantage: If data on disk A is corrupted, data on disk B will also become corrupted.

The most common form of RAID is RAID 5. RAID 5 striping is useful because it offers a balance of performance and usability. RAID 5 stripes both data and parity information across three or more drives, whereas RAID 3 uses a dedicated parity drive.

Striping the data and parity across all drives removes the drive stress that the dedicated parity drive inflicts. Fault tolerance is provided by ensuring that, if any one drive dies, the other drives maintain adequate information to allow for continued operation and eventual rebuilding of the failed drive (once replaced).

Just a bunch of disks (JBOD) is somewhat like RAID, but it is really not RAID at all. JBOD can use existing hard drives of various sizes, combined together into one massive logical disk. JBOD provides no fault tolerance and no increase in speed. The only benefit of JBOD is that you can use existing disks, and if one drive fails, you lose the data on only that drive. Both of these advantages are minimal, so don't expect to see too many organizations actually using this technique.

To better understand how RAID and JBOD technologies compare, take a moment to review Figure 8.10.

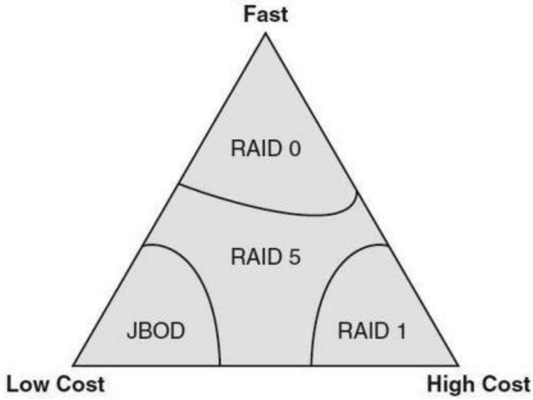


FIGURE 8.10 RAID Technologies

ExamAlert

Fault tolerance and RAID are important controls. For the CISSP exam, you should be able to define RAID and describe specific levels and each level's attributes. For example, you should know that RAID 1 has the highest cost per byte, and RAID 5 is the most widely used type.

Fault Tolerance

Fault tolerance requires a redundant system so that in the event of a failure, a backup system can take the place of the primary system. Tape and hard drives are commonly used for fault tolerance. A tape-based system is an example of a *sequential access storage device* (*SASD*). If you need information from a portion of the tape, you need to traverse the tape drive to the required position in order to access the information. A hard drive is an example of a *direct access storage device* (*DASD*). The advantage of a DASD is that information can be accessed much more quickly.

One option that can be used to speed up the sequential process when large amounts of data need to be backed up is a *redundant array of independent tapes* (*RAIT*). RAIT is efficient when large numbers of write operations are needed for massive amounts of data. RAIT stripes the data across multiple tapes, much as a RAID array and can function with or without parity.

Another technology, *massive array of inactive disks* (*MAID*), offers a distributed hardware storage option for the storage for data and applications. It was designed to reduce the operational costs and improve long-term reliability of disk-based archives and backups. MAID is similar to RAID except that it provides power management and advanced disk monitoring. MAID might or might not stripe data and/or supply redundancy. A MAID system powers down inactive drives, reduces heat output, reduces electrical consumption, and increases the disk drive's life expectancy.

Storing and managing so much data can become a massive task for an organization. Organizations might have tape drives, MAID, RAID, optical jukeboxes, and other storage solutions to manage. To control all these systems, many organizations now use *storage area networks* (*SANs*). Although SANs are not common in small organizations, large organizations with massive amounts of data can use them to provide redundancy, fault tolerance, and backups. The beauty of this type of system is that the end user does not have to know the location of the information; the user must only make a request for the data, and the SAN retrieves and recovers it.

It is not just data that can be made fault tolerant. Computer systems can also benefit from fault tolerance. Redundant servers can be used, and the computing process can be distributed to take advantage of the power of many computers. There are two related ways to provide fault tolerance for computer systems:

- **Clustering**: Clustering involves grouping computers to reach a greater level of usability than is possible with redundant servers. Whereas a redundant server waits until it's needed, a clustered server actively participates in responding to the server's load. If one of the clustered servers fails, the remaining servers can pick up the slack.

Note

A *server farm* can be used as a cluster of computers for complex tasks or in cases where supercomputers might have been used in the past.

- **Distributed computing**: This technique is similar to clustering except there is no central control. *Distributed computing*, also known as *grid computing*, can be used for processes that require massive amounts of computer power. Because grid computing is not under centralized control, processes that require high security should not be considered. Distributed computing also differs from clustering in that distributed computers can add or remove themselves as they please.

Note

An example of distributed computing can be seen in the 2020 project Minecraft@ Home, which was used to study questions related to Minecraft, such as the properties of worlds that can be generated from different random seeds.

Data and Information Recovery

Solutions to data interruptions include backups, offsite storage, and remote journaling. Because data processing is essential to most organizations, a data and information recovery plan is critical. The objective of such a plan is to back up critical software and data to enable quick restores with the least possible loss of content. Policy should dictate when backups are performed, where the media is stored, who has access to the media, and what the reuse or rotation policy will be. Types of backup media include tape reels, tape cartridges, removable hard drives, solid-state storage, disks, and cassettes.

Tape and optical systems still have the majority of the market share for backup systems. Common types of media include:

- 8 mm tape
- CDR/W media (recommended for temporary storage only)
- Digital audio tape (DAT)
- Digital linear tape (DLT)
- Quarter inch tape (QIC)
- Write-once/read-many (WORM)

ExamAlert

CISSP exam questions regarding different backup types can be quite tricky. Make sure you clearly know the difference before the exam. Backups can also be associated with disaster recovery planning metrics such as RPO, RTP, and MTTR.

Backups

Backups need to be stored somewhere, and they need to be accessible when it’s time to restore not just data but applications and configuration settings as well. Where the backup media is stored can have a real impact on how quickly data can be restored and brought back online. The media should be stored in more than one physical location to reduce the possibility of loss. Remote sites should be managed by a media librarian. It is this individual's job to maintain the site, control access, rotate media, and protect this valuable asset. Unauthorized access to the media is a huge risk because it could impact the organization's capability to provide uninterrupted service. Who transports the media to and from the remote site is also an important concern. Important backup and restoration considerations include the following:

- Maintenance of secure transportation to and from the site
- Use of bonded delivery vehicles
- Appropriate handling, loading, and unloading of backup media
- Use of drivers trained in proper procedures related to picking up, handling, and delivering backup media
- Legal obligations for data, such as encrypted media, and separation of sensitive data sets, such as credit card numbers and credit card security codes
- 24/7 access to the backup facility in the event of an emergency

An organization should contract its offsite storage needs with a known firm that demonstrates control of its facility and is responsible for its maintenance. Physical and environmental controls at offsite storage locations should be equal to or better than those in the organization's own facility. A letter of agreement should specify who has access to the media and who is authorized to drop it off or pick it up. There should also be agreement on response times that will be met in the event of a disaster. Onsite storage should maintain copies of recent backups to ensure the capability to recover critical files quickly.

Backup media should be securely maintained in an environmentally controlled facility with physical control appropriate for critical assets. The area should be fireproof, and those depositing or removing media should have records of their access logged by a media librarian.

Table 8.7 lists some sample functions and their recovery times.

TABLE 8.7 **Organization Functions and Example Recovery Times**

Function	Recovery Time	Recovery Strategy
Database	Minutes to hours	Database shadowing (covered later in this chapter, in the section "Other Data Backup Methods")
Help desk	7 to 14 days	Warm site

Function	Recovery Time	Recovery Strategy
Research and development	Several weeks to a month	Cold site
Purchasing	1 to 2 days	Hot site
Payroll	1 to 5 days	Multiple site

Software itself can be vulnerable, even when good backup policies are followed, because sometimes software vendors go out of business or no longer support needed applications. In these instances, *escrow agreements* can help. Escrow agreements allow an organization to obtain access to the source code of business-critical software if the software vendor goes bankrupt or otherwise fails to perform as required. Given the myriad compilers and operating systems, source code escrow agreements now address everything required to build a product, including operating systems, tools, and compilers.

Each backup method has benefits and drawbacks. Full backups are the most comprehensive but take the longest time to create. So, even though it might seem best to do a full backup every day, it might not be possible due to the time and expense.

Tip

Two basic methods can be used to back up data: automated and on-demand backups. Automated backups are scheduled to occur at a predetermined time. On-demand backups can be scheduled at any time.

Full Backups

During a full backup, all data is backed up, and no files are skipped or bypassed; you simply designate which server to back up. A full backup takes the longest to perform and the least time to restore because only one backup data set is required.

Differential Backups

With a differential backup, a full backup is typically done once a week, and a differential backup, which involves backing up all files that have changed since the last full backup, is done more frequently, typically daily. If you need to restore, you need the last full backup and the most recent differential backup.

Differential backups make use of files' *archive bits*. The archive bit indicates that a file is ready for archiving, or backup. A full backup clears the archive bit for each backed-up file. Then, if anyone makes changes to one of these files, its archive bit is toggled on. During a differential backup, all the files that have the archive bit on are backed up, but the archive bit is not cleared until the next full backup. Because more files will likely be modified during the week, the differential backup time will increase each day until another full backup is performed; still, this method takes less time than a daily full backup. The value of a differential backup is that only two backup data sets are required: the full backup and the differential backup.

Incremental Backups

With an incremental backup strategy, a full backup is scheduled for once a week (typically), and only files that have changed since the previous full backup *or* previous incremental backup are backed up more frequently (usually daily).

Unlike in a differential backup, in an incremental backup, the archive bit is cleared on backed-up files; therefore, incremental backups back up only changes made since the last incremental backup. This is the fastest backup option, but it takes the longest to restore because the full backup must be restored, and then all the incremental backups must be restored, in order.

Tape Rotation Schemes

Tapes and other media used for backups eventually fail. It is important to periodically test backup media to verify its functionality. Some tape rotation methods include the following:

- **Simple**: A simple tape-rotation scheme uses one tape for every day of the week and then repeats the pattern the following week. One tape can be for Monday, one for Tuesday, and so on. You add a set of new tapes each month and then archive the previous month's set. After a predetermined number of months, you put the oldest tapes back into use.
- **Grandfather-father-son (GFS)**: With this scheme, you typically use one tape for monthly backups, four tapes for weekly backups, and four tapes for daily backups (assuming that you are using a five-day work week). It is called *grandfather-father-son* because the scheme establishes a kind of hierarchy: The grandfather is the single monthly backup, the fathers are the four weekly backups, and the sons are the four daily backups.

- **Tower of Hanoi**: This tape-rotation scheme is named after a mathematical puzzle. It involves using five sets of tapes, labeled A through E. Set A is used every other day; set B is used on the first non-A backup day and is used every 4th day; set C is used on the first non-A or non-B backup day and is used every 8th day; set D is used on the first non-A, non-B, or non-C day and is used every 16th day; and set E alternates with set D.

Note

Some backup applications perform *continuous backups* and keep a database of backup information. These systems are useful when a restoration is needed because the application can provide a full restore, a point-in-time restore, or a restore based on a selected list of files MG.

Data Replication Techniques

Data replication can be handled using two basic techniques, each of which provides various capabilities:

- **Synchronous replication**: This technique uses an atomic write operation, which can either complete on both sides or be abandoned. Its strength is that it guarantees no data loss.
- **Asynchronous replication**: This technique updates as allowed but may experience some performance degradation. Its downside is that the remote storage facility may not have the most recent copy of data; therefore, some data may be lost in the case of an outage.

Other Data Backup Methods

Other alternatives exist for further enhancing an organization's resiliency and redundancy. Some organizations use the following techniques by themselves, and others combine these techniques with other backup methods:

- **Database shadowing**: Databases are high-value assets for most organizations. File-based incremental backups can read only entire database tables and are considered too slow. A database shadowing system writes the data to two physical disks. It creates good redundancy by duplicating the database sets to mirrored servers. Therefore, this is an excellent way to provide fault tolerance and redundancy. Shadowing mirrors changes to the database as they occur.

- **Electronic vaulting**: Electronic vaulting involves making a copy of database changes to a secure backup location. It is a batch-process operation in which all current records, transactions, and/or files are copied to the offsite location. To implement vaulting, an organization typically loads a software agent onto the systems to be backed up, and then, periodically, the vaulting service accesses the software agent on these systems to copy changed data.
- **Remote journaling**: Remote journaling is similar to electronic vaulting, except that information is duplicated to the remote site as it is committed on the primary system. By performing live data transfers, this mechanism allows alternate sites to be fully synchronized and fault tolerant at all times. Depending on the configuration, it is possible to configure remote journaling to record only the occurrence of transactions and not the contents of the transactions. Remote journaling can provide a very high level of redundancy.
- **Storage area network (SAN)**: A SAN supports disk mirroring, backup and restore, archiving, and retrieval of archived data in addition to data migration from one storage device to another. A SAN can be implemented locally or can use storage at a redundant facility.
- **Cloud computing backup**: This type of backup can offer a cost-savings alternative to traditional backup techniques. These backups should be carefully evaluated, as there are many concerns when using cloud-based services. Cloud backups can be deployed in a variety of configurations, such as onsite private clouds or offsite public or private clouds.

Caution

If you use offsite public cloud storage, you should encrypt the backup.

Choosing the Right Backup Method

It is not easy to choose the right backup method. To start the process, a disaster recovery team must consider the length of outage the organization can endure and how current the restored information must be:

- **Recovery point objective (RPO)**: This metric indicates how much data an organization can afford to lose. The greater the RPO, the more tolerant the process is to interruption.

- **Recovery time objective (RTO)**: This metric specifies the maximum acceptable time to recover the data. This same metric would be used to evaluate the application that stores the data or the time it would take to transfer the data to the alternate site. The goal for disaster recovery planning would be to determine the time it would take to get the data up and running, whether at the primary site or an alternate site. The greater the RTO, the longer the recovery process can take; an organization that can tolerate interruption can handle a larger RTO.

Figure 8.11 illustrates how RPO and RTO can be used to determine acceptable downtime.

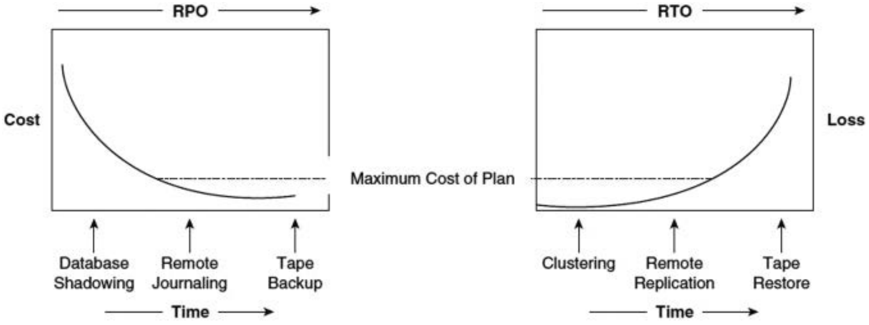


FIGURE 8.11 RPO and RTO

ExamAlert

For the CISSP exam, you must know the terms RPO and RTO.

The RPO and RTO metrics are very important. What you should realize about them both is that the lower the time requirements are, the higher the maintenance cost will be to provide for reduced restoration capabilities. For example, most banks have a very small RPO because they cannot afford to lose any processed information. Think of the recovery strategy calculations as being designed to meet the required recovery time frames. You can calculate maximum tolerable downtime (MTD) as follows:

MTD = RTO + WRT

where WRT is the work recovery time, which is simply the remainder of the MTD used to restore all business operations (see Figure 8.12).

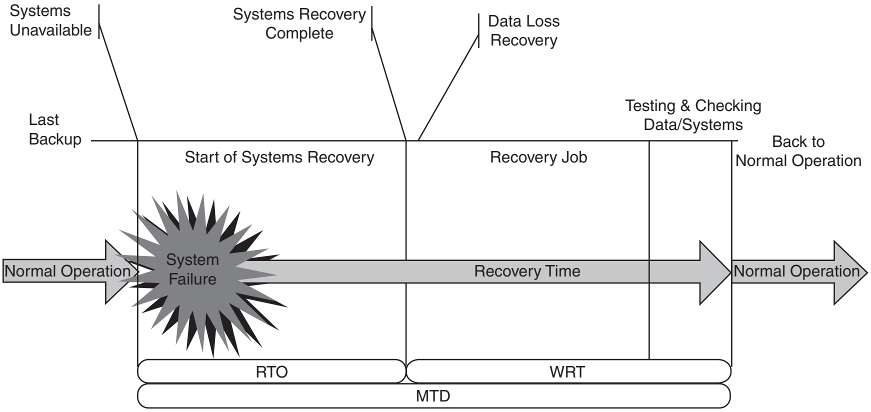


FIGURE 8.12 **MTD, RTO, and WRT**

Plan Design and Development

After determining the RPO and the RTO, the next phase of the business continuity planning process is plan design and development. In this phase, the team designs and develops a detailed plan for the recovery of critical business systems. The plan should focus on major catastrophes and what to do in the event that the entire facility is destroyed. If the organization can handle these types of events, less severe events that render the facility unusable for a time can be readily dealt with.

A business continuity plan (BCP) should include information on both long-term and short-term goals and objectives. In creating the plan, the business continuity planning team should follow these steps:

1. Identify time-sensitive critical functions and priorities for restoration.
2. Identify support systems needed by time-sensitive critical functions.
3. Estimate potential outages and calculate the minimum resources needed to recover from the catastrophe.
4. Select recovery strategies and determine which vital personnel, systems, and equipment will be needed to accomplish the recovery. (There must be a team for the primary site and the alternate site.)
5. Determine who will manage the restoration and testing process.
6. Determine what type of funding and fiscal management are needed to accomplish these goals.

The plan should also detail how the organization will contact and mobilize employees, provide for ongoing communication between employees, interface with external groups and the media, and provide employee services. The following sections discuss these processes.

Personnel Mobilization

The process for contacting employees in the event of an emergency needs to be worked out before a disaster. The process chosen depends on the nature and frequency of the emergency. *Outbound dialing systems* and *call trees* are widely used. An outbound dialing system stores the numbers to be called in an emergency. These systems can provide various services, including the following:

- **Call rollover**: If one number gets no response, the next is called.
- **Leave a recorded message**: If an answering machine answers, a message can be left for the individual.
- **Request a call back**: Even if a message is left, the system will continue to call back until the user calls in to the predefined phone number.

A call tree is a communication system in which the person in charge of the tree calls a lead person on each "branch," who in turn calls all the "leaves" on that branch. If call trees are used, the team should verify that there is a feedback mechanism built in. For example, the last person on any branch of the tree may call and confirm that he or she got the message. This can help ensure that everyone has been contacted. Call trees can be automated with VoIP and public switched telephone networks (PSTNs) and online services.

Personnel mobilization can also be triggered by emails to tablets, smartphones, and so on. Such systems require the email server to be functioning.

It is also important to plan for executive succession planning. An organization needs to be able to continue even if key personnel are not available. The organization should have measures in place that account for the potential loss of key individuals. If there is no executive succession planning, the loss of key individuals could mean the organization may not be able to continue.

Interface with External Groups

A public affairs officer (PAO) typically decides how to interact with external groups. Such interactions can affect the long-term reputation of your business. Damaging rumors can easily start, and it is important to have protocols in place for dealing with incidents, accidents, and catastrophes. An organization must decide how to deal with response teams, the fire department, the police department, and ambulance and other emergency response personnel. If you do not tell the public what you want them to know, the media will decide for you, or your employees or former employees may use social media to spread messages you may not want out there; therefore, it is important to have a policy and craft a statement for your PAO.

A media spokesperson should be identified to deal with the media. Negative public opinion can be costly. It is important to have a properly trained spokesperson to speak for and represent the organization. This person must be in the communication path to have the facts before speaking or meeting with the press. He or she should engage with senior management and legal counsel prior to making any public statements.

During a crisis, an organization should meet with the media only after adequately preparing. The organization's plan should include generic communications that address each possible incident. The spokesperson also needs to know how to handle tough questions. Liability should never be assumed; the spokesperson should simply state that an investigation has begun. Tackling tough issues up front will enable an organization to create a preapproved framework to call on if a real disaster occurs.

Employee Services

Organizations have some responsibilities to employees and to their families: Paychecks must continue, and employees need to be taken care of. Employees must be trained in what to do in the event of emergencies and in what they can expect from the organization. Insurance and other necessary services must continue.

> **Caution**
>
> The number-one priority of any business continuity or disaster recovery plan is to protect the safety of humans.

Before a disaster occurs, senior management must determine who will be in charge during a disaster to avoid chaos and confusion. Employees must know what is expected of them and who is in charge. It is important to make the decision before an adverse event occurs and record it in policy. It is also important to specify a succession of command because people may die during a disaster.

Someone in an organization must have the authority to allocate emergency funding when needed. In addition, controls must be in place to ensure that funds are not misappropriated.

Insurance

Insurance is one option that organizations can consider implementing to eliminate a portion of the risk uncovered during the BIA. Just as individuals can purchase insurance for a host of reasons, organizations can purchase protection insurance. An organization may purchase hacker or cyber insurance (which might include potential penalties and fines) and insurance for outages and business interruptions, and it may purchase insurance that covers the following assets:

- Data centers
- Software
- Documents, records, and important papers
- Errors and omissions
- Media transportation

Insurance is not without drawbacks. Insurance often involves high premiums, delayed claim payouts, denied claims, and problems proving real financial loss. Also, most insurance policies pay for only a percentage of any actual loss and do not pay for lost income, increased operating expenses, or consequential loss. It is also important to note that many insurance companies will not ensure organizations that have not exercised due care in the implementation of disaster recovery and business continuity plans.

Implementation

When the business continuity planning team finishes developing its plan, it is ready to submit a completed plan for implementation. A BCP is a result of all information gathered during the project initiation, the BIA, and the recovery strategies phase. A final checklist for completeness ensures that the plan addresses all relevant factors, including the following:

- The type of funding and fiscal management needed to accomplish the stated goals
- The procedures for declaring a disaster and under what circumstances this will occur

- Evaluation of potential disasters and the minimum resources needed to recover from various catastrophes
- Critical functions and priorities for restoration
- The recovery strategy and equipment that will be needed to accomplish the recovery
- Individuals who are responsible for each function in the plan
- The individual(s) who will manage the restoration and testing process

The completed BCP should be presented to senior management for approval. References for the plan should be cited in all related documents so that the plan is maintained and updated whenever there is a change or update to the infrastructure. When senior management approves the plan, it must be released and disseminated to employees. Awareness training for the individuals who would be responsible for carrying out the plan is critical and will help ensure that everyone understands what their tasks and responsibilities are in the event of an emergency.

Awareness and Training

It is important to ensure that all employees as well as internal and external personnel involved in the BCP, including contractors and consultants, know what to do in the event of an emergency. Although you will certainly require support from external agencies, such as law enforcement, if a disaster occurs, they are not likely to have time to participate in your training; however, having a face-to-face meeting with them and getting to know them prior to a disaster is a good idea so that you understand their resources and capabilities.

If employees are untrained, they might simply stop what they're doing and run for the door in the event of an emergency. Or, even worse, they might not leave when an alarm has sounded, even though the plan requires that they leave because of possible danger. Instructions should be written in easy-to-understand language that uses common terminology.

Caution

Although some organizations might feel that the business continuity planning is done when the plan is complete, it is important to remember that no demonstrated recovery exists until the plan has been tested.

Testing

The final phase of the business continuity planning process is to test and maintain the plan. Training and awareness programs are also developed during this phase. Testing a disaster recovery plan is critical. Without performing a test, there is no way to know whether the plan will work. Testing, which transforms theoretical plans into reality, should be repeated at least once a year.

Tests should start with the easiest parts of the plan and then build to more complex items. The initial tests should focus on items that support core processing, and they should be scheduled during a time that causes minimal disruption to normal business operations. As a CISSP candidate, you should be aware of the five different types of business continuity planning tests:

- **Checklist test**: Although it is not considered a replacement for a live test, a checklist test is a good first test. A checklist test is performed by sending copies of the plan to different department managers and business unit managers for review. Each recipient reviews the plan to make sure nothing has been overlooked.
- **Structured walkthrough**: This test, also known as a tabletop test, is performed by having the members of the emergency management team and business unit managers meet to discuss the plan. They walk through the plan line by line to see how an actual emergency would be handled and to discover discrepancies. Reviewing the plan in this way often makes errors and omissions apparent.

Tip

The primary advantage of a structured walkthrough is that it helps you discover discrepancies between different departments.

- **Simulation**: A simulation is a drill involving members of the response team acting in the same way they would if there were an actual emergency. This test proceeds to the point of recovery or to relocation to the alternate site. The primary purpose of this test is to verify that members of the response team can perform the required duties with only the tools they would have available in a real disaster.
- **Parallel test**: A parallel test is similar to a structured walkthrough but actually invokes operations at the alternate site. Operations at the new and old sites are run in parallel.

- **Full interruption test**: This type of test is the most detailed, time-consuming, and disruptive to a business. A full interruption test mimics a real disaster, and all steps are performed to complete backup operations. It includes all the individuals who would be involved in a real emergency, both internal and external to the organization. Although a full interruption test is the most thorough, it is also the scariest, and it can be so disruptive that it actually creates a disaster.

ExamAlert

For the CISSP exam, you need to know the differences between these test types. You should also know the advantages and disadvantages of each test.

The final step of the business continuity planning process is to combine all this information into the BCP and inter-reference it with the organization's other emergency plans. Although the organization will want to keep a copy of the plan onsite, there should be another copy offsite. If a disaster occurs, rapid access to the plan will be critical.

Caution

Access to the BCP should be restricted so that only those with a need to know can access the entire plan. In the wrong hands, a BCP could become a playbook for an attack.

Monitoring and Maintenance

When the testing process is complete, a few additional items still need to be considered. All the hard work that has gone into developing the plan can be lost if controls are not put in place to maintain the current level of business continuity and disaster recovery. Life is not static, and an organization's BCP should note be static either. The BCP should be a living document, subject to constant change.

To ensure that the BCP is maintained, you need to build in responsibility for the plan. You can do this using several vehicles:

- **Job descriptions**: Individuals responsible for the plan should have this responsibility detailed in their job descriptions. Management should work with HR to have this information added to the appropriate documents. To enforce a plan, you need to have someone to hold accountable.

- **Performance reviews**: The accomplishment (or lack of accomplishment) of appropriate plan maintenance tasks should be discussed in the responsible individual's periodic evaluations.
- **Audits**: The audit team should review the plan and make sure it is current and appropriate. The audit team should also inspect the offsite storage facility and review its security, policies, and configuration.

Table 8.8 lists the individuals responsible for specific parts of the business continuity planning process.

TABLE 8.8 **Business Continuity Planning Process Responsibilities**

Person or Department	Responsibility
Senior management	Project initiation, ultimate responsibility, overall approval, and support
Middle management or business	Identification and prioritization of critical systems unit managers
Business continuity planning committee and team members	Planning, day-to-day management, implementation, and testing of the plan
Functional business units	Plan implementation, incorporation, and testing

Disaster recovery implications for monitoring, maintenance, and recovery should be part of any discussions related to procuring new equipment, modifying current equipment, hiring key personnel, or making changes to the infrastructure. The best method to accomplish this is to add BCP review into all change management procedures. If changes to the approved plans are required, they must also be documented and structured using change management; the plan should be updated and distributed if even 10% of the plan, employees, or organization are affected by the change. A change control document should be kept with the plan at all times, and it should have good version control. A centralized command and control structure eases this burden.

Tip

Senior management is ultimately responsible for the BCP, including funding, project initiation, overall approval, and support.

Exam Prep Questions

1. You have been given an attachment that was sent to the head of payroll and was flagged as malicious. You have been asked to examine the malware, and you have decided to execute the malware inside a virtual environment. What is this environment called?

   ❍ **A.** Honeypot

   ❍ **B.** Hyperjacking

   ❍ **C.** Sandbox

   ❍ **D.** Decompiler

2. Which of the following is not a security or operational reason to use mandatory vacations?

   ❍ **A.** It allows the organization the opportunity to audit employee work.

   ❍ **B.** It ensures that the employee is well rested.

   ❍ **C.** It keeps one person from being able to easily carry out covert activities.

   ❍ **D.** It ensures that employees will know that illicit activities could be uncovered.

3. What type of control is an audit trail?

   ❍ **A.** Application

   ❍ **B.** Administrative

   ❍ **C.** Preventative

   ❍ **D.** Detective

4. Which of the following is not a benefit of RAID?

   ❍ **A.** Capacity benefits

   ❍ **B.** Increased recovery time

   ❍ **C.** Performance improvements

   ❍ **D.** Fault tolerance

5. Separation of duties is related to which of the following?

   ❍ **A.** Dual controls

   ❍ **B.** Principle of least privilege

   ❍ **C.** Job rotation

   ❍ **D.** Principle of privilege

6. Phreakers target which of the following resources?

   ❍ **A.** Mainframes

   ❍ **B.** Networks

   ❍ **C.** PBX systems

   ❍ **D.** Wireless networks

7. You recently emailed a colleague you worked with years ago. The email you sent him was rejected, and you have been asked to re-send it. What has happened with the message transfer agent?

   ❍ **A.** Whitelist

   ❍ **B.** Graylist

   ❍ **C.** Blacklist

   ❍ **D.** Black hole

8. Your organization has experienced a huge disruption. In this type of situation, which of the following is designed to take on operational capabilities when the primary site is not functioning?

   ❍ **A.** BCP

   ❍ **B.** Audit

   ❍ **C.** Incident response

   ❍ **D.** COOP

9. Which RAID type provides data striping but no redundancy?

   ❍ **A.** RAID 0

   ❍ **B.** RAID 1

   ❍ **C.** RAID 3

   ❍ **D.** RAID 4

10. Which of the following is the fastest backup option but takes the longest to restore?

    ❍ **A.** Incremental

    ❍ **B.** Differential

    ❍ **C.** Full

    ❍ **D.** Grandfathered

11. Which of the following types of intrusion detection systems compares normal to abnormal activity?

    ❍ **A.** Pattern-based IDS

    ❍ **B.** Statistical-based IDS

❍ **C.** Traffic-based IDS

❍ **D.** Protocol-based IDS

12. Which of the following processes involves overwriting data with zeros?

❍ **A.** Formatting

❍ **B.** Drive-wiping

❍ **C.** Zeroization

❍ **D.** Degaussing

13. What type of RAID provides a stripe of mirrors?

❍ **A.** RAID 1

❍ **B.** RAID 5

❍ **C.** RAID 10

❍ **D.** RAID 15

14. Which of the following is the name of a multidisk technique that offers no advantage in speed and does not mirror, although it does allow drives of various sizes to be used and can be used on two or more drives?

❍ **A.** RAID 0

❍ **B.** RAID 1

❍ **C.** RAID 5

❍ **D.** JBOD

15. You have been assigned to a secret project that requires a massive amount of processing power. Which of the following techniques is best suited for your needs?

❍ **A.** Redundant servers

❍ **B.** Clustering

❍ **C.** Distributed computing

❍ **D.** Cloud computing

16. Which of the following water sprinkler systems does not activate until triggered by a secondary mechanism?

❍ **A.** Dry pipe

❍ **B.** Wet pipe

❍ **C.** Pre-action

❍ **D.** Deluge

17. Which of the following is not a component of CPTED?

❍ **A.** Natural access control

❍ **B.** Natural reinforcement

❍ **C.** Natural surveillance

❍ **D.** Territorial reinforcement

18. The method of fire suppression used depends on the type of fire that needs to be extinguished. Which of the following fire-suppression methods does not suppress any of a fire's three key elements and led to the creation of the fire tetrahedron?

❍ **A.** CO_2

❍ **B.** Halon

❍ **C.** Water

❍ **D.** Dry-pipe system

19. Which of the following is the *best* answer that correctly describes the difference between MTBF and MTTR?

❍ **A.** MTBF is the estimated time that a piece of hardware, device, or system will operate before it fails. MTTR is an estimate of how long it will take to repair the equipment and get it back into use.

❍ **B.** MTBF is the time required to correct or repair a device in the event that it fails, and MTTR is the estimated time that a piece of hardware, device, or system will operate before it fails.

❍ **C.** MTBF is a value that can be used to compare devices to one another and also to determine the need for an SLA for a device and MTTR is the estimated time that a piece of hardware, device, or system will never fail before.

❍ **D.** There is no need for an organization to determine MTBF and MTTR for assets if it is located in an area where natural disasters such as hurricanes are not common.

20. Business continuity and disaster recovery planning is likely to be a very large, complex, and multidisciplinary process that brings together key associates within the organization. Which of the following *best* describes the role of senior management in this process?

❍ **A.** To plan for money for the disaster recovery project manager, technology experts, process experts, or other financial requirements from various departments in the organization

❍ **B.** To make disaster recovery planning a priority, commit and allow staff time for the process, and set hard dates for completion

❍ **C.** To manage the multidisciplinary team to keep all the team members all on the same page

❍ **D.** To be experts and understand specific processes that require special skill sets

21. Which of the following BCP tests carries the most risk?

- ❍ **A.** Full interruption test
- ❍ **B.** Parallel test
- ❍ **C.** Walkthrough
- ❍ **D.** Checklist test

22. Which of the following is the best description of what a software escrow agreement does?

- ❍ **A.** Provides a vendor with additional assurances that the software will be used per licensing agreements
- ❍ **B.** Specifies how much a vendor can charge for updates
- ❍ **C.** Gives an organization access to source code under certain conditions
- ❍ **D.** Provides a vendor access to an organization's code if there are questions of compatibility

23. Which of the following tape-rotation schemes involves using five sets of tapes, labeled A through E?

- ❍ **A.** Tower of Hanoi
- ❍ **B.** Son-father-grandfather
- ❍ **C.** Complex
- ❍ **D.** Grandfather-father-son

24. If the recovery point objective (RPO) is low, which of the following techniques would be the most appropriate solution?

- ❍ **A.** Clustering
- ❍ **B.** Database shadowing
- ❍ **C.** Remote journaling
- ❍ **D.** Tape backup

25. You have been assigned to the business recovery planning team responsible for backup options and offsite storage. Your organization is considering purchasing software from a small startup operation that has a proven record for unique software solutions. To mitigate the potential for loss, which of the following should you recommend?

- ❍ **A.** Clustering
- ❍ **B.** Software escrow
- ❍ **C.** Insurance
- ❍ **D.** Continuous backup

26. When developing a business continuity plan, what should be the number-one priority?

❍ **A.** Minimizing outage times

❍ **B.** Mitigating damage

❍ **C.** Documenting every conceivable threat

❍ **D.** Protecting human safety

Answers to Exam Prep Questions

1. **C.** A virtual environment where you can safely execute suspected malware is called a sandbox. Answer A is incorrect because a honeypot is a fake vulnerable system deployed to lure attackers. Answer B is incorrect because hyperjacking is a type of attack against a virtual system. Answer D is incorrect because a decompiler is used to disassemble an application.
2. **B.** Mandatory vacations are not primarily for employee benefit but to better secure the organization’s assets. Answers A, C, and D are incorrect because they list valid reasons to use mandatory vacations: Mandatory vacations enable the organization to audit employee work, keep one person from being able to easily carry out covert activities, and ensure that employees will know that illicit activities could be uncovered.
3. **D.** Audit trails are considered a detective type of control. Answers A, B, and C are incorrect because audit trails are not application, administrative, or preventive controls.
4. **B.** RAID provides capacity benefits, performance improvements, and fault tolerance; therefore, answers A, C, and D are incorrect. Although RAID might reduce recovery time, it certainly won’t increase it.
5. **B.** Separation of duties is closely tied to the principle of least privilege. Separation of duties is the process of dividing duties so that more than one person is required to complete a task, and each person has only the minimum resources needed to complete the task. Answer A is incorrect because dual controls are implemented to require more than one person to complete an important task. Answer C is incorrect because job rotation is used to prevent collusion. Answer D is incorrect because the principle of privilege would be the opposite of what is required.
6. **C.** Phreakers target phone and voice (PBX) systems. Answer A is incorrect because phreakers do not typically target mainframes. Answer B is incorrect because hackers might target networks, but phreakers target phone systems. Answer D is incorrect because wireless war drivers or hackers, not phreakers, target networks.
7. **B.** Graylisting rejects any email sender that is unknown. Mail from a legitimate email server will be retransmitted after a period of time. This moves the graylisted email off the hold list and onto the whitelist and, at that time, places the email in the inbox of the receiving account. Whitelisting only approves what is on an allowed list, whereas blacklisting blocks specific items. Black holes silently discard or drop traffic without informing the source.
8. **D.** COOP is designed to take on operational capabilities when the primary site is not functioning. Business continuity plans generally focus on the continuation of business services in the event of any type of interruptions. Therefore, answers A, B, and C are incorrect.
9. **A.** RAID 0 provides data striping but no redundancy. Answers B, C, and D are incorrect because RAID 1 provides disk mirroring, RAID 3 provides byte-level striping with a dedicated parity disk, and a RAID 4 drive is considered a dedicated parity drive.

10. **A.** Incremental backup is the fastest backup option, but has the longest restoration time. Answers B, C, and D are incorrect: Grandfathered backup is not a valid answer, a differential backup takes less time overall but takes longer to restore, and a full backup takes the longest to perform, although it’s the fastest to restore.
11. **B.** A statistical-based IDS compares normal activity to abnormal activity. Pattern-, traffic-, and protocol-based IDSs do not; therefore, answers A, C, and D are incorrect.
12. **C.** Zeroization overwrites data with zeros. Answer A is incorrect because formatting does not remove any data from the file allocation table (FAT). Answer B is incorrect because drive-wiping writes patterns of ones and zeros. Answer D is incorrect because degaussing works by means of a magnetic field.
13. **C.** RAID 10 provides a stripe of mirrors. RAID 1 offers only striping. RAID 5 is seen as a combination of good, cheap, and fast because it provides data striping at the byte level, good performance, and good fault tolerance. RAID 15 is a combination of RAID 1 and RAID 5.
14. **D.** JBOD can use existing hard drives of various sizes, combined into one massive logical disk. There is no fault tolerance and no increase in speed. The only benefit of JBOD is that you can use existing disks, and if one drive fails, you lose the data on only that drive. Answers A, B, and C are incorrect because RAID 0, RAID 1, and RAID 5 do not match the description provided.
15. **B.** Clustering is a means of grouping computers and moving to a greater level of usability. Answer A is incorrect because a redundant server waits until it’s needed before being used. Answer C is incorrect because distributed computing is not centrally controlled and, therefore, should not be used for sensitive or classified work. Answer D is incorrect because placing sensitive information in the cloud can be problematic in terms of security.
16. **C.** A pre-action fire sprinkler system is a combination system. Pipes are initially dry, and they do not fill with water until a predetermined temperature is reached. Even then, the system does not activate until a secondary mechanism triggers. Answers A, B, and D are incorrect because they are triggered without a secondary mechanism.
17. **B.** Natural reinforcement is not a component of CPTED. CPTED comprises natural access control (answer A), natural surveillance (answer C), and territorial reinforcement (answer D). CPTED is unique in that it considers the factors that facilitate crime and seeks to use the proper design of a facility to reduce the fear and incidence of crime. At the core of CPTED is the belief that physical environments can be structured in such a way as to reduce crime.
18. **B.** Halon is unique in that it does not work in the same way as most fire-suppression agents. Halon interferes with the chemical reaction of a fire and led to the creation of the fire tetrahedron. The other answers are incorrect because water (answer C) removes one of the needed items for a fire, as does carbon dioxide (answer A). A dry-pipe system (answer D) is a water suppression system design and does not hold water continuously.
19. **A.** The MTBF is the lifetime of a device. The MTTR is the time that would be required to correct or repair a device in the event that it fails. Answer B is not the correct description. Answer C describes only part of the correct answer, as it is

only an estimate of the failure rate. Answer D is not correct because these values are not affected by natural disasters.

20. **B.** The best answer is B. If senior management does not fully support the DRP, the plan will likely fail. Answer A is not the best answer because it describes the roles of a budget manager or budget department. Answer C is not the best answer because it describes the roles of a project manager. Answer D is not the best answer as it describes the roles of a subject matter expert.

21. **A.** A full interruption is the test most likely to cause its own disaster. All the other answers listed are not as disruptive, so answers B, C, and D are incorrect.

22. **C.** A software escrow agreement allows an organization to obtain access to the source code of business-critical software if the software vendor goes bankrupt or otherwise fails to perform as required. Answer A is incorrect because an escrow agreement does not provide the vendor with additional assurances that the software will be used per licensing agreements. Answer B is incorrect because an escrow agreement does not specify how much a vendor can charge for updates. Answer D is incorrect because an escrow agreement does not address compatibility issues; it grants access to the source code only under certain conditions.

23. **A.** The Tower of Hanoi involves using five sets of tapes, labeled A through E. Set A is used every other day. Set B is used on the first non-A backup day and is used every 4th day. Set C is used on the first non-A or non-B backup day and is used every 8th day. Set D is used on the first non-A, non-B, or non-C day and is used every 16th day. Set E alternates with set D. Answer B is incorrect because son-father-grandfather is not the correct name of a backup type. Answer C is incorrect because complex does not refer to a specific backup type. Answer D is incorrect because grandfather-father-son includes four tapes for weekly backups, one tape for monthly backups, and four tapes for daily backups; this does not match the description in the question.

24. **D.** The RPO is the earliest point at which recovery can occur. If an organization has a low RPO, tape backup is acceptable because there is a low need to capture the most current data. If the backup occurs at midnight and the failure is at noon the next day, the organization has lost 12 hours of data. Answers A, B, and C are incorrect because each of these would be used when a higher RPO, or more current data, is required.

25. **B.** The core issue here is that the software provider is a small startup that may not be around in a few years. The organization must therefore protect itself so that it has access to the source code. An escrow agreement allows an organization to obtain access to the source code of business-critical software if the software vendor goes bankrupt or otherwise fails to perform as required. Answers A, C, and D are incorrect because clustering and continuous backup do nothing to provide the organization access to the source code should they cease to exist, and, while insurance is an option, the expense is not necessary if the organization has rights and access to the code in the event that something occurs.

26. **D.** The protection of human safety is always the number-one priority of a security professional. Answers A, B, and C are incorrect. Minimizing outages is important but not number one. Preventing damage is also important, but protection of human safety is number one. It not possible to identify and place a dollar amount on every conceivable threat.

Need to Know More?

Snort IDS: www.it.uu.se/edu/course/homepage/sakdat/ht05/assignments/pm/programme/Introduction_to_snort.pdf

Security operations resource protection: www.process.st/it-security-processes/

The Open Source Security Testing Methodology Manual: www.isecom.org/OSSTMM.3.pdf

Digital forensic tools: https://www.guru99.com/computer-forensics-tools.html

The evolution of firewalls: https://www.techrepublic.com/article/understand-the-evolution-of-firewalls/

Disaster recovery testing: www.enterprisestorageforum.com/backup-recovery/disaster-recovery-testing.html

Configuration management best practices: https://blog.inedo.com/configuration-management-best-practices

Duress alarms: https://alltronic.com.au/security-blog/how-does-a-duress-alarm-work

System resilience and fault tolerance: www.itperfection.com/cissp/security-operations-domain/system-resilience-high-availability-qos-and-fault-tolerance/

Xcopy Commands: https://www.lifewire.com/xcopy-command-2618103

Logging and monitoring best practices: https://www.dnsstuff.com/logging-monitoring-best-practices

CHAPTER 9

Software Development Security

Terms you'll need to understand:

- Acceptance testing
- Cohesion
- Coupling
- Tuple
- Polyinstantiation
- Inference
- Fuzzing
- Bytecode
- Database
- Buffer overflow

Topics you'll need to master:

- The role of security in the software development lifecycle
- Database design
- The Capability Maturity Model
- The steps of the development lifecycle
- How to determine the effectiveness of software security
- The impact of acquired software security
- Different types of application design techniques
- The role of change management
- The primary types of databases

Introduction

Software plays a key role in the productivity of most organizations, but in many cases, we must contend with bugs and vulnerabilities in software. If you were to buy a defective car that exploded in minor accidents, the manufacturer would be forced to recall the car. However, if you buy a buggy piece of software, you have little recourse: You could wait for a patch, buy an upgrade, or maybe just buy another vendor's product. Well-written applications are essential for good security. This chapter focuses on topics a security professional must know in order to apply security in the context of the CIA triad (confidentiality, integrity, and availability) to the software development lifecycle (SDLC), including programming languages, application design methodologies, change management, and database design.

Databases contain some of the most critical assets of an organization and are often targeted by hackers. As a security professional, you must understand design, security issues, control mechanisms, and common vulnerabilities of databases. In addition to protecting the corporation's database from attacks, a security professional must be sensitive to the interconnectivity of databases and the rise of large online cloud databases.

Integrating Security into the Development Lifecycle

As a security professional, you are not expected to be an expert programmer or understand the inner workings of a Python script. You must, however, know the overall environment in which software and systems are developed. You must understand and integrate security into the SDLC. You must also understand the software development process and be able to recognize whether adequate controls have been developed and implemented. It is important to keep in mind that it's always cheaper to build in security up front than it is to add it later. Organizations accomplish this by using a structured approach that offers a number of benefits:

- Minimizes risk
- Maximizes return on investment from using the software
- Establishes security controls so that the risk associated with using software is mitigated

New systems are created when new opportunities are discovered; organizations take advantage of these technologies to solve existing problems, accelerate business processes, and improve productivity. Although it's easy to see the need to incorporate security from the beginning of the process, the historical reality of design and development has been deficient in this regard. Most organizations are understaffed, and duties are not properly separated. Too often, inadequate consideration is given to the implementation of access-limiting controls from within a program's code.

Code that is not properly secured has exposure points and vulnerabilities. New technologies and developments such as cloud computing and the Internet of Things (IoT) have made using a structured, secure development process even more important than in the past. It is critical that development teams enforce a structured SDLC that has checks and balances and where security is considered from start to finish.

Avoiding System Failure

No matter how hard we plan, systems fail. Organizations must prepare for failures through the use of compensating controls that help limit the damage. Some examples of compensating controls are checks and application controls and fail-safe procedures.

Checks and Application Controls

The easiest way to minimize problems in the processing of data is to ensure that only accurate, complete, and timely inputs can occur. Even poorly written applications can be made more robust by adding controls that check limits, data formats, and data lengths; these controls provide *data input validation*. Controls verifying that data is only processed through authorized routines should be in place. These application controls should be designed to detect any problems and to initiate corrective action. If there are mechanisms in place that permit the override of these security controls, their use should be logged and reviewed. Table 9.1 lists some common types of controls.

TABLE 9.1 **Checks and Controls**

Check or Application Control	Description
Sequence check	Verifies that all sequence numbers fall within a specific series. For example, checks are numbered sequentially. If the day's first-issued check is number 120, and the last check is number 144, all checks issued that day should fall between those numbers, and none should be missing.
Limit check	Ensures that data to be processed does not exceed a predetermined limit. For example, if a sale item is limited to five per customer, sales over that quantity should trigger an alert.
Range check	Ensures that data is within a predetermined range. For example, a date range check might verify that any date input is after 01/01/2021 and before 01/01/2025.
Validity check	Looks at the logical appropriateness of data. For example, orders to be processed today should be dated with the current date.
Table lookups	Verifies that a data point matches a data point in a set of values entered into a lookup table.
Existence check	Verifies that all required data is entered and appropriate.
Completeness check	Ensures that all required data has been added and that no fields contain null values.
Duplicate check	Ensures that a transaction is not a duplicate. For example, before a payment is made on invoice 833 for $1,612, accounts payable should verify that invoice number 833 has not already been paid.
Logic check	Verifies logic between data fields. For example, if Michael lives in Houston, his zip code cannot be the Dallas zip code 76450.

Failure States

Because all applications can fail, it is important that developers create mechanisms for safe failure with damage contained. Well-coded applications have built-in recovery procedures that are triggered if failure is detected; to protect a system from compromise, services can be terminated and systems can be disabled until the cause of failure can be investigated.

Tip

Systems that recover into a fail-open state are open to compromise as an attacker could easily strike. Systems should not typically fail open because of the security risk. However, some intrusion detection systems/intrusion prevention systems (IDSs/IPSs) go into fail-open state to prevent disruption of traffic.

The Software Development Lifecycle

The software development lifecycle (SDLC), also referred to as the system development lifecycle, is a framework for system development that can facilitate and structure the development process. It describes a process for planning, creating, testing, and deploying an information system. The National Institute of Standards and Technology (NIST) defines the SDLC in NIST SP 800-34 as "the scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation."

Many other framework models exist, such as the Microsoft Security Development Lifecycle (SDL), which consists of the phases training, requirements, design, implementation, verification, release, and response. Although the stages and specific terms vary from one framework to the next, security concerns should be integrated into every stage. The overall goal is the same: to control the development process and add security at each level or stage of the process.

The SDLC has seven distinct stages:

1. Project initiation
2. Functional requirements and planning
3. Software design specifications
4. Software development and build
5. Acceptance testing and implementation
6. Operational/maintenance
7. Disposal

ExamAlert

Read all CISSP exam questions carefully to make sure you understand the context in which SDL, SDLC, and other terms are being used.

Regardless of the names that a given framework might assign to the various steps, the goal of a framework is to provide security in the software development lifecycle. The failure to adopt a structured development model increases a product's risk of failure, and it is likely that the final product will not meet the customer's needs. Table 9.2 describes the stages of development and the activities that occur in each phase.

TABLE 9.2 **SDLC Stages and Activities**

Stage	Description	Activities
1	Project initiation	Determine project feasibility, cost, and benefit analysis Conduct payback analysis Establish a preliminary project timeline Conduct risk analysis
2	Functional requirements and planning	Define the need for the solution Identify the requirements Review proposed security controls
3	Software design specifications	Develop detailed design specifications Review support documentation Examine adequacy of security controls
4	Software development and build	Develop code Check modules
5	Acceptance testing and implementation	Enforce separation of duties Perform testing
6	Operational/maintenance	Release into production Perform certification and accreditation
7	Disposal	At end of life, remove data from system or application and then from production Define the level of sanitization and destruction of unneeded data that is appropriate for classification

Project Initiation

The project initiation stage usually involves a meeting that includes everyone involved with the project to answer big questions like What are we doing? Why are we doing it? and Who is our customer? At this meeting, the feasibility of the project is considered. The cost of the project must be discussed, as well as the potential benefits that the product is expected to bring to the system's users. A *payback analysis* should be performed to determine how long the project will take to pay for itself. In other words, the payback analysis determines how much time will lapse before accrued benefits overtake accrued and continuing costs.

If the decision is to move the project forward, the team should develop a preliminary timeline. Discussions should be held to determine the level of risk involved with handling data and to establish the ramifications of accidental exposure. This activity clarifies the precise type and nature of information that will be processed, as well as its level of sensitivity. This first look at security must be completed before the functional requirements and planning stage begins.

ExamAlert

For the CISSP exam, you should understand that users should be brought into the process as early as possible. You are building something for them and must make sure that the designed system/product meets their needs.

Functional Requirements and Planning

The functional requirements and planning phase is the time to fully define the need for the solution and map how the proposed solution meets the need. This stage requires the participation of management as well as users. Users need to identify requirements and desires they have regarding the design of the application. Security representatives must verify the identified security requirements and determine whether adequate security controls are being defined.

An *entity relationship diagram* (*ERD*) is often used to help map the identified and verified requirements to the needs being met. An ERD defines the relationship between the many elements of a project. An ERD is similar to a database, grouping together like data elements. Each entity has a specific attribute, called the *primary key*, which is drawn as a rectangular box containing an identifying name. Relationships, drawn as diamonds, describe how the various entities are related to each other.

Figure 9.1 shows the basic design of an ERD. An ERD can be used to help define a data dictionary. After the data dictionary is designed, the database schema is developed to further define tables and fields and the relationships between them. The completed ERD becomes the blueprint for the design and is referred to during the design phase.

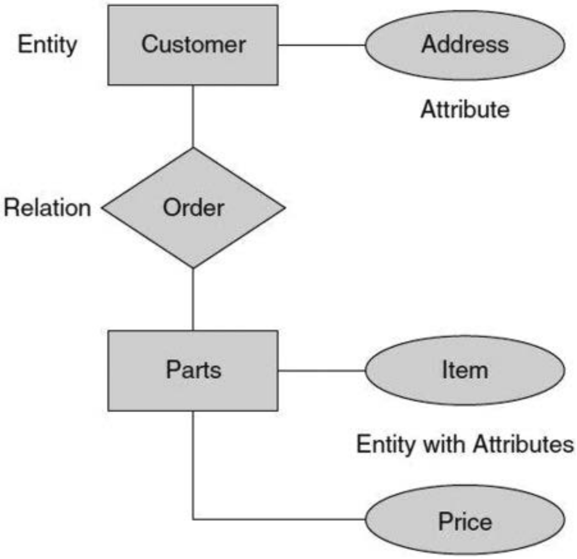


FIGURE 9.1 **Entity Relationship Diagram**

Software Design Specifications

Detailed design specifications can be generated either for a program that will be created or in support of the acquisition of an existing program. All functions and operations are described during the software design specifications stage. Programmers design screen layouts and create process diagrams. Supporting documentation is also generated. The output of the software design specifications stage is a set of specifications that delineates the new system as a collection of modules and subsystems.

Scope creep—the expansion of the scope of the project—most often occurs during this stage. Small changes in the design can add up over time. Although little changes might not appear to have big costs or impacts on the schedule of a project, these changes can have a cumulative effect and increase both the length and cost of the project.

Proper detail at this stage plays a large role in the overall security of the final product. Security should be the focus here as controls are developed to ensure input, output, audit mechanisms, and file protection. Sample input controls include dollar counts, transaction counts, error detection, and correction. Sample output controls include validity checking and authorization controls.

Software Development and Build

During the software development and build stage, programmers work to develop the application code specified in the previous stage, as illustrated in Figure 9.2.

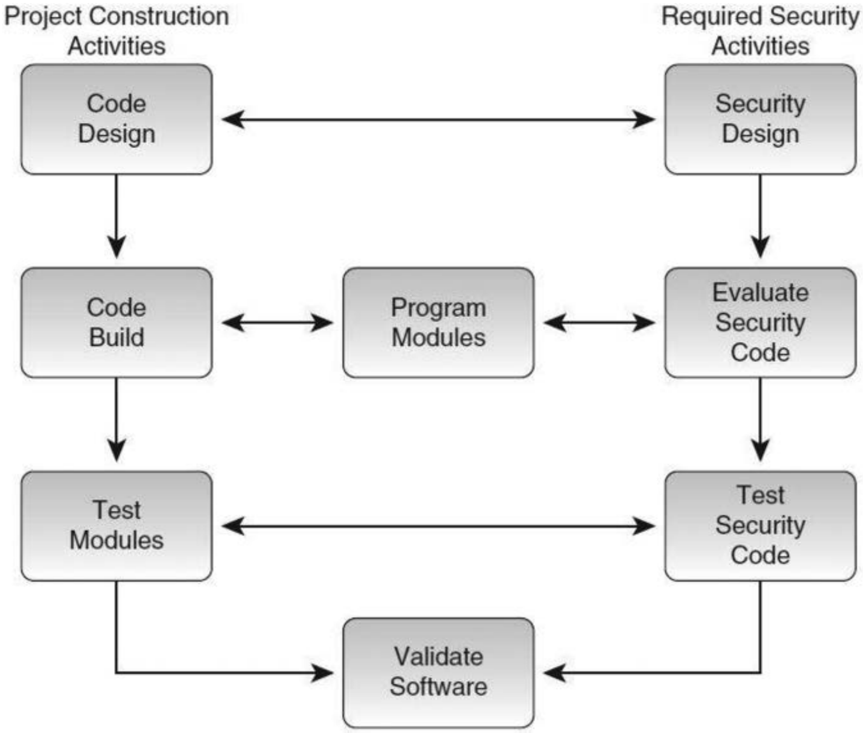


FIGURE 9.2 **Development and Build Stage Activities**

Programmers should strive to develop modules that have high cohesion and low coupling. *Cohesion* refers to the ability of a module to perform a single task with low input from other modules. *Coupling* refers to the interconnections or dependencies between modules. Low coupling means that a change to one module should not affect another, and the module has high cohesion.

Tip

Sometimes you may not actually need to build software because purchasing a previously developed product is easier. In such situations, you still need to consider security. You need to fully test the acquired software to verify its security implications. With purchased software, the source code might not be available, and you may need to perform other types of testing.

This stage includes testing of the individual modules developed, and accurate results have a direct impact on the next stage: integrated testing with the main program. *Maintenance hooks* are sometimes used at this point in the process to allow programmers to test modules separately without using normal access control procedures. It is important that these maintenance hooks, also referred to as *backdoors*, be removed before the software code goes to production. Programmers might use online programming facilities to access the code directly from their workstations. Although this typically increases productivity, using online facilities and leaving maintenance hooks in place increases the risk that someone will gain unauthorized access to the program library.

ExamAlert

For the CISSP exam, you should understand that separation of duties is of critical importance during the SDLC process. Activities such as development, testing, and production should be properly separated, and duties should not overlap. For example, programmers should not have direct access to production (or released) code or have the ability to change production or released code.

Caution

Maintenance hooks, or backdoors, are software mechanisms that are installed to bypass the system's security protections during the development and build stage. To prevent a potential security breach, these hooks must be removed before a product is released into production. As an example, The TextPortal application did not remove a maintenance hook, and it therefore had a weakness that could have enabled an attacker to obtain unauthorized access (see www.securityfocus.com/bid/7673/discuss). With this application, the undocumented password god2 could be used for the default administrative user account.

Several types of controls should be built into a program during this stage:

- **Preventive controls**: These controls include user authentication and data encryption.
- **Detective controls**: These controls provide audit trails and logging mechanisms.
- **Corrective controls**: These controls add fault tolerance and data integrity mechanisms.

Three types of testing can be used to validate the security of the application:

- **Unit testing**: This type of testing examines an individual program or module.
- **Interface testing**: This type of testing examines hardware or software to evaluate how well data can be passed from one entity to another.
- **System testing**: This series of tests starts in this phase and continues into the acceptance testing phase. It includes recovery testing, security testing, stress testing, volume testing, and performance testing.

Caution

Reverse engineering can be used to reduce development time. However, reverse engineering is somewhat controversial because it can be used to bypass normal access control mechanisms or disassemble another organization's program illegally. Most software licenses make it illegal to reverse engineer the associated code. In addition, laws such as the Digital Millennium Copyright Act (DMCA) can also prohibit the reverse engineering of code.

Acceptance Testing and Implementation

The acceptance testing and implementation stage, which occurs when the application coding is complete, should not be performed by the programmers who created the code. Instead, testing should be performed by test experts or quality assurance engineers. An important concept here is separation of duties. If the code were built and verified by the same individuals, errors might be overlooked, and security functions might be bypassed.

You need to conduct this stage of the SDLC even when acquiring software instead of building your own. If you acquire software, you must assess the security impact of the software. You should have in place a software assurance policy that defines the software acquisition process:

- Planning
- Procurement and contracting
- Implementation and acceptance
- Follow-on

Note

Because usability, not security, is typically the central goal with a purchased piece of software, it is critical that security be included in a product specification.

Models vary greatly on specifically what tests should be completed and how much, if any, iteration is necessary within that testing. Table 9.3 lists some common types of acceptance and verification tests of which you should be aware.

TABLE 9.3 **Acceptance and Verification Test Types**

Test Type	Description
Alpha test	This type of test is used to evaluate the first and earliest version of a completed prerelease application.
Pilot/beta test	This type of test is used to evaluate and verify the functionality of a prerelease application with limited users on limited production systems.
Whitebox test	This type of test verifies the inner program logic; it can be cost-prohibitive for large applications or systems.
Blackbox test	This is a type of integrity-based testing that looks at inputs and outputs but not the inner workings.
Function test	This type of test validates an application against a checklist of requirements.
Regression test	This type of test is used after a change is made to verify that inputs and outputs are correct and that interconnected systems show no abnormalities in how subsystems and processes are affected by the change.
Parallel test	This type of test is used to verify a new or changed application by feeding data into the new application and simultaneously into the old, unchanged application and comparing the results.
Sociability test	This type of test verifies that the application can operate in its targeted environment.
Final test	This type of test is usually performed after project staff are satisfied with all other tests and just before the application is ready to be deployed.

When all pertinent issues and concerns have been worked out between the QA engineers, the security professionals, and the programmers, an application is ready for deployment.

ExamAlert

For the CISSP exam, you should understand that fuzzing is a form of blackbox testing that involves entering malformed data inputs and monitoring the application's response. Fuzzing is commonly referred to as "garbage in, garbage out" testing because it throws "garbage" at the application to see what it can handle.

Operations/Maintenance

During the operations/maintenance phase, an application is prepared for release into its intended environment. This is the final opportunity to assess the effectiveness of the software's security. Logging ensures accountability and nonrepudiation, and it facilitates audits. Some guidelines and best practices for logging include NIST SP 800-92 and the Open Web Application Security Project (OWASP) Cheat Sheet on logging.

This is the stage where final user acceptance is performed, and any required certification and/or accreditation is achieved. It is also the stage at which management accepts the application and agrees that it is ready for use.

Certification requires a technical review of a system or an application to ensure that it does what it is supposed to do. Certification testing often includes an audit of security controls, a risk assessment, and/or a security evaluation. Typically, the results of certification testing are compiled into a report that becomes the basis for *accreditation*, which is management's formal acceptance of a system or an application. Management might request additional testing, ask questions about the certification report, or simply accept the results. When the system or application is accepted, a formal acceptance statement is usually issued.

Tip

Certification is a technical evaluation and analysis of the security features and safeguards of a system or an application to establish the extent to which the security requirements are satisfied and vendor claims are verified.

Accreditation is a formal process in which management officially approves the certification.

Operations management begins when an application is rolled out. Maintenance, support, and technical response must be addressed. Data conversion might also need to be considered. If an existing application is being replaced, data from the old application might need to be migrated to the new application. The rollout of the application might occur all at once or in a phased manner over time. Changeover techniques include the following:

- **Parallel operation**: The old and new applications are run simultaneously, with all the same inputs, and the results between the two applications are compared. Fine-tuning can be performed on the new application as needed. As confidence in the new application improves, the old application can be shut down. The primary disadvantage of this method is that both applications must be maintained for a period of time.
- **Phased changeover**: With a large application, a phased changeover might be possible. With this method, applications are upgraded one piece at a time.
- **Hard changeover**: This method establishes a date on which users are forced to change over. The advantage of a hard changeover is that it forces all users to change at once. However, it introduces a level of risk into the environment because things can go wrong.

Disposal

The disposal stage of the SDLC is reached when the application or system is no longer needed. Those involved in this stage of the process must consider how to dispose of the application securely, archive any information or data that might be needed in the future, perform disk sanitization (to ensure confidentiality), and dispose of equipment. This is an important step that is sometimes overlooked.

Disposal Is a Big Problem

Computer forensics investigators at the University of Glamorgan in the United Kingdom examined more than 100 drives purchased at random on eBay. All but 2 of the drives contained data. The other 98 drives contained various amounts of residual information. One contained psychological reports on schoolchildren, and several others contained different types of confidential information.

If hard drives are not destroyed, they should be wiped and sanitized. One standard is U.S. Department of Defense 5220.22-M, which recommends overwriting all addressable locations with a character, its complement, and then a random character to verify that the residual data has been cleared and sanitized.

Development Methodologies

A crucial part of system development is finding a good framework and adhering to the process it entails. The sections that follow explain several proven software development processes. Each of these models involves a predictable lifecycle. Each model has strengths and weaknesses. Some work well when a time-sensitive or high-quality product is needed, whereas others offer greater quality control and can scale to very large projects.

The Waterfall Model

Probably the most well-known software development process is the *waterfall model*. This model, which was developed by Winston Royce in 1970, operates as the name suggests, progressing from one level down to the next. An advantage of the waterfall method is that it provides a sense of order and is easily documented.

The original waterfall model prevented developers from returning to stages once they were complete; the process flowed logically from one stage to the next. Modified versions of the model are common today, including the V-shaped methodology shown in Figure 9.3.

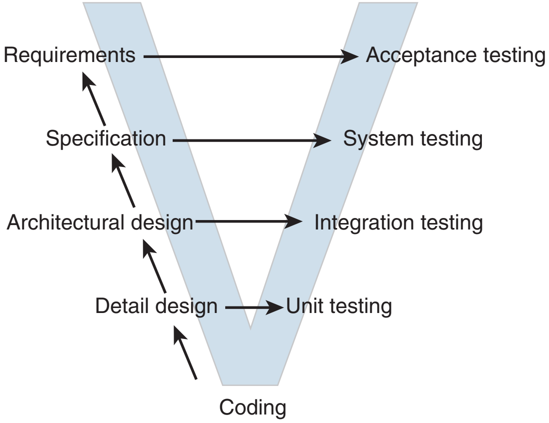


FIGURE 9.3 **The V-Shaped Modified Waterfall Model**

In the V-shaped model, instead of moving down only, the process steps are bent upward after the coding phase, to form the V shape for which the model is named. The V-shaped model requires testing during the entire development process. It is best used with projects that are small in scope. The primary disadvantage is that it does not work for large and complex projects because it does not allow for much revision.

The Spiral Model

In the spiral model, which was developed in 1988 by Barry Boehm, each phase starts with a design goal and ends with the client review. The client can be either internal or external and is responsible for reviewing progress. Analysis and engineering efforts are applied at each phase of the project.

An advantage of the spiral model is that it takes risk very seriously. Each phase of a project contains its own risk assessment, and each time a risk assessment is performed, the schedules and estimated cost to complete are reviewed, and a decision is made to continue or cancel the project. The spiral model works well for large projects. The disadvantage of this method is that it is much slower and takes longer to complete than the waterfall model. Figure 9.4 illustrates this model.

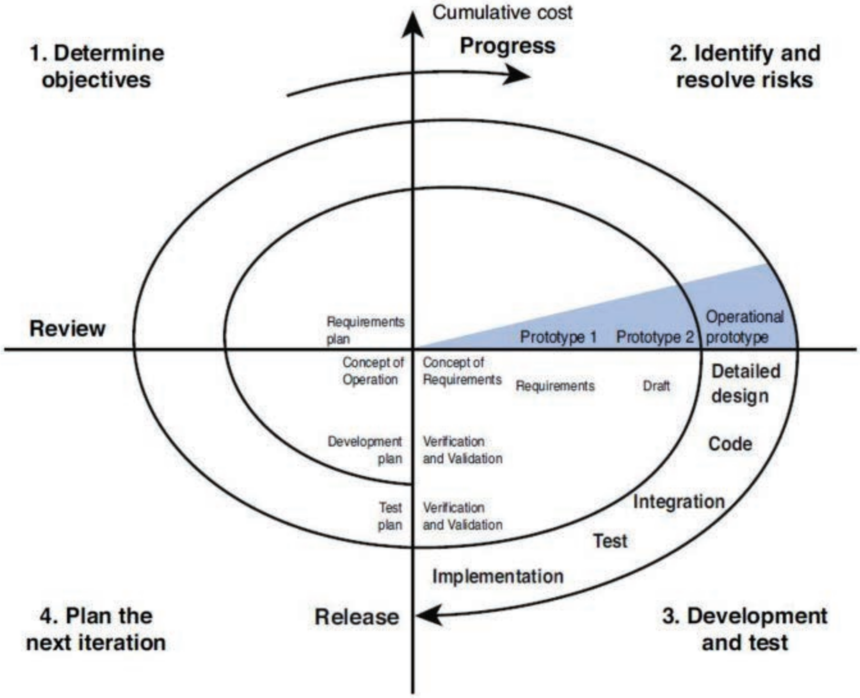


FIGURE 9.4 The Spiral Model

Joint Application Development (JAD)

Joint application development (*JAD*) is a process developed at IBM in 1977 that accelerates the design of information technology solutions. An advantage of JAD is that it helps developers work effectively with the users who will be using the applications developed. A disadvantage is that it requires users, expert developers, and technical experts to work closely together throughout the entire process. Projects that are good candidates for JAD have some of the following characteristics:

- Involve a group of users whose responsibilities cross department or division boundaries
- Are considered critical to the future success of the organization
- Involve users who are willing to participate
- Are developed in a workshop environment
- Use a facilitator who has no vested interest in the outcome

Rapid Application Development (RAD)

Rapid application development (*RAD*) is a fast application development process that delivers results quickly. RAD is not suitable for all projects, but it works well for projects that are on strict time limits. However, the decisions made quickly in RAD can lead to poor design and product. RAD is therefore not used for critical applications, such as shuttle launches. Two of the most popular RAD tools for Microsoft Windows are Delphi and Visual Basic.

Incremental Development

Incremental development is an approach that involves staged development of systems. Work is defined so that development is completed one step at a time. A minimal working application might be deployed, with subsequent releases to enhance functionality and/or scope.

Prototyping

Prototyping frameworks aim to reduce the time required to deploy applications. These frameworks use high-level code to quickly turn design requirements into application screens and reports that users can review. User feedback is gathered to fine-tune an application and improve it. Top-down testing works best with this development construct. Although prototyping clarifies user requirements, it also leads to the quick creation of a skeleton of a product with no guts surrounding it. Seeing complete forms and menus can confuse users and clients and lead to overly optimistic project timelines. Also, because change happens quickly, changes might not be properly documented, and scope creep might occur. Prototyping is often used for proprietary products being designed for specific customers.

ExamAlert

Prototyping is the process of building a proof-of-concept model that can be used to test various aspects of a design and verify its marketability. Prototyping is widely used during the development process.

Modified Prototype Model (MPM)

The modified prototype model (MPM) was designed to be used for web development. MPM focuses on quickly deploying basic functionality and then gathering user feedback to expand that functionality. MPM is especially useful when the final nature of the product is unknown.

Computer-Aided Software Engineering (CASE)

Computer-aided software engineering (CASE) enhances the SDLC by using software tools and automation to perform systematic analysis, design, development, and implementation of software products. The tools are useful for large, complex projects that involve multiple software components and lots of people. Its disadvantages are that it requires building and maintaining software tools and training developers to understand how to use the tools effectively. CASE can be used in the following cases:

- For modeling real-world processes and data flows through applications
- For developing data models to better understand processes
- For developing process and functional descriptions of models
- For producing databases and database management procedures
- For debugging and testing code

Note

There are many different approaches in software development. Some are new takes on old methods and others have adapted a relatively new approach. Lean software development is one example and is a translation of lean manufacturing principles and practices to the software development domain. Its main goal is continuous product improvement at all operational levels and stages.

Agile Development Methods

Agile software development allows teams of programmers and business experts to work together closely.

According to the agile manifesto (see agilemanifesto.org):

> We are uncovering better ways of developing software by doing it and helping others do it. Through this work, we have come to value:
>
> - Individuals and interactions over processes and tools.
> - Working software over comprehensive documentation.
> - Customer collaboration over contract negotiation.
> - Responding to change over following a plan.

Agile project requirements are developed using an iterative approach, and an agile project is mission driven and component based. Agile development may make use of an integrated product team (IPT), which is a multitalented group of people who are responsible for creating and delivering a specified process or product. IPTs should be formed to manage the development of individual product elements or sustainment processes. These teams should be empowered to make critical decisions. Popular agile development models include the following:

- **Extreme programming (XP)**: The XP development model requires that teams include business managers, programmers, and end users. These teams are responsible for developing usable applications in short time frames. One potential problem with XP is that teams are responsible not only for coding but also for writing the tests used to verify the code. In addition, there is minimal focus on structured documentation, and XP does not scale well for large projects.

- **Scrum**: Scrum is an iterative development method in which repetitions referred to as *sprints* typically last 30 days each. Scrum is typically used with object-oriented technology and requires strong leadership and a team that can meet at least briefly each day. The planning and direction of tasks passes from the project manager to the team. The project manager's main task is to work on removing any obstacles from the team's path. The scrum development method owes its name to the team dynamic structure of rugby.

Note

Toyota developed an efficient development methodology known as kanban that stresses the use of virtual walls to track the various activities the team is tracking. These walls are typically divided into three columns: Planned, In Progress, and Done.

Maturity Models

The *Capability Maturity Model* (*CMM*) was designed as a framework for software developers to improve the software development process. It allows software developers to progress from an anything-goes type of development to a highly structured, repeatable process. As software developers grow and mature, their productivity increases, and the quality of their software products becomes more robust. Through the standardization activities of ISO 15504, the CMM officially became the Capability Maturity Model Integration (CMMI) in 2007. The CMMI includes five maturity levels, as shown in Table 9.4.

TABLE 9.4 **CMMI Levels**

Maturity Level	Description
Initial	This is an ad hoc process with no assurance of repeatability.
Managed	Change control and quality assurance are in place and controlled by management, although formal processes are not defined.
Defined	Defined processes and procedures are in place and used. Qualitative process improvement is in place.
Quantitatively managed	Data is collected and analyzed. A process improvement program is used.
Optimizing	Continuous process improvement is in place and considered in the budget.

Note

The five levels of the CMMI, as shown in Figure 9.5, have similarities with agile development methods, such as XP and scrum. The CMMI contains process areas and goals, and each goal comprises practices.

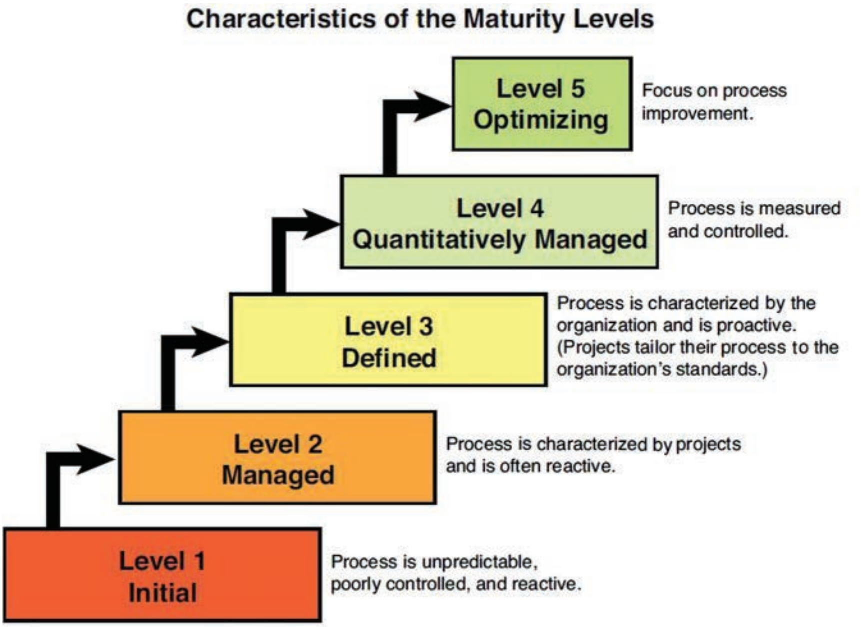

Characteristics of the Maturity Levels
Level 5
Optimizing
Focus on process improvement.
Level 4
Quantitatively Managed
Process is measured and controlled.
Level 3
Defined
Process is characterized by the organization and is proactive. (Projects tailor their process to the organization's standards.)
Level 2
Managed
Process is characterized by projects and is often reactive.
Level 1
Initial
Process is unpredictable, poorly controlled, and reactive.

FIGURE 9.5 The CMMI

Carnegie Mellon University introduced the IDEAL model for software process improvement. It is a process-improvement and defect-reduction methodology. Table 9.5 outlines the maturity levels of the IDEAL model.

TABLE 9.5 **IDEAL Model**

Maturity Level	Description
Initiating	Define the process improvement project.
Diagnosing	Identify the baseline of the current software development process.
Establishing	Define a strategic plan to improve the current software development process.
Acting	Implement the software process improvement plan.
Leveraging	Maintain and improve the software based on lessons learned.

Scheduling

Scheduling involves linking individual tasks. The link relationships are based on earliest start date or latest expected finish date. Gantt charts provide a way to display these relationships.

The *Gantt chart* was developed in the early 1900s as a tool to assist the scheduling and monitoring of activities and progress. Gantt charts show the start and finish dates of each element of a project. Gantt charts also show the relationships between activities in a calendar-like format. They have become some of the primary tools used to communicate project schedule information. The baseline of a Gantt chart illustrates what will happen if a task is finished early or late.

Program evaluation and review technique (PERT) is the preferred tool for estimating time when a degree of uncertainty exists. PERT uses a critical path method that applies a weighted average duration estimate.

PERT uses probabilistic time estimates to create a three-point—best, worst, and most likely time—evolution of activities. The PERT weighted average is calculated as follows:

$$\text{PERT weighted average} = \text{Optimistic time} + 4 \times \text{Most likely time} + \text{Pessimistic time} / 6$$

Every task branches out to three estimates:

- **One**: The most optimistic time in which the task can be completed.
- **Two**: The most likely time in which the task will be completed.
- **Three**: The worst-case scenario or longest time in which the task might be completed.

Change Management

Change management is a formalized process for controlling modifications made to systems and programs: analyze a request, examine its feasibility and impact, and develop a timeline for implementing the approved changes. The change management process provides all concerned parties with an opportunity to voice their opinions and concerns before changes are made. Although types of changes vary, change control follows a predictable process with the following typical steps:

1. Request the change.
2. Approve the change request.

3. Document the change request.
4. Test the proposed change.
5. Present the results to the change control board.
6. Implement the change, if approved.
7. Document the new configuration.
8. Report the final status to management.

Tip

One important piece of change management that is sometimes overlooked is a way to back out of the change. Sometimes things can go wrong, and a change needs to be undone.

DevOps is an example of a change management approach that uses agile principles. DevOps, which combines development and operations, includes the following elements:

- **Testability**: Develop/test against simulated production systems.
- **Deployability**: Deploy with automated processes that are iterative, repeatable, frequent, and reliable.
- **Monitorability**: Monitor the application to address issues early on.
- **Modifiability**: Allow for efficient feedback by creating effective communication channels.

Documentation is the key to a good change control process. Tracking should include receiving the request, evaluating the cost/benefit, and prioritizing the work of the developers and team. The system maintenance staff of the department requesting a change should keep a copy of that change's approval. Without a change control process in place, there is significant potential for security breaches. The following are indicators of poor change control:

- There is no formal change control process in place.
- Changes are implemented directly by the software vendors or others without internal control; this can indicate a lack of separation of duties.
- Programmers place code in an application that is not tested or validated.
- A change that is made was not authorized by the change review board.

- The programmer has access to both the object code and the production library; this situation presents a threat because the programmer might be able to make unauthorized changes to production code.
- Version control is not implemented.

In some cases, such as emergency situations, a change might occur without going through the change control process. These emergencies typically are in response to situations that endanger production or could halt a critical process. If programmers are to be given special access or provided with an increased level of control, the security professional with oversight should make sure that checks are in place to track those programmers' access and record any changes made.

Database Management

Databases are important to business and government organizations as well as to individuals because they provide a way to catalog, index, and retrieve related pieces of information and facts. These repositories of data are widely used. If you have booked a reservation on a plane, looked up the history of a used car you were thinking about buying, or researched the ancestry of your family, you have most likely used a database during your quest.

A database can be centralized or distributed, depending on the database management system (DBMS) that has been implemented. The DBMS allows the database administrator to control all aspects of the database, including design, functionality, and security. There are several popular types of database management systems:

- **Hierarchical database management system**: A hierarchical database links structures into a tree structure. Each record can have only one owner. Because of this, a hierarchical database often can't be used to relate to structures in the real world.
- **Network database management system**: This type of database system was developed to be more flexible than a hierarchical DBMS. The network database model is referred to as a *lattice structure* because each record can have multiple parent and child records.
- **Relational database management system**: A relational database consists of a collection of tables linked to each other by their primary keys. Many

organizations use this model. Most relational databases use SQL as their query language. A relational DBMS (RDBMS) is a collection based on set theory and relational calculations. This type of database groups data into ordered pairs of relationships (each pair consisting of a row and column) known as a tuple. The majority of modern databases are relational.

- **Object-relational database system**: This type of database system is similar to an RDBMS but is written in an object-oriented programming language. This allows it to support extensions to the data model and to be a middle ground between relational databases and object-oriented databases.

Database Terms

In case you are not familiar with the world of databases, this section provides a review of some common database-related terms that security professionals should be familiar with (see Figure 9.6):

- **Aggregation**: The process of combining several low-sensitivity items and drawing medium- or high-sensitivity conclusions.
- **Inference**: The process of deducing privileged information from available unprivileged sources.
- **Attribute**: A characteristic about a piece of information. Where a row in a database table represents a database object, each column in that row represents an attribute of that object.
- **Field**: The smallest unit of data within a database.
- **Foreign key**: An attribute in one table that cross-references to an existing value that is the primary key in another table.
- **Granularity**: Refers to the level of control a program has over the view of the data that someone can access. Highly granular databases make it possible to restrict views, according to the user's clearance, at the field or row level.
- **Relation**: A defined interrelationship between the data elements in a collection of tables.
- **Tuple**: A record used to represent a relationship among a set of values. In an RDBMS, a tuple identifies a column and a row.

- **Schema**: The totality of the defined tables and interrelationships for an entire database, which defines how the database is structured.
- **Primary key**: A key that uniquely identifies each row and assists with indexing a table.
- **View**: The database construct that an end user can see or access.

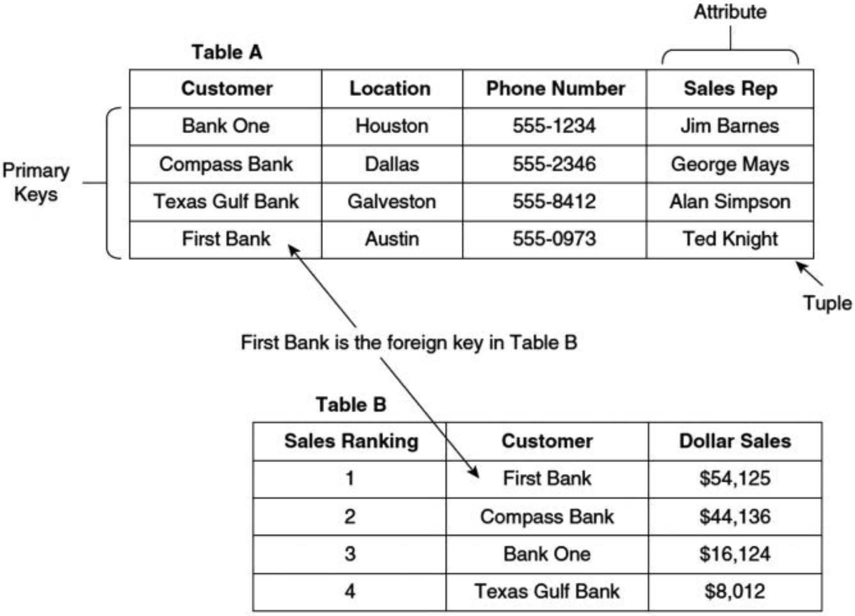


Table A

Customer	Location	Phone Number	Sales Rep
Bank One	Houston	555-1234	Jim Barnes
Compass Bank	Dallas	555-2346	George Mays
Texas Gulf Bank	Galveston	555-8412	Alan Simpson
First Bank	Austin	555-0973	Ted Knight

Table B

Sales Ranking	Customer	Dollar Sales
1	First Bank	$54,125
2	Compass Bank	$44,136
3	Bank One	$16,124
4	Texas Gulf Bank	$8,012

FIGURE 9.6 Illustration of Database Terms

An Example of Aggregation and Inference

Many students struggle with the concepts of aggregation and inference. The following are the two examples I use in the classroom to explain these concepts.

Aggregation refers to adding together available information. An aggregation attack is possible when pieces of information can be combined from different sources with different data classification levels to result in a composite view of data that exceeds the user's access. For example, when Mike was a teenager, he would tell his parents he was spending the night at his friend's house Friday night. His friend would tell his own parents that he was spending the night at Mike's house. This enabled Mike and his friend to stay out late until one parent called the other, at which point both were able to verify that Mike and his friend were at neither house.

Inference results from someone's ability to fill in gaps in the information provided. Inference is possible when retrieved, authorized information can be used to deduce new information. For example, consider a situation in HR, where an employee is authorized to see payroll as department totals only but is not authorized to see individual salaries. In fact, this employee might still be able to infer what someone is paid. If the employee can look at payroll totals the month before a new individual starts and then look at the total the month after the individual is hired, the difference allows the employee to draw an inference about the new individual's salary.

Integrity

The integrity of data refers to its accuracy. To protect the integrity of the data in a database, specialized controls are used, including rollbacks, checkpoints, commits, and savepoints. There are two types of data integrity:

- **Semantic integrity**: Assures that the data in any field is of the appropriate type. Controls that check for the logic of data and operations affect semantic integrity.

- **Referential integrity**: Assures the accuracy of cross-references between tables. Controls that ensure that foreign keys only reference existing primary keys affect referential integrity.

Transaction Processing

Transaction management is critical in assuring integrity. Without proper locking mechanisms, multiple users could be altering the same record simultaneously, and there would be no way to ensure that transactions were valid and complete. This is especially important with online systems that respond in real time. These systems, known as *online transaction processing* (*OLTP*) systems, are used in many industries, including banking, airlines, mail order, supermarkets, and manufacturing. Programmers involved in database management use the ACID test when discussing whether a database management system has been properly designed to handle OLTP:

- **Atomicity**: Results of a transaction are either all or nothing.

- **Consistency**: Transactions are processed only if they meet system-defined integrity constraints.

- **Isolation**: The results of a transaction are invisible to all other transactions until the original transaction is complete.

- **Durability**: Once a transaction is complete, the results of the transaction are permanent.

Database Vulnerabilities and Threats

Protecting databases is not an easy task. Database attacks are some of the most common attack vectors, and SQL injection has topped the OWASP list for more than 10 years. Many database security issues are directly attributed to poor development practices. As a security professional, you should understand the following common vulnerabilities and threats:

- **SQL injection**: This type of attack, typically caused by unsanitized input, allows the attacker to inject a SQL query via the input data from the client to the application.
- **Default, blank, or weak passwords**: Authentication credentials should be strong, and all weak and blank passwords removed.
- **Extensive privileges**: The level of access provided should be only what's needed to do the task. Administrator privileges should not be provided.
- **Broken configuration management**: Active measurement of the environment is required to detect undocumented changes, which typically reduce security.
- **Enabled features that are not needed**: It is important to remove, block, and disable all features that are not needed. Reducing the attack surface makes it harder for an attacker to succeed.
- **Privilege escalation**: This is a vulnerability in which an attacker gains an additional level of access.
- **Denial of service (DoS)**: A DoS attack may not give the attacker access, but it can disrupt normal operations and block others from accessing the database.
- **Unpatched database**: Unpatched systems are common vulnerabilities. Patching is a key component of security.
- **Unencrypted sensitive data**: Encryption is one of the key controls to protecting sensitive data.
- **Buffer overflow**: This is yet another common vulnerability. All data should have proper input validation done to ensure that the data is formatted correctly and with normal bounds of operation. (Buffer overflows are discussed later in this chapter.)

Tip

When you take the CISSP exam, be sure to read the questions closely as a single word can make an answer right or wrong. For example, *configuration* management is an active measurement of the environment to detect undocumented changes, whereas *change* management is a mandatory process that involves documenting planned changes to the environment.

Artificial Intelligence and Expert Systems

An *expert system* is a computer program that contains a knowledge discovery database, a set of rules, and an inference engine. This data mining technique can be used to discover nontrivial information and extract knowledge from a large amount of data. At the heart of such a system is the *knowledge base*—a repository of information against which the rules are applied.

Expert systems are typically designed for specific purposes and have the capability to infer. For example, a hospital might have a knowledge base that contains various types of medical information; if a doctor enters the symptoms weight loss, emotional disturbances, impaired sensory perception, pain in the limbs, and periods of irregular heart rate, the expert system can scan the knowledge base and diagnose the patient as suffering from beriberi.

Tip

How advanced are expert systems? A computer named Watson, created by IBM, can win at Jeopardy! and beat human opponents by looking for the answers in unstructured data using a natural query software language (see https://www.ibm.com/ibm/history/ibm100/us/en/icons/watson/).

The challenge in the creation of knowledge bases is to ensure that their data is accurate, that access controls are in place, that the proper level of expertise was used in developing the system, and that the knowledge base is secured.

Neural networks are networks that are capable of learning new information (see Figure 9.7). Artificial intelligence (AI) is possible thanks to the combination of expert systems and neural networks. Neural networks make use of multiple levels of nodes to filter data and apply weights; they mimic processes used by the human brain. Eventually, an output is triggered, and a fuzzy solution is provided. It’s called a fuzzy solution because it can lack exactness.

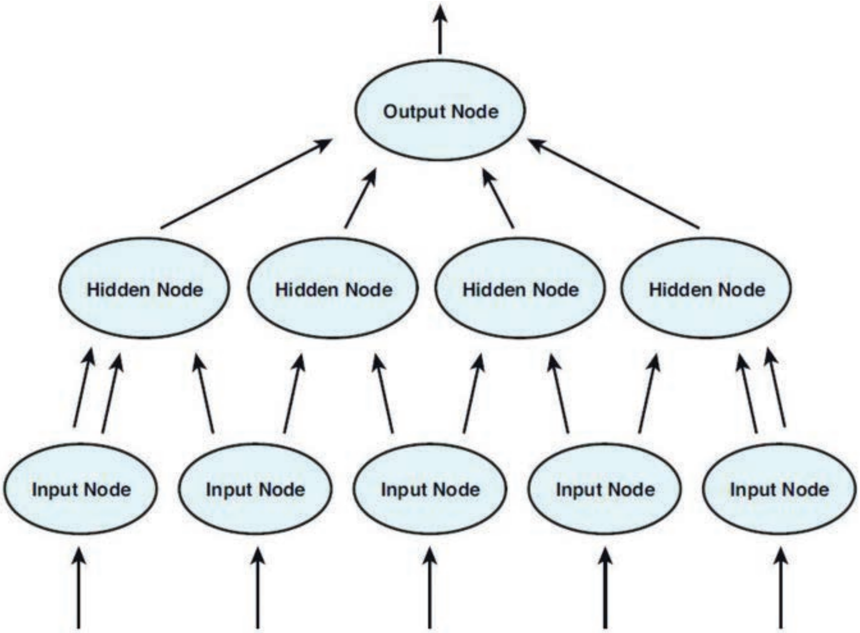


FIGURE 9.7 Artificial Neural Network

Programming Languages, Secure Coding Guidelines, and Standards

Programming languages permit the creation of instructions that a computer can understand. The types of tasks that get programmed and the instructions or code used to create a program depend on the nature of the organization. Programming has evolved through five generations of languages, as illustrated in Figure 9.8 and described in the list that follows:

- **Generation 1**: Machine language, the native language of a computer, consisting of binary ones and zeros.
- **Generation 2**: Assembly language, human-readable notation that translates easily into machine language.
- **Generation 3**: High-level programming language. The 1960s through the 1980s saw the emergence and growth of many third-generation languages (3GLs), such as Fortran, COBOL, C+, and Pascal.

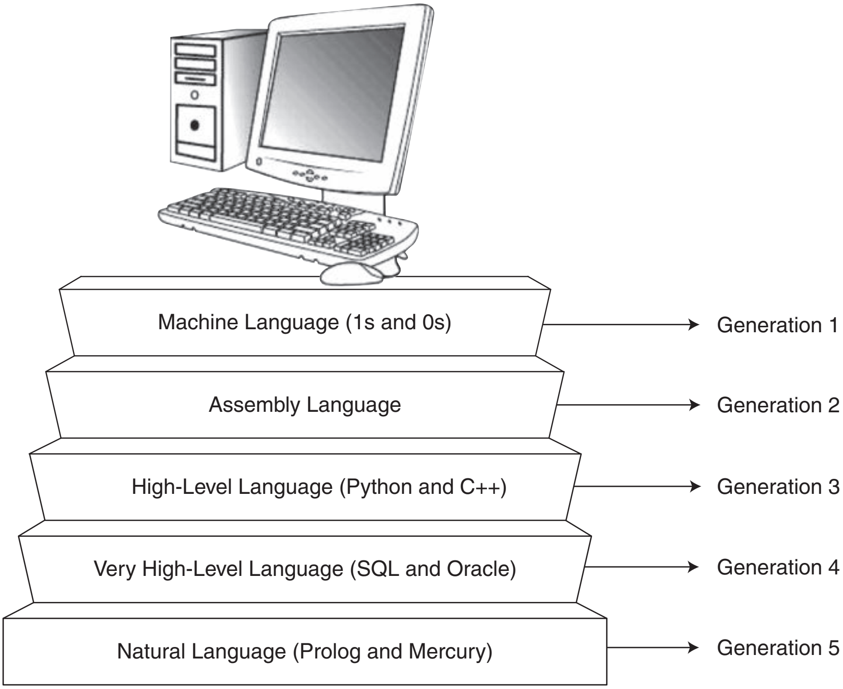

Machine Language (1s and 0s)
Generation 1
Assembly Language
Generation 2
High-Level Language (Python and C++)
Generation 3
Very High-Level Language (SQL and Oracle)
Generation 4
Natural Language (Prolog and Mercury)
Generation 5

FIGURE 9.8 **Programming Languages**

- **Generation 4**: Very high-level language. This generation of languages grew from the 1970s through the early 1990s. Fourth-generation languages (4GLs), such as SQL, are typically used to access databases.
- **Generation 5**: Natural language. Fifth-generation languages (5GLs) took off in the 1990s and were considered the wave of the future. 5GLs are categorized by their use of inference engines and natural language processing. Mercury and Prolog are two examples of fifth-generation languages.

After the code is written, it must be translated into a format that the computer will understand. These are the three most common methods:

- **Assembler**: An assembler translates assembly language into machine language.
- **Compiler**: A compiler translates a high-level language into machine language.

- **Interpreter**: Instead of compiling an entire program, an interpreter translates a program line by line. Interpreters have a fetch-and-execute cycle. An interpreted language is much slower to execute than a compiled or assembled program, but it does not need a separate compilation or assembly step.

Hundreds of different programming languages exist. Many have been written for specific niches or to meet market demands. The following are some examples of common programming languages:

- **ActiveX**: This language provides a foundation for higher-level software services, such as transferring and sharing information among applications. ActiveX controls are a Component Object Model (COM) technology. COM is designed to hide the details of an individual object and focus on the object's capabilities. An extension to COM is COM+.
- **C, C+, C++, and C#**: The C programming language, which replaced B, was designed by Dennis Ritchie. C was originally designed for UNIX and is very popular and widely used. From a security perspective, some C functions are known to be susceptible to buffer overflows.
- **HTML**: Hypertext Markup Language (HTML) is a markup language that is used to create web pages.
- **Java**: This is a general-purpose computer programming language, developed in 1995 by Sun Microsystems.
- **Visual Basic**: This programming language was designed to be used by anyone and enables rapid development of practical programs.
- **Ruby**: This object-oriented programming language was developed in the 1990s for general-purpose use. It has been used in the development of such projects as Metasploit.
- **Scripting languages**: A scripting language is a type of programming language that is usually interpreted rather than compiled and allows some control over a software application. Perl, Python, and Java are examples of scripting languages.
- **XML**: Extensible Markup Language (XML) is a markup language that specifies rules for encoding documents. XML is widely used on the Internet.

Object-Oriented Programming

Multiple development frameworks have been created to assist in defining, grouping, and reusing both code and data. Methods include data-oriented system programming, component-based programming, web-based applications, and object-oriented programming. Of these, the most commonly deployed is *object-oriented programming* (*OOP*), an object technology that grew from modular programming. OOP allows a programmer to reuse and interchange code between programs in modular fashion without starting over from scratch. It has been widely embraced because it is efficient and results in relatively low programming costs. Because OOP makes use of modules, a programmer can easily modify an existing program. Java and C++ are two examples of OOP languages.

In OOP, objects are grouped into classes, and all objects in a class share a particular structure and behavior. Characteristics from one class can be passed down to another through the process of inheritance. OOP relies on the following concepts:

- **Encapsulation**: This is the process of hiding the functionality of an object inside that object or, for a process, hiding the functionality inside that process's class. Encapsulation permits a developer to keep information disjointed—that is, to separate distinct elements so that there is no direct unnecessary sharing or interaction between the various parts.

- **Polymorphism**: In general, polymorphism means that one thing has the capability to take on many appearances or make copies of itself. In OOP, polymorphism is used to invoke a method on a class without needing to care about how the invocation is accomplished. Likewise, the specific results of the invocation can vary because objects have different variables that respond differently.

- **Polyinstantiation**: In general, polyinstantiation means that multiple instances of information are being generated. Polyinstantiation is used in many settings. For example, polyinstantiation is used to display different results to different individuals who pose identical queries on identical databases, due to those individuals possessing different security levels. It is widely used by the government and military to unify information bases while protecting sensitive or classified information. Without polyinstantiation, an attacker might be able to aggregate information from various sources to mount an inference attack and determine secret information. Initially, a piece of information by itself appears useless, like a piece to a puzzle, but when you put together several pieces of the puzzle, you begin to form an accurate picture.

Object-oriented design (OOD) is used to bridge the gap between a real-world problem and a software solution. OOD modularizes data and procedures, making it possible to provide a detailed description of how a system is to be built. Object-oriented analysis (OOA) and OOD are sometimes combined as object-oriented analysis and design (OOAD).

CORBA

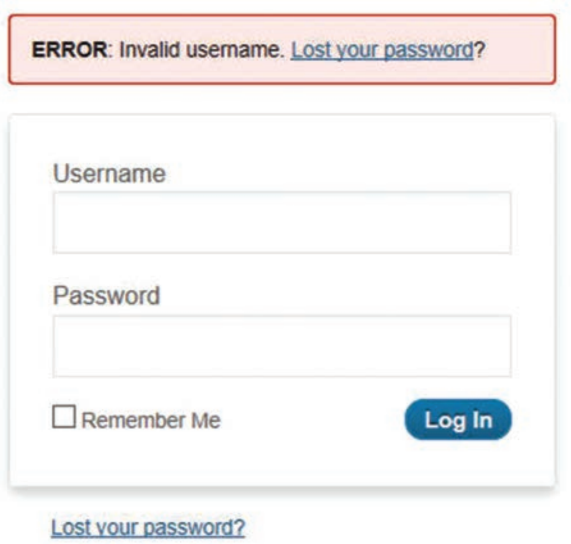
Functionality that exists in a different environment from your code can be accessed and shared using vendor-independent middleware known as *Common Object Request Broker Architecture* (*CORBA*). CORBA's purpose is to allow different vendor products, such as computer languages, to work seamlessly across distributed networks of diversified computers. The heart of the CORBA system is the *Object Request Broker* (*ORB*), which simplifies the process of requesting server objects for clients. The ORB locates a requested object, transparently activates it as necessary, and then delivers the requested object to the client.

Security of the Software Environment

The security of software is a critical concern. Protection of the confidentiality, integrity, and availability of data and program variables is one of the top concerns of a security professional. During the software design phase, you should consider risk analysis and mitigation. It's critical that the software development team identify, understand, and mitigate any risks that might make the organization vulnerable. Total risk refers to the probability and size of a potential loss. Every development project has elements of risk. For example, in an application that will deal with order quantities, the numbers should be positive; if you made it possible for someone to order negative 17 of an item, you would face added risk. Sanitizing inputs and outputs to allow only qualified values reduces the attack surface. Think of the attack surface as all of the potential ways in which an attacker can attack the application. Integrity of your code can be verified with hashing tools such as MD5sum or SHA1sum.

A *vulnerability* is a flaw, loophole, or weakness in an application that leads it to process critical data insecurely. A threat actor who can exploit vulnerabilities can gain access to software. Some common software vulnerabilities include escalation of privileges, buffer overflow, SQL injection, cross-site request forgery (CSRF), and cross-site scripting (XSS). It is important to remember that fixing security weaknesses and vulnerabilities at the source code level is much cheaper than waiting until later in the process. Penetration testing and fuzzing are much more expensive than fixing a vulnerability before the build process is complete.

Threat modeling is another technique that can be used to reduce risk and calculate the attack surface. Threat modeling details the potential attacks, targets, and any vulnerabilities of an application. It can also help determine the types of controls needed to prevent an attack. For example, when you enter an incorrect username or password, do you get a generic response, or does the application respond with too much data, as shown in Figure 9.9? Just keep in mind that the best practice from a security standpoint is to not identify which entry was invalid and provide only a generic message.



ERROR: Invalid username. Lost your password?

FIGURE 9.9 **Non-generic Response That Should Be Flagged by Threat Modeling**

A security professional should also consider the following:

- **What is the software environment?** Where is the software used? Is it on a mainframe, or maybe a publicly available website? Is the software run on a server, or is it downloaded and executed on the client (mobile code)?
- **What programming language and toolset were used?** Some languages, such as C, are known to be vulnerable to buffer overflows.

Note

Java is estimated to be installed on more than 850 million computers, 3 billion phones, and millions of TVs, but it was not until August 2014 that the company changed its update software to remove older, vulnerable versions of Java during the installation process.

- **What security issues and concerns are present in the source code?** Depending on how the code is processed, it may or may not be easy to identify problems. For example, a compiler translates a high-level language into machine language, whereas an interpreter translates the program line by line. It is important to determine whether an attacker can change input, process, or output data and whether the program will flag on these errors.
- **How do you identify malware and defend against it?** At a minimum, malware protection (antivirus) software needs to be deployed and methods to detect unauthorized changes need to be implemented.

> **Note**
>
> Regardless of the programming language used there are multiple secure coding standards to help build robust, secure applications. These standards include Application Security and Development Security Technical Implementation Guide (ASD STIG), CERT Software Engineering Institute (SEI), Open Web Application Security Project (OWASP) Top 10, and the Center of Internet Security (CIS) Top 20.

A risk assessment should be conducted for all application programming interfaces (APIs). Fuzz testing can be used to validate security controls and reduce the attack surface. APIs use function calls and offer developers the ability to bypass traditional web pages and interact directly with the underlying service. This type of functionality also comes with risk. Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) are examples of API styles. REST is an architectural style and uses uniform service locators. SOAP is a protocol and uses service interfaces. It is a standardized protocol that aids in sending messages using other protocols, such as HTTP and SMTP. REST was created to address the problems of SOAP. Three methods of authentication for RESTful APIs include the following:

- **Basic**: This method provides the lowest security. Basic authentication should not be used.
- **OAuth 1.0a**: This method is a secure but complicated process.
- **OAuth 2.0**: This method is similar to OAuth 1.0a but is less complex and lacks a signature.

Security doesn't stop after the software development process. The longer a program has been in use, the more vulnerable it becomes as attackers have more time to probe and explore methods to exploit it. Attackers might even analyze patches to determine what the patches are trying to fix and figure out how such vulnerabilities might be exploited.

Security professionals need to do proper planning for timely patch and update deployment. A *patch* is a fix to a particular problem in software applications or operating system code that does not create a security risk but does create problems with the application. A *hot fix* is quick but lacks full integration and testing, and it addresses only a specific issue. A *service pack* is a collection of all the patches to date; it is considered critical and should be installed as soon as possible.

Mobile Code

Mobile code, which is widely used on the web, is software that will be downloaded from a remote system and run on the computer performing the download. The security issue with mobile code is that it is executed locally. Many times, the user might not even know that the code is executing. Examples of mobile code include scripts, VBScript, applets, Flash, Java, and ActiveX controls. With mobile code, the downloaded program runs with the access rights of the logged-in user.

Java is the dominant programming language of mobile code. It is a compiled high-level language that can be used on any type of computer. It uses a sandbox security scheme. Java is extremely portable because the output of the Java compiler is not executable code but bytecode. *Bytecode* is a type of instruction set designed for efficient execution by a software interpreter to be executed by the Java runtime system, which is called the Java Virtual Machine (JVM).

A Java *applet* is a specific type of Java program that is designed to be transmitted over the Internet and automatically executed by a Java-compatible web browser, such as Edge, Firefox, Chrome, or Safari. The security issue with applets is that they are downloaded on demand, without further interaction with the user.

Buffer Overflow

A *buffer* is a temporary data storage area whose length and type are defined in the program code that creates it or by the operating system. *Buffer overflows* occur when programmers use unsecured functions or don’t enforce limits on buffers—basically, when programmers do not practice good coding techniques. For example, a program should check for and prevent any attempt to stuff 32 letters into a buffer intended for 24 digits. However, this type of error checking does not always occur, and attackers commonly use buffer overflows to gain access to systems and/or for privilege escalation. Attackers can use unprotected buffers to attempt to inject and run malicious code. Worse, if the original code executed has administrator or root rights, those privileges are granted to the attacker as well. In such a case, the attacker can gain access to a privileged command shell on the system that is under attack. When this occurs, the attacker has complete control.

Buffer overflows are a huge problem, and any hacker, ethical or not, is going to search for them. The best way to prevent buffer overflows is to have perfect programs. Because that is not possible, you can implement some compensating controls:

- **Audit the code**: The individuals who write code should not be the ones auditing that code. Manual audits should be performed by a different group of individuals who are trained to look for poorly written code and potential security problems. Although audits are effective, they can be expensive and time-consuming with large, complex programs.
- **Use safer functions**: Some programming languages offer more support against buffer overflows than C. If C is going to be used, ensure that safer C library support is used.
- **Improved compiler techniques**: Compilers such as Java automatically check whether a memory array index is working within the proper bounds.
- **Harden the stack**: Buffer overflows lead to overwrites of code and pointers in the program's stack space, which holds the code and predefined variables. This overwriting is called "smashing the stack" (see insecure.org/stf/smashstack.html). However, products such as StackGuard and Visual Basic have evolved special guard buffers called *canaries* that are compiled into code. A *canary* is a protected zone that is added between chunks of stack code. The code's execution is immediately halted if a canary is breached in a stack smashing attempt. Such techniques are not 100% effective and might still be vulnerable to heap overflows.

Financial Attacks

A large number of the attacks that occur today are perpetrated for financial reasons. One example is rounding-down attacks, which involve skimming off small amounts of money by rounding down the last few digits. With a bank account that has $8,239,128.45 in it, and an attacker might round down the amount to $8,239,128.40. A *salami* attack is similar; it involves slicing off small amounts of money so that the last few digits are truncated. For example, $8,239,128.45 would become $8,239,128. Both rounding and salami attacks take advantage of the fact that small amounts will not be missed and that over time the pennies will add up to big profits for the attacker. (When you take a break from studying, check out the 1999 movie *Office Space* to see a good example of an attempted salami attack.)

An attacker might even plant code with the thought of waiting until a later date to have it execute. This is called a *logic bomb*, and while logic bombs are not just for financial attacks, they can cause a great deal of damage. A logic bomb can be designed to detonate on some predetermined action or trigger. Because they are buried so deep in the code, logic bombs are difficult to discover or detect before they become active. Fired employees might use them to strike back at their former employer.

Change Detection

Hashing can enable a security professional to detect malicious code and is commonly used as an indicator of compromise (IOC). IOCs are simply pieces of forensic data, such as changed hashes, entries found in system log entries or other items that identify potentially malicious activity. Hash-based application verification ensures that an application has not been modified or corrupted; it does so by comparing the file's hash value to a previously calculated value, and if these values match, the file is presumed to be unmodified.

Change detection is another useful technique. Change detection software, such as Tripwire, detects changes to system and configuration files. Most of these programs work by storing a hashed value of the original file in a database. Periodically, the file is rechecked, and the hashed values are compared. If the two values do not match, the program can trigger an alert to signal that there might have been a compromise. Change detection combined with other technologies such as SIEM, IDP, and end point protection forms the basics of cyber security controls.

Hashed values are the most widely used mechanisms for detecting changes in files. Most software vendors provide Web-accessible summaries that list the fingerprints of all files included in their products. This gives users a way to ensure that they have authentic files.

Viruses and Worms

Malware has been around since the dawn of the computer era. Two common types of malware are viruses and worms. Some viruses and worms can spread quickly, and others spread slowly. *Fast-infection* viruses infect all files that they are capable of infecting. On the other hand, *sparse infectors* have more limited rates of spread. Viruses operate as file infection, macro, polymorphic, multipartite, and fileless infectors. Fileless malware emerged in 2017 and can execute in one of several ways including windows registry manipulation, memory code injection, and script-based techniques. Typically, fileless malware is written directly to the RAM, and executes from memory. Petya and WannaCry both used fileless techniques as part of their cyber kill chains.

Sometimes a virus is not malware at all and just simply a hoax. While not a true virus, a meme virus spreads like one and is basically a chain letter or email message that is continually forwarded.

Worms, unlike viruses, require no interaction on the user's part to replicate and spread. One of the first worms to be released on the Internet was the RTM worm. It was developed by Robert Morris Jr. in 1988 and was meant only to be a proof of concept. The goals of worms and even malware in general now tend to be much more specific. For example, Stuxnet was developed to target programmable logic controllers (PLCs) that control the automation of centrifuges used for separating nuclear material.

Traditionally, antivirus contains a library of signatures that it uses to detect viruses. A *signature* identifies a pattern of bytes found in the virus code. Here is an example of a virus signature:

```
X5O!P%@AP[4\PZX54(P^)7CC)7$EICAR-STANDARD-
ANTIVIRUS-TEST-FILE!$H+H*
```

This file is actually harmless, but it contains a signature like one found in a classic virus. This particular sequence was developed by the European Institute of Computer Anti-Virus Research (EICER) as a means of testing the functionality of antivirus software.

Next-generation antivirus goes beyond malware signatures and heuristics and uses predictive analytics driven by machine learning and artificial intelligence combined with threat intelligence. Next-generation antivirus can be used to prevent many types of known and unknown malware by monitoring; responding to attacker tactics, techniques, and procedures (TTPs); and examining patterns and activities associated with specific threat actors. These techniques along with advances in User Behavior Analytics (UBA) have changed the threat and defense landscape. UBA is the use of machine learning to model the behavior of legitimate users on corporate networks to detect anonymous behavior that could be the sign of a cyberattack.

Exam Prep Questions

1. As a security professional, you must understand the different types of application updates. All updates should be obtained from the manufacturer only and deployed into production only after being tested on non-production systems. Which of the following is the best answer that describes updates, patches, hot fixes, and service packs?

❍ **A.** A hot fix has undergone full integration testing, has been released to address vulnerability, and addresses a specific issue; in most cases, a hot fix is not appropriate for all systems. A security patch lacks full integration and testing, has been released to address a vulnerability, and is mandatory. A service pack is a collection of patches that are critical and should be installed quickly.

❍ **B.** A hot fix is quick, lacks full integration and testing, and addresses a specific issue; in most cases, a hot fix is not appropriate for all systems. A security patch is a collection of fixes that are critical and has been released to address a vulnerability. A service pack is a collection of patches and is considered critical.

❍ **C.** A hot fix is a quick collection of critical, install-ASAP patches that address a specific issue; in most cases, a hot fix is not appropriate for all systems. A security patch has undergone full integration testing and has been released to address a vulnerability. A service pack is a collection of patches.

❍ **D.** A hot fix is slow, has full integration and testing, and addresses a broad set of problems; in most cases, a hot fix is appropriate for all systems. A security patch is a collection of fixes that are not critical. A service pack is a collection of patches and is not considered critical.

2. Which of the following describes the CIA triad when applied to software security?

❍ **A.** Confidentiality prevents unauthorized access, integrity prevents unauthorized modification, and availability deals with countermeasures to prevent denial of service to authorized users.

❍ **B.** Confidentiality prevents unauthorized modification, integrity prevents unauthorized access, and availability deals with countermeasures to prevent denial of service to authorized users.

❍ **C.** Confidentiality prevents unauthorized access, integrity prevents unauthorized modification, and availability deals with countermeasures to prevent unauthorized access.

❍ **D.** Confidentiality deals with countermeasures to prevent denial of service to authorized users, integrity prevents unauthorized modification, and availability prevents unauthorized access.

3. Which of the following tools can be used for change detection?

   ❍ **A.** DES

   ❍ **B.** Checksums

   ❍ **C.** md5sum

   ❍ **D.** Parity bits

4. Bob has noticed that when he inputs too much data into his new Internet application, it momentarily locks up the computer and then halts the program. Which of the following best describes this situation?

   ❍ **A.** Fail-safe

   ❍ **B.** Buffer overflow

   ❍ **C.** Fail-open

   ❍ **D.** Fail-soft

5. Which of the following types of database management systems is considered a lattice structure, with each record having multiple parent and child records?

   ❍ **A.** Hierarchical database management system

   ❍ **B.** Network database management system

   ❍ **C.** Object-oriented database management system

   ❍ **D.** Relational database management system

6. Which database term refers to the capability to restrict certain fields or rows from unauthorized individuals?

   ❍ **A.** Low granularity

   ❍ **B.** High resolution

   ❍ **C.** High granularity

   ❍ **D.** Low resolution

7. Which of the following types of testing involves entering malformed, random data?

   ❍ **A.** XSS

   ❍ **B.** Buffer overflow

   ❍ **C.** Fuzzing

   ❍ **D.** Whitebox testing

8. OmniTec’s new programmer has left several entry points in its new e-commerce shopping cart program for testing and development. Which of the following terms best describes these entry points?

❍ **A.** Trojan

❍ **B.** Security flaws

❍ **C.** SQL injections

❍ **D.** Backdoor

9. What type of languages are Generation 2 programming languages?

❍ **A.** Assembly

❍ **B.** Machine

❍ **C.** High level

❍ **D.** Natural

10. Which of the following is considered middleware?

❍ **A.** Atomicity

❍ **B.** OLE

❍ **C.** CORBA

❍ **D.** Object-oriented programming

11. After Debbie becomes the programmer for the new payroll application, she places some extra code in the application that will cause the program to halt if she is fired and her name is removed from payroll. What type of attack has she launched?

❍ **A.** Rounding down

❍ **B.** Logic bomb

❍ **C.** Salami

❍ **D.** Buffer overflow

12. While working on a penetration test assignment, you discover that the organization’s database-driven e-commerce site will let you place a negative quantity into an order field so that the system will credit you money. Which of the following best describes this failure?

❍ **A.** Referential integrity error

❍ **B.** Buffer overflow

❍ **C.** Semantic integrity error

❍ **D.** Rounding down

13. Which of the following best describes bytecode?

❍ **A.** It is processor specific.

❍ **B.** It is used with ActiveX.

❍ **C.** It is not processor specific.

❍ **D.** It is used with COM and DCOM.

14. Which of the following is one of the best ways to deal with attacks like SQL, LDAP, and XML injection attacks?

❍ **A.** Using type-safe languages

❍ **B.** Manually reviewing code

❍ **C.** Using emanations

❍ **D.** Performing adequate parameter validation

15. Say that there are two objects, and neither of them knows how the other object works. The two objects are hidden from each other. Which of the following programming techniques would this scenario be most closely associated with?

❍ **A.** Data modeling

❍ **B.** Network database management system

❍ **C.** Object-oriented programming

❍ **D.** Relational database management system

Answers to Exam Prep Questions

1. **B.** A hot fix is quick, lacks full integration and testing, and addresses a specific issue; in most cases, a hot fix is not appropriate for all systems. A security patch is a collection of fixes that are critical and has been released to address a vulnerability. A service pack is a collection of patches and is considered critical. Answers A, C, and D are all incorrect because the definitions are swapped and connected to the wrong solutions. Software updates are optional and are usually functionality, not security, related. Firmware releases are produced to address security issues with hardware.
2. **A.** Confidentiality prevents unauthorized access, integrity prevents unauthorized modification, and availability deals with countermeasures to prevent denial of service to authorized users. Answers B, C, and D are incorrect and are just scrambled definitions that look similar to confuse the test taker.
3. **C.** One of the ways in which malicious code can be detected is through the use of change detection software. This software has the capability to detect changes to system and configuration files. Popular programs that perform this function include Tripwire and md5sum. Answer A is incorrect because DES is an asymmetric algorithm. Answers B and D are incorrect because both checksums and parity bits can be easily changed and, therefore, do not protect the software from change.
4. **D.** A fail-soft occurs when a detected failure terminates the application while the system continues to function. Answers A and C are incorrect because a fail-safe terminates the program and disables the system, while a fail-open is the worst of events because it allows attackers to bypass security controls and easily compromise the system. Answer B is incorrect because although a buffer overflow could be the root cause of the problem, the question asks why the application is halting in the manner described.
5. **B.** Network database management systems are designed for flexibility. The network database model is considered a lattice structure because each record can have multiple parent and child records. Answer A is incorrect because hierarchical database management systems are structured like a tree: Each record can have only one owner, and because of this restriction, hierarchical databases often can't be used to relate to structures in the real world. Answer C is incorrect because object-oriented database management systems are not lattice based and don't use a high-level language like SQL. Answer D is incorrect because relational database management systems are considered collections of tables that are linked by their primary keys.
6. **C.** Granularity refers to control over the view someone has of a database. With highly granular databases, it is possible to restrict certain fields or rows from unauthorized individuals. Answer A is incorrect because low granularity gives a database manager little control. Answers B and D are incorrect because high resolution and low resolution do not apply to the question.
7. **C.** Fuzzing is a form of blackbox testing that involves entering random input and monitoring for flaws or a system crash. The idea is to look for problems in the application. Answers A, B, and D are incorrect: This is not an example of whitebox testing, a buffer overflow, or XSS.

8. **D.** A backdoor is a technique used by programmers as a secret entry point into a program. Programmers find them useful during application development; however, they should be removed before the code is finalized. All other answers are incorrect: Answer B is also a security flaw, but it is not as specific as trapdoor; Trojans (answer A) are malicious in nature and pretend to be something they are not; and SQL injection (answer C) is targeted against databases.

9. **A.** Programming languages are categorized as follows: Generation 1 is machine language, Generation 2 is assembly language, Generation 3 is high-level language, Generation 4 is very high-level language, and Generation 5 is natural language.

10. **C.** Common Object Request Broker Architecture (CORBA) is vendor-independent middleware. Its purpose is to tie together different vendor products so that they can seamlessly work together over distributed networks. Answer B is incorrect because Object Linking and Embedding (OLE) is a proprietary system developed by Microsoft to allow applications to transfer and share information. Answer A is incorrect because atomicity deals with the validity of database transactions. Answer D is incorrect because object-oriented programming is a modular form of programming.

11. **B.** A logic bomb is designed to detonate sometime later, typically after the perpetrator leaves; it is usually buried deep in the code. Answers A, C, and D are incorrect: Rounding down involves skimming off small amounts of money by rounding down the last few digits; a salami attack involves slicing off small amounts of money so that the last few digits are truncated; and buffer overflow involves putting more information in a buffer than it is intended to hold.

12. **C.** Semantic integrity controls logical values, data, and operations that could affect them, such as placing a negative number in an order quantity field. Answers A, B, and D are incorrect: Referential integrity ensures that foreign keys only reference existing primary keys; buffer overflow involves putting more information in a buffer than it is intended to hold; and rounding down involves skimming off small amounts of money by rounding down the last few digits.

13. **C.** Bytecode is not processor specific and is a form of intermediate code used by Java. Answers A, B, and D are incorrect: Bytecode is not processor specific and can run on many systems; bytecode is not associated with ActiveX; and COM and DCOM are technologies associated with ActiveX.

14. **D.** Adequate parameter validation is seen as the best approach to dealing with input problems. All data must be checked for validity when input, when processed, and when output. Answers A, B, and C are incorrect: Moving to a type-safe language does not prevent buffer overflows; although manual review of code may find some problems, this might not always be possible; and switching to mobile code is not feasible in all situations.

15. **C.** Object-oriented development allows an object to hide the way an object works from other objects. Answers A, B, and D are incorrect: Data modeling considers data independently, network database management systems are designed for flexibility, and relational database management systems are considered collections of tables that are linked by their primary keys.

Need to Know More?

Building security software: www.owasp.org/index.php/OWASP_Guide_Project

Assessing security of acquired software: www.delltechnologies.com/en-us/blog/assessing-security-acquired-software-one-size-fit/

Six steps to change management: www.techrepublic.com/article/implement-change-management-with-these-six-steps/5074869

Object-oriented programming: encyclopedia2.thefreedictionary.com/Object-oriented+programming

Development methodologies: www.synopsys.com/blogs/software-security/top-4-software-development-methodologies/

Maturity models: www.process.st/maturity-model/

Change management: www.prosci.com/resources/articles/what-is-change-management

Security of code repositories: https://blog.cyberint.com/what-you-need-to-know-about-code-repository-threats

The history of SQL injection attacks: motherboard.vice.com/read/the-history-of-sql-injection-the-hack-that-will-never-go-away

SQL injection and database manipulation: www.securiteam.com/securityreviews/5DP0N1P76E.html

Secure coding practices: https://wiki.sei.cmu.edu/confluence/display/seccode/Top+10+Secure+Coding+Practices

This page intentionally left blank

Practice Exam I

You will have 90 minutes to complete this exam, which consists of 60 questions. The actual CISSP exam requires a minimum passing score of 700 out of 1,000. Ensure that you read each question, looking for details that would rule out any of the possible answers. Many times there will be two or more correct answers; however, there is only one best answer, and that is the one you should select. In the real world, a security professional often has several options to secure a network, but one option is better than the others. This is the case, for example, when choosing the best encryption to secure data or wireless networks.

Remember that the CISSP exam asks many conceptual questions for which there may not be perfect answers. If you encounter such a question, choose the best answer. Leaving a question blank will count against you, so you are always better off taking a guess than leaving a question blank. The exam may present you with drag-and-drop questions or scenarios, and it may offer figures or diagrams. Examine each question carefully, and if you are taking the adaptive exam, keep in mind that once you pass a question, you cannot go back to it.

Practice Exam Questions

1. What type of access control features a policy decision point and a policy enforcement point?

❍ **A.** Mandatory access control

❍ **B.** Discretionary access control

❍ **C.** Attribute-based access control

❍ **D.** Role-based access control

2. Information security models bridge the gap between access control concepts and implementation of the concepts through the operating system. Place each of the following models into the category that best describes its design. Some categories may not be used.

❍ **A.** Biba

❍ **B.** Clark-Wilson

❍ **C.** Bell-LaPadula

❍ **D.** Brewer and Nash

Integrity (1)	Confidentiality (2)	Conflict of Interest (3)

3. What form of biometric system analyzes the features that exist in the colored tissue surrounding the pupil to validate access?

❍ **A.** Retina scanner

❍ **B.** Cornea scanner

❍ **C.** Iris scanner

❍ **D.** Optic nerve scanner

4. What is the most important item to consider when examining biometric systems?

❍ **A.** The crossover acceptance rate; the lower the number, the better the biometric system

❍ **B.** The crossover error rate; the higher the number, the better the biometric system

❍ **C.** The crossover acceptance rate; the higher the number, the better the biometric system

❍ **D.** The crossover error rate; the lower the number, the better the biometric system

5. You have been asked to help with an authentication problem reported after your organization moved to biometric authentication. One of your company's employees enrolled with a fingerprint reader and was able to authenticate for several weeks using the new system. Then, one day, the employee complained that after cutting his finger, he could no longer authenticate and received a Type I error. What is most likely the problem?

- ❍ **A.** The system does not examine enough information to determine the user.
- ❍ **B.** Fingerprint readers are not very good at handling Type I errors by nature because these readers are very dynamic.
- ❍ **C.** Fingerprint readers are not very good at handling Type I errors by nature because these readers have high crossover error rates.
- ❍ **D.** The system examines too much information and needs to be configured to be less sensitive.

6. Which of the following fence heights will deter only casual trespassers?

- ❍ **A.** 2–3 feet
- ❍ **B.** 3–4 feet
- ❍ **C.** 4–5 feet
- ❍ **D.** 5–7 feet

7. In terms of policies and procedures, who is responsible for the protection of an organization's assets and data?

- ❍ **A.** User
- ❍ **B.** Data owner
- ❍ **C.** Data custodian
- ❍ **D.** Security auditor

8. Which of the following is considered a flaw, a loophole, an oversight, or an error that makes an organization susceptible to attack or damage?

- ❍ **A.** Risk
- ❍ **B.** Vulnerability
- ❍ **C.** Exposure
- ❍ **D.** Threat

9. Which of the following is the correct formula for determining single loss expectancy?

- ❍ **A.** Single loss expectancy = Asset value / Exposure factor
- ❍ **B.** Single loss expectancy = Asset value × Exposure factor
- ❍ **C.** Single loss expectancy = Risk / Exposure factor
- ❍ **D.** Single loss expectancy = Vulnerability × Exposure factor

10. Estimating potential loss is an important task of CISSP-certified professionals. Which of the following answers lists the correct steps, in the correct order, for performing a quantitative assessment?

- ○ **A.** Estimate potential losses, perform a vulnerability assessment, and determine annual loss expectancy
- ○ **B.** Estimate potential losses, conduct a threat analysis, and rank losses as high, medium, or low
- ○ **C.** Assemble a team, prepare a matrix of critical systems and services, and rank losses as high, medium, or low
- ○ **D.** Estimate potential losses, conduct a threat analysis, and determine annual loss expectancy

11. What is the Delphi technique an example of?

- ○ **A.** A BCP analysis technique
- ○ **B.** A quantitative assessment technique
- ○ **C.** A DRP analysis technique
- ○ **D.** A qualitative assessment technique

12. What is the formula for total risk?

- ○ **A.** (Threat – Countermeasure) / Asset value = Total risk
- ○ **B.** (Threat – Countermeasure) × Asset value = Total risk
- ○ **C.** Threat × Vulnerability × Asset value = Total risk
- ○ **D.** Threat × Vulnerability / Asset value = Total risk

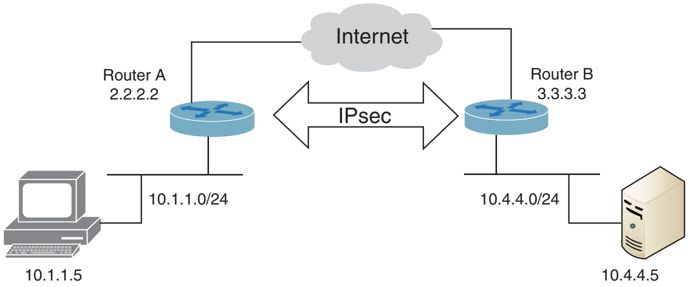
13. What method of dealing with risk occurs when individuals do a cost/benefit analysis and determine that the cost of the benefits outweighs the cost of the potential losses?

- ○ **A.** Risk reduction
- ○ **B.** Risk rejection
- ○ **C.** Risk transference
- ○ **D.** Risk acceptance

14. At which protection ring layer do you find the security kernel?

- ○ **A.** Layer 0
- ○ **B.** Layer 1
- ○ **C.** Layer 2
- ○ **D.** Layer 4

15. You have been brought in as a consultant for a small local startup firm that has given you the diagram shown below. Initially, the firm wants to connect to remote sites but would like to plan for remote user access in the future. In this case, which VPN method is not likely to work through NAT?



- ❍ **A.** IPsec transport mode
- ❍ **B.** IPsec tunnel with AH
- ❍ **C.** IPsec tunnel with ESP
- ❍ **D.** Suggest they use PPTP

16. Which of the following are considered temporary storage units within the CPU?

- ❍ **A.** I/O buffer
- ❍ **B.** Registers
- ❍ **C.** Control circuits
- ❍ **D.** ALUs

17. Confidentiality and integrity are important concepts when discussing security models. Which of the following was one the first models developed to address only the goal of integrity?

- ❍ **A.** Biba
- ❍ **B.** Clark-Wilson
- ❍ **C.** Brewer and Nash
- ❍ **D.** Chinese Wall

18. Which of the following is considered the first security model to be based on confidentiality?

- ❍ **A.** Biba
- ❍ **B.** Bell-LaPadula
- ❍ **C.** Graham-Denning
- ❍ **D.** Clark-Wilson

19. Which of the following blackbox testing techniques is very similar to a narrowly scoped penetration test?

❍ **A.** IAST

❍ **B.** DAST

❍ **C.** RASP

❍ **D.** SAST

20. You are a consultant for a contractor that is doing work for an individual government agency. The government requires that all people must have a clearance for most restricted information in the information system and a valid need to know. However, all people do not have to have a clearance for all information in the information system. What mode of security do you recommend for this contractor?

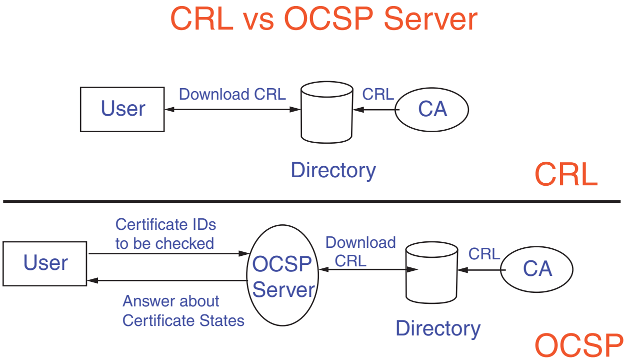
❍ **A.** Dedicated security mode

❍ **B.** System high security mode

❍ **C.** Compartmented security mode

❍ **D.** Multilevel security mode

21. When using PKI, there are two ways you can handle revocation of certificates, as shown in the following figure. When using Online Certificate Status Protocol (OCSP), messages are encoded and typically transmitted over HTTP. Which of the following is not true about using OSCP instead of using certificate revocation lists (CRLs)?



❍ **A.** Does not mandate encryption

❍ **B.** Contains more information than a typical CRL

❍ **C.** Discloses that a particular network host used a particular certificate at a particular time

❍ **D.** Places less burden on client resources

22. You have been asked to examine a database to evaluate referential integrity. Which of the following should you review?

❍ **A.** Field

❍ **B.** Aggregation

❍ **C.** Composite key

❍ **D.** Foreign key

23. Which of the following wireless standards uses frequency-hopping spread spectrum (FHSS) by default?

❍ **A.** Bluetooth

❍ **B.** 802.11a

❍ **C.** 802.11b

❍ **D.** LiFi

24. Which of the following is a technology that meets the needs of multi-tenant data centers by providing the necessary segmentation on a large scale?

❍ **A.** VLAN

❍ **B.** A trunk

❍ **C.** VXLAN

❍ **D.** CDMA

25. How many DS0 channels are bundled to make a T1?

❍ **A.** 18

❍ **B.** 21

❍ **C.** 24

❍ **D.** 32

26. Which of the following is a security technique that breaks data centers and cloud environments into segments down to the individual workload level?

❍ **A.** Microsegmentation

❍ **B.** Firewalls

❍ **C.** Zerotrust

❍ **D.** SDWAN

27. Which of the following best defines transaction persistence?

❍ **A.** Database transactions should be all or nothing to protect the integrity of the database.

❍ **B.** A database should be in a consistent state, and there should not be a risk of integrity problems.

❍ **C.** A database should be the same before and after a transaction has occurred.

❍ **D.** Databases should be available to multiple users at the same time without endangering the integrity of the data.

28. Which of the following refers to the capability to combine data from separate sources to gain information?

❍ **A.** Metadata

❍ **B.** Inference

❍ **C.** Aggregation

❍ **D.** Deadlocking

29. Ted considers himself a skillful hacker. He has devised a way to replace the existing startup programs between the time when a system boots and the time when the system actually executes these programs. He believes that if he can perfect his attack, he can gain control of the system. What type of attack is described here?

❍ **A.** Synchronous attack

❍ **B.** TOC/TOU attack

❍ **C.** DCOM attack

❍ **D.** Pass the hash attack

30. Which of the following is evidence that is not based on personal knowledge but that was told to the witness?

❍ **A.** Best evidence

❍ **B.** Secondary evidence

❍ **C.** Conclusive evidence

❍ **D.** Hearsay evidence

31. Which mode of DES functions by XORing each block of ciphertext with the next plaintext block to be encrypted, with the result being a dependency on all the previous blocks?

❍ **A.** ECB

❍ **B.** CBC

❍ **C.** CFB

❍ **D.** OFB

32. What mode of DES is susceptible to meet-in-the-middle attacks?

❍ **A.** DES

❍ **B.** 2DES

❍ **C.** 3DES

❍ **D.** 3DES EDE2

33. Which asymmetric cryptosystem is used for digital signatures?

❍ **A.** DES

❍ **B.** SHA1

❍ **C.** Diffie-Hellman

❍ **D.** ECC

34. When developing the organization's contingency plan, which of the following should not be included in the process?

❍ **A.** Damage assessment team

❍ **B.** Legal counsel

❍ **C.** Salvage team

❍ **D.** Red team

35. Which of the following is a valid form of attack against ARP?

❍ **A.** Flooding

❍ **B.** Spanning tree attack

❍ **C.** Name server poisoning

❍ **D.** Reverse lookup

36. Which of the following is considered an authentication type that can use smart cards and certificates?

❍ **A.** CHAP

❍ **B.** EAP

❍ **C.** MS-CHAP

❍ **D.** PAP

37. Which of the following address ranges is not listed in RFC 1918?

❍ **A.** 10.0.0.0 to 10.255.255.255

❍ **B.** 172.16.0.0 to 172.31.255.255

❍ **C.** 172.16.0.0 to 172.63.255.255

❍ **D.** 192.168.0.0 to 192.168.255.255

38. Which of the following is not a reason email should be protected?

- ❍ **A.** Encryption is a difficult, time-consuming process.
- ❍ **B.** Faking email is easy.
- ❍ **C.** Sniffing email is easy.
- ❍ **D.** Stealing email is difficult.

39. Which of the following statements about instant messaging is incorrect?

- ❍ **A.** It has no capability for scripting.
- ❍ **B.** It can bypass corporate firewalls.
- ❍ **C.** It lacks encryption.
- ❍ **D.** It uses insecure password management.

40. ActiveX is used by which of the following technologies?

- ❍ **A.** Java
- ❍ **B.** CORBA
- ❍ **C.** EJB
- ❍ **D.** DCOM

41. Which of the following protocols is said to use "a web of trust"?

- ❍ **A.** PKI
- ❍ **B.** IGMP
- ❍ **C.** PGP
- ❍ **D.** DKIM

42. Which of the following is considered the act of encouraging or inducing a person to commit a crime in order to bring criminal charges against that individual?

- ❍ **A.** Inducement
- ❍ **B.** Entrapment
- ❍ **C.** Honeypotting
- ❍ **D.** Enticement

43. Which of the following terms describes the coalition of nations that has been meeting for many years to work on solving the world's economic problems?

- ❍ **A.** G8
- ❍ **B.** MLAT
- ❍ **C.** SWAT
- ❍ **D.** UN Resolution 1154

44. Which of the following is not one of the main BCP testing strategies?

❍ **A.** Partial interruption

❍ **B.** Structured walkthrough

❍ **C.** Parallel

❍ **D.** Full interruption

45. In a BCP, critical resources are usually divided into five primary categories. What are these categories?

❍ **A.** Business, administrative, user, technical, and data

❍ **B.** Administrative, policy, user, technical, and data

❍ **C.** Business, facility and supply, user, technical, and nontechnical

❍ **D.** Business, facility and supply, user, technical, and data

46. Which of the following allows developers the ability to bypass traditional web pages and interact directly with the underlying service?

❍ **A.** SOAP

❍ **B.** APIs

❍ **C.** OAuth

❍ **D.** REST

47. Which of the following protocols is used for router multicasting?

❍ **A.** ICMP

❍ **B.** RIPv1

❍ **C.** 224.0.0.1

❍ **D.** IGMP

48. VoIP uses which of the following to deal with network congestion?

❍ **A.** Time-division multiplexing

❍ **B.** TCP protocol

❍ **C.** VLANs technology

❍ **D.** Isochronous design

49. Which of the following is a network technology based on transferring data in cells or packets of a fixed size?

❍ **A.** ATM

❍ **B.** ISDN

❍ **C.** SMDS

❍ **D.** Microsegmentation

50. WEP has vulnerabilities. Which of the following is not a reason it is vulnerable?

❍ **A.** Shared WEP keys among all clients

❍ **B.** An RC4 engine not properly initialized

❍ **C.** 20-bit initialization vector

❍ **D.** 40-bit WEP keys

51. You are an advisory board member for a local nonprofit organization. The organization has been given a new server, and members plan to use it to connect their 24 client computers to the Internet for email access. Currently, none of these computers has antivirus software installed. Your research indicates that there is a 95% chance that these systems will become infected after email is in use. A local vendor has offered to sell 25 copies of antivirus software to the nonprofit organization for $400 total. The nonprofit's 10 paid employees make only about $9 an hour each. There's a good chance that a virus could bring down the network for an entire day. What would be the ALE for this proposed change?

❍ **A.** $423

❍ **B.** $950

❍ **C.** $720

❍ **D.** $684

52. The Common Criteria rating "structurally tested" means the design meets what level of verification?

❍ **A.** EAL 1

❍ **B.** EAL 2

❍ **C.** EAL 4

❍ **D.** EAL 5

53. Which of the following is a technique that can be used to prevent an attacker from making lateral movements once he or she gains a reverse shell on a server?

❍ **A.** Microsegmentation

❍ **B.** Zero trust

❍ **C.** Port mirroring

❍ **D.** Enforced governance compliance

54. What Bell-LaPadula model rule states that someone at one security level cannot write information to a lower security level?

❍ **A.** Star (*) property

❍ **B.** Simple security rule

❍ **C.** Simple integrity property

❍ **D.** Strong star rule

55. You are an advisory board member for an organization that has decided to go forward with a proposed Internet and email connectivity project. Here are the projected details:

24 computers are connected to the Internet.

There is a 95% probability of virus infection.

10 paid employees each make $9 an hour.

A successful virus outage could bring down the network for an entire day.

25 copies of antivirus software will cost the organization $399.

The CEO would like to know how much money, if any, will be saved through the purchase of antivirus software. How much money will be saved?

○ **A.** $218

○ **B.** $285

○ **C.** $380

○ **D.** $490

56. Which of the following is considered the first line of defense against human attack?

○ **A.** Cryptography

○ **B.** Physical security

○ **C.** Business continuity planning

○ **D.** Policies

57. Which of the following statements about HVAC is correct?

○ **A.** HVAC should be a closed-loop system with negative pressurization.

○ **B.** HVAC should be an open-loop system with positive pressurization.

○ **C.** HVAC should be an open-loop system with negative pressurization.

○ **D.** HVAC should be a closed-loop system with positive pressurization.

58. Which of the following types of fire detectors uses rate-of-rise sensors?

○ **A.** Flame activated

○ **B.** Heat activated

○ **C.** Smoke activated

○ **D.** Ion activated

59. A fire caused by electrical equipment is considered which class of fire?

○ **A.** D

○ **B.** C

○ **C.** B

○ **D.** A

60. While Jim is examining the clapper valve of a failed fire suppression system on the loading dock, he starts to wonder whether he has installed the right fire suppression system. The facility is unheated and located in a major city in the northeastern United States. Based on this information, which system should Jim be using?

❍ **A.** Deluge

❍ **B.** Wet pipe

❍ **C.** Pre-action

❍ **D.** Dry pipe

Practice Exam II

You will have 90 minutes to complete this exam, which consists of 60 questions. The actual CISSP exam requires a minimum passing score of 700 out of 1,000. Ensure that you read each question, looking for details that would rule out any of the possible answers. Many times there will be two or more correct answers; however, there is only one best answer, and that is the one you should select. In the real world, a security professional often has several options to secure a network, but one option is better than the others. This is the case, for example, when choosing the best encryption to secure data or wireless networks.

Remember that the CISSP exam asks many conceptual questions for which there may not be perfect answers. If you encounter such a question, choose the best answer. Leaving a question blank will count against you, so you are always better off taking a guess than leaving a question blank. The exam may present you with drag-and-drop questions or scenarios, and it may offer figures or diagrams. Examine each question carefully, and if you are taking the adaptive exam, keep in mind that once you pass a question, you cannot go back to it.

Practice Exam Questions

1. What fence height is required to prevent a determined intruder?

❍ **A.** 4 feet

❍ **B.** 6 feet

❍ **C.** 8 feet

❍ **D.** None of these answers is correct.

2. A fire caused by combustible metals would be considered which class of fire?

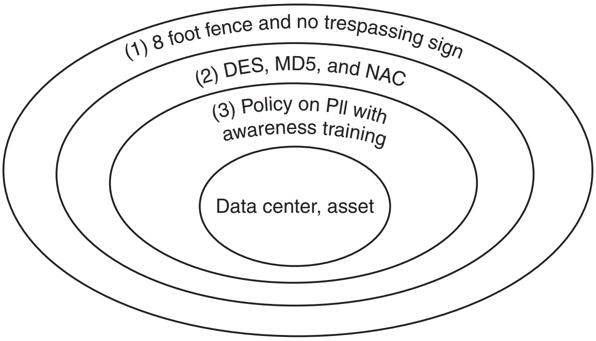
❍ **A.** A

❍ **B.** B

❍ **C.** C

❍ **D.** D

3. Controls should be implemented using a layered approach. Review the following diagram. Which order does the diagram most closely represent?


(1) 8 foot fence and no trespassing sign
(2) DES, MD5, and NAC
(3) Policy on PII with awareness training
Data center, asset

Layered defense

❍ **A.** (1) Physical/preventive, (2) administrative/preventive, (3) technical/deterrent control layered approach

❍ **B.** (1) Physical/preventive/deterrent, (2) technical/preventive/detective/, (3) administrative/preventive layered approach

❍ **C.** (1) Deterrent/preventive, (2) administrative/detective, (3) preventive training

❍ **D.** (1) Physical/preventive/deterrent, (2) hardware/software preventive, (3) administrative/preventive layered approach

4. Which of the following types of card keys contains rows of copper strips?

❍ **A.** Magnetic strip

❍ **B.** Electronic circuit

❍ **C.** Magnetic stripe

❍ **D.** Active electronic

5. Tony's company manufactures proprietary tractor-trailer tracking devices. Now that employees will be issued laptops, Tony is concerned about the loss of confidential information if an employee's laptop is stolen. Which of the following would be the best defensive method?

- ❍ **A.** Use integrity programs such as MD5 and SHA to verify the validity of installed programs.
- ❍ **B.** Place labels on the laptops offering a reward for stolen or missing units.
- ❍ **C.** Issue laptop users locking cables to secure the units and prevent their theft.
- ❍ **D.** Encrypt the hard drives.

6. Under what conditions can halon be expected to degrade into toxic compounds?

- ❍ **A.** At temperatures greater than 500°F
- ❍ **B.** At temperatures greater than 900°F and concentrations greater than 10%
- ❍ **C.** At temperatures greater than 900°F
- ❍ **D.** At temperatures greater than 500°F and concentrations greater than 7%

7. According to NIST perimeter lighting standards, critical areas should be illuminated to what measurement?

- ❍ **A.** 10 feet in height, with 2 foot-candles of illuminance
- ❍ **B.** 12 feet in height, with 4 foot-candles of illuminance
- ❍ **C.** 8 feet in height, with 2 foot-candles of illuminance
- ❍ **D.** 8 feet in height, with 4 foot-candles of illuminance

8. What type of biometric error signifies that an authorized user has been denied legitimate access?

- ❍ **A.** Type I
- ❍ **B.** Type II
- ❍ **C.** Type III
- ❍ **D.** Type IV

9. In biometrics, the point at which the FAR equals the FRR is known as which of the following?

- ❍ **A.** Crossover error rate
- ❍ **B.** Error acceptance rate
- ❍ **C.** Crossover acceptance rate
- ❍ **D.** Failure acceptance rate

10. RSA's SecurID is an example of which of the following?

❍ **A.** SSO system

❍ **B.** Synchronous authentication

❍ **C.** Token authentication

❍ **D.** Asynchronous authentication

11. Which of the following is a weak implementation of EAP?

❍ **A.** EAP-FAST

❍ **B.** LEAP

❍ **C.** PEAP

❍ **D.** EAP-TLS

12. When discussing the security of SSO systems, which of the following is considered a disadvantage?

❍ **A.** Single sign-on involves a lot of maintenance and overhead because all systems are tied together.

❍ **B.** The biggest disadvantage of single sign-on is that system time on all systems must be held to very tight standards; deviations from these standards can lead to serious access problems.

❍ **C.** There are no real disadvantages to single sign-on.

❍ **D.** Breaching single sign-on allows an intruder access to all systems tied to the SSO implementation.

13. Snort started as what type of system?

❍ **A.** Behavior-based IPS

❍ **B.** Signature-based IDS

❍ **C.** Behavior-based IDS

❍ **D.** Signature-based IPS

14. What type of attack is also known as a race condition?

❍ **A.** Synchronous attack

❍ **B.** Buffer overflow

❍ **C.** Asynchronous attack

❍ **D.** Scanlog attack

15. I/O drivers and utilities are typically found at what protected ring layer?

❍ **A.** Layer 1

❍ **B.** Layer 2

❍ **C.** Layer 3

❍ **D.** Layer 0

16. What type of CPU can interleave two or more programs for execution at any one time?

❍ **A.** Multiprogramming

❍ **B.** Multitasking

❍ **C.** Multiapp

❍ **D.** Multiprocessor

17. What portion of the CPU performs arithmetic and logical operations on binary data?

❍ **A.** I/O buffer

❍ **B.** Registers

❍ **C.** Control circuit

❍ **D.** ALU

18. You are a security consultant for a contracting agency. The agency chief wants to prevent subjects from writing information to a higher level than the subject's security clearance. He also wants to ensure that subjects from a higher clearance level cannot read information at a lower level. The agency requires some type of access control model for its information systems to protect the integrity of its data. What is your best recommendation for the model to use in this case?

❍ **A.** Bell-LaPadula

❍ **B.** Biba

❍ **C.** State machine

❍ **D.** Clark-Wilson

19. How many stages are involved in the Lockheed Martin Cyber Kill Chain framework?

❍ **A.** 5

❍ **B.** 7

❍ **C.** 4

❍ **D.** 6

20. Which of the following has become a major trend in software development as an alternative or companion to virtualization?

❍ **A.** Microservices

❍ **B.** Serverless

❍ **C.** Containerization

❍ **D.** Embedded systems

21. Which of the following is considered the totality of protection mechanisms within a computer system and is responsible for enforcing security?

❍ **A.** Rings of protection

❍ **B.** The security kernel

❍ **C.** TCB

❍ **D.** Resource isolation

22. Johnny is worried that someone might be able to intercept and decrypt his VoIP phone calls. Which of the following protocols is most closely associated with VoIP?

❍ **A.** SKYP

❍ **B.** SLIP

❍ **C.** S/MIME

❍ **D.** SIP

23. Which of the following wireless standards uses direct-sequence spread spectrum (DSSS) by default?

❍ **A.** Bluetooth

❍ **B.** 802.11a

❍ **C.** 802.11b

❍ **D.** 802.11ac

24. What is a rogue AP?

❍ **A.** An individual connected to an unauthorized modem

❍ **B.** An unauthorized AP attached to a corporate network

❍ **C.** An unauthorized modem attached to a network

❍ **D.** An individual intercepting wireless traffic from inside or outside an organization

25. Which of the following is typically used with software to search for defects during various phases of the software development process to prevent issues and outages before the software is placed in production?

❍ **A.** Fuzzing

❍ **B.** Synthetic transactions

❍ **C.** Fagen inspection

❍ **D.** RASP

26. Which of the following does a T1 line use to multiplex DS0s into a composite T1?

❍ **A.** Channel division

❍ **B.** Frequency-hopping spread spectrum

❍ **C.** Frequency division

❍ **D.** Time division

27. Which of the following focuses on how to repair and restore a data center and the information at an original or new primary site?

❍ **A.** BCP

❍ **B.** BCM

❍ **C.** DRP

❍ **D.** BIA

28. What type of service is used to provide protection for source code in the event that the manufacturer declares bankruptcy or goes broke?

❍ **A.** Government access to keys

❍ **B.** MAD

❍ **C.** Electronic vaulting

❍ **D.** Software escrow

29. Which of the following describes the cooperative effort between the United States and Europe to exchange information about European citizens between European firms and North American parent corporations?

❍ **A.** SB 168

❍ **B.** Demar Act

❍ **C.** Safe Harbor Act

❍ **D.** Safety Shield Act

30. Which of the following best describes an approved type of forensic duplication?

❍ **A.** Logical copy

❍ **B.** Bit copy

❍ **C.** Microsoft Backup

❍ **D.** Xcopy

31. Which of the following best describes the SET protocol?

- ❍ **A.** Originated by Victor Miller and Neal Koblitz for use as a digital signature cryptosystem. It is useful in applications for which memory, bandwidth, or computational power is limited.
- ❍ **B.** Originated by MasterCard and Visa to be used on the Internet for credit card transactions. It uses digital signatures.
- ❍ **C.** Originated by Victor Miller and Neal Koblitz for use as a key exchange cryptosystem. It is useful in applications for which memory, bandwidth, or computational power is limited.
- ❍ **D.** Originated by MasterCard and Visa to be used on the Internet for credit card transactions. It uses the SSL protocol.

32. Which of the following information-management systems uses artificial intelligence?

- ❍ **A.** Polyinstantiation
- ❍ **B.** Known signature scanning
- ❍ **C.** Application programming interface
- ❍ **D.** Knowledge discovery in databases

33. DNS lookups that are less than 512 bytes are typically performed on which of the following protocols and ports?

- ❍ **A.** UDP port 53
- ❍ **B.** UDP port 69
- ❍ **C.** TCP port 53
- ❍ **D.** UDP port 161

34. Bob is worried that a program someone gave him at DEF CON has been altered from the original. Which of the following is a valid technique that Bob can use to verify the program's authenticity?

- ❍ **A.** Run AES against the program.
- ❍ **B.** Compare the size and date with those of the version found on the developer's website.
- ❍ **C.** Run md5sum and check against the md5sum from developer sites.
- ❍ **D.** Calculate a digital signature.

35. Which of the following is not an email encryption security standard?

- ❍ **A.** IMAP
- ❍ **B.** MOSS
- ❍ **C.** PGP
- ❍ **D.** PEM

36. Which of the following best describes link encryption?

❍ **A.** Data is encrypted at the point of origin and is decrypted at the destination.

❍ **B.** The message is decrypted and re-encrypted as it passes through each successive node, using a key common to the two nodes.

❍ **C.** The KDC shares a user-unique key with each user.

❍ **D.** It requires a session key that the KDC shares between the originator and the final destination.

37. Diameter uses which of the following as a base?

❍ **A.** TACACS

❍ **B.** TACACS+

❍ **C.** RADIUS

❍ **D.** Kerberos

38. The ACID test is used to describe what?

❍ **A.** Behavior-based intrusion detection systems

❍ **B.** Database transactions

❍ **C.** Signature-based intrusion detection systems

❍ **D.** The strength of a cryptographic function

39. Which fault-tolerant system can back up media in much the same way as disk striping?

❍ **A.** RAID

❍ **B.** RAIT

❍ **C.** JBOD

❍ **D.** SOAR

40. Which of the following is a stream cipher?

❍ **A.** DES

❍ **B.** Camellia

❍ **C.** RC4

❍ **D.** Twofish

41. Which of the following is considered the weakest mode of DES?

❍ **A.** Electronic Code Book

❍ **B.** Cipher Block Chaining

❍ **C.** Cipher Feedback

❍ **D.** Output Feedback

42. Which ethical standard states that “access and use of the Internet is a privilege and should be treated as such by all users”?

❍ **A.** RFC 1087

❍ **B.** (ISC)^2 Code of Ethics

❍ **C.** The Ten Commandments of Computer Ethics

❍ **D.** RFC 1109

43. Which of the following would be considered the oldest and most well-known software development method?

❍ **A.** Spiral

❍ **B.** Clean room

❍ **C.** Waterfall

❍ **D.** V-shaped waterfall

44. Which of the following techniques would not be considered one of the techniques used by fileless malware?

❍ **A.** RAM

❍ **B.** Multipartite

❍ **C.** Memory code injection

❍ **D.** Windows register manipulation

45. HTTPS uses TCP and which of the following ports?

❍ **A.** 80

❍ **B.** 110

❍ **C.** 111

❍ **D.** 443

46. Which of the following is considered the oldest type of database system?

❍ **A.** Hierarchical

❍ **B.** Network

❍ **C.** Relational

❍ **D.** Object oriented

47. The IEEE separates the OSI data link layer into two sublayers. What are they?

❍ **A.** Media MAC Control and Media Access Control

❍ **B.** Logical Link Control and Media Access Control

❍ **C.** High-Level Data Link Control and Media MAC Control

❍ **D.** Data Link Control and Media MAC Control

Questions 48 and 49 refer to the following table.

User and Object List

Dwayne	Object 1	Object 2	Object 3
Mike	Write	Read	Read/write
Christine	No access	Read	Read
Betsy	Read/write	Read	Read

48. What does the model shown in the table represent?

❍ **A.** MAC

❍ **B.** RBAC

❍ **C.** LBAC

❍ **D.** Access control matrix

49. Using the model shown in the table, Mike, Christine, Dwayne, and Betsy are _________, and Object 1, Object 2, and Object 3 are _____.

❍ **A.** Objects; subjects

❍ **B.** Subject; objects

❍ **C.** Names of users; resources the users access

❍ **D.** Names of the users; objects the users access

50. 802.11 networks are identified by which of the following?

❍ **A.** Security identifier (SID)

❍ **B.** Broadcast name

❍ **C.** Kismet

❍ **D.** Service set identifier (SSID)

51. Which of the following refers to a dynamic, adaptive technology that leverages large-scale threat history data to proactively block and remediate future malicious attacks on a network?

❍ **A.** Threat intelligence

❍ **B.** Intrusion detection and prevention (IDP)

❍ **C.** Security information and event management (SIEM)

❍ **D.** User and entity behavior analytics (UEBA)

52. The Common Criteria rating “functionality tested” means the design meets what level of verification?

❍ **A.** EAL 1

❍ **B.** EAL 2

❍ **C.** EAL 4

❍ **D.** EAL 5

53. Which of the following is not addressed by the Clark-Wilson security model?

❍ **A.** Blocking unauthorized individuals from making changes to data

❍ **B.** Maintaining internal and external consistency

❍ **C.** Protecting the confidentiality of information

❍ **D.** Blocking authorized individuals from making unauthorized changes to data

54. Which of the following individuals would be responsible for maintaining and protecting the company’s assets and data?

❍ **A.** User

❍ **B.** Data owner

❍ **C.** Data custodian

❍ **D.** Security auditor

55. Which of the following is the proper formula for calculating ALE?

❍ **A.** Single loss expectancy (SLE) × Annualized rate of occurrence (ARO)

❍ **B.** Asset value × Annualized rate of occurrence (ARO)

❍ **C.** Single loss expectancy (SLE) × Annualized rate of occurrence (ARO)

❍ **D.** Asset value / Annualized rate of occurrence (ARO)

56. Which of the following best describes a qualitative assessment?

❍ **A.** A qualitative assessment deals with real numbers and seeks to place dollar values on losses. These dollar amounts are then used to determine where to apply risk controls.

❍ **B.** A qualitative assessment assigns a rating to each risk.

❍ **C.** A qualitative assessment is performed by experts or external consultants who seek to place dollar values on losses.

❍ **D.** A qualitative assessment is performed by experts or external consultants, is based on risk scenarios, and assigns non-dollar values to risks.

57. Facilitated Risk Analysis Process (FRAP) is an example of what?

❍ **A.** A BCP analysis technique

❍ **B.** A quantitative assessment technique

❍ **C.** A DRP analysis technique

❍ **D.** A qualitative assessment technique

58. Classification levels like confidential and secret are tied to which data classification scheme?

❍ **A.** ISO 17799

❍ **B.** U.S. Department of Defense (DoD)

❍ **C.** RFC 2196 Site Security Guidelines

❍ **D.** Commercial Data Classification Standard (CDCS)

59. Which of the following methods of dealing with risk is considered the least prudent course of action?

❍ **A.** Risk reduction

❍ **B.** Risk rejection

❍ **C.** Risk transference

❍ **D.** Risk acceptance

60. Your employer is pleased that you have become CISSP certified and would now like you to evaluate your company's security policy. Your boss believes that encryption should be used for all network traffic and that a $50,000 encrypted database should replace the current customer database. Based on what you know about risk management, on what should you base your decision to use encryption and purchase the new database? Choose the most correct answer.

❍ **A.** If an analysis shows that there is potential risk, the cost of protecting the network and database should be weighed against the cost of the deterrent.

❍ **B.** If an analysis shows that the company's network is truly vulnerable, systems should be implemented to protect the network data and the customer database.

❍ **C.** If the network is vulnerable, systems should be implemented to protect the network and the database, regardless of the price.

❍ **D.** Because it is only a customer database and the company is not well known, the probability of attack is not great; therefore, the risk should be accepted or transferred through the use of insurance.

This page intentionally left blank

Answers to Practice Exam I

1. C
2. A 1
   B 1
   C 2
   D 3
3. C
4. D
5. D
6. B
7. B
8. B
9. B
10. D
11. D
12. C
13. D
14. A
15. B
16. B
17. A
18. B
19. B
20. C
21. B
22. D
23. A
24. C
25. C
26. A
27. B
28. C
29. B
30. D
31. B
32. B
33. D
34. D
35. A
36. B
37. C
38. D
39. A
40. D
41. C
42. B
43. A
44. A
45. D
46. B
47. D
48. D
49. A
50. C
51. D
52. B
53. A
54. A
55. B
56. B
57. D
58. B
59. B
60. D

Question 1

The correct answer is C. Attribute-based access control (ABAC) makes use of objects and environmental attributes that are checked by a policy decision point and a policy enforcement point against a policy. Answer A is incorrect because mandatory access control (MAC) uses labels. Answer B is incorrect because discretionary access control (DAC) leaves access control up to the owner's discretion. Answer D is incorrect because role-based access control (RBAC) models are used extensively by banks and other organizations that have very defined roles. See Chapter 6.

Question 2

The correct answer is shown in the table below. Information security models are a key topic that you can expect to be questioned on. While there are more than the four shown in this question, these are some of the most commonly tested models. Both Biba and Clark-Wilson are integrity models (which you can remember based on the fact that each has an i in its name). Bell-LaPadula is an example of a confidentiality model, and the primary purpose of Brewer and Nash is to prevent conflicts of interest. See Chapter 4.

Integrity (1)	Confidentiality (2)	Conflict of Interest (3)
Biba	Bell-LaPadula	Brewer and Nash
Clark-Wilson		

Question 3

The correct answer is C. Iris recognition functions by analyzing the features that exist in the colored tissue surrounding the pupil to confirm a match. These systems can analyze more than 200 points for comparison. Answer A is incorrect because retina scanning analyzes the layer of blood vessels in the eye. The retina is also more prone to change than the iris. Answer B is incorrect because cornea scanning does not exist. Answer D is incorrect because optic nerve scanning does not exist. See Chapter 6.

Question 4

The correct answer is D. The crossover error rate (CER) is as a percentage in which a lower number indicates a better biometric system. It is the most important measurement when attempting to determine the accuracy of a biometric system. Answers A and C are incorrect because there is no crossover acceptance rate. Answer B is incorrect because higher numbers are less accurate. See Chapter 6.

Question 5

The correct answer is D. A biometric system cannot examine all the detail in an object, or it will be prone to false rejection (Type I) errors. Answers A, B, and C are incorrect because Type I errors occur when legitimate users are improperly denied access. If these systems do not examine enough information about an object, however, they are prone to false acceptances (Type II) errors. Type II errors occur when unauthorized individuals are granted access to resources and devices they should not have. Fingerprints are fairly static metrics, and some systems are very accurate. You should know the difference between Type I and Type II errors and how CER is used. See Chapter 6.

Question 6

The correct answer is B. A 3- to 4-foot fence will deter casual trespassers. Answers A, C, and D do not correctly address the question: Fences 2 to 3 feet high can be easily crossed and would not be considered deterrents. Fences that are 5–7 feet high are more difficult to climb than shorter fences. Fences that are 8 feet high should be used to deter a determined intruder. See Chapter 6.

Question 7

The correct answer is B. The data owner, who is typically a member of senior management, is responsible for protecting company assets and data. Answer A is incorrect because the user is the individual who uses the documentation. Answer C is incorrect because the data custodian is responsible for maintaining and protecting the company's assets and data. Answer D is incorrect because an auditor makes periodic reviews of the documentation, verifies that it is complete, and ensures that users are following its guidelines. See Chapter 8.

Question 8

The correct answer is B. A vulnerability is a flaw, a loophole, an oversight, or an error that makes an organization susceptible to attack or damage. Answer A is incorrect because a risk is potential harm that can arise from an event. Answer C is incorrect because exposure is the amount of damage that could result from a vulnerability. Answer D is incorrect because a threat is a natural or human-caused event that could have some type of negative impact on an organization. See Chapter 3.

Question 9

The correct answer is B. The correct formula for determining single loss expectancy is Single loss expectancy = Asset value × Exposure factor. Answers A, C, and D are incorrect because none of them shows the correct formula. Factors to consider when calculating SLE include physical destruction or theft of assets, loss of data, theft of information, and threats that might cause delays in processing. See Chapter 3.

Question 10

The correct answer is D. Quantitative assessment deals with numbers and dollar amounts. It attempts to assign a cost (monetary value) to the elements of risk assessment and to the assets and threats of a risk analysis. To complete the assessment, first estimate potential losses, then conduct a threat analysis, and finally determine annual loss expectancy. Answers A, B, and C do not list the steps needed to perform a quantitative assessment. See Chapter 3.

Question 11

The correct answer is D. The Delphi technique is an example of a qualitative assessment technique. It is not used for quantitative assessment, DRP, or BCP; therefore, answers A, B, and C are incorrect. See Chapter 3.

Question 12

The correct answer is C. The formula for total risk is Threat × Vulnerability × Asset value. Answers A, B, and D are incorrect because they do not show how to find total risk. See Chapter 3.

Question 13

The correct answer is D. Risk acceptance means that the risk has been analyzed, and the individuals responsible have decided that they will accept this risk. Answer A is incorrect because risk reduction involves implementing a countermeasure to alter or reduce the risk. Answer B is incorrect because risk rejection means that the responsible party has decided to ignore the risk. Answer C is incorrect because risk transference involves transferring the risk to a third party, such as an insurer. See Chapter 3.

Question 14

The correct answer is A. Protection rings support the security of a system. Layer 0 is the most trusted ring, and the security kernel resides at layer 0. Answers B, C, and D are incorrect because the security kernel is not located in layer 1, layer 2, or layer 4. See Chapter 4.

Question 15

The correct answer is B. Answers A, C, and D would all work; the question asks which would not work. Authentication Header (AH) checks the integrity of an IP address and is intrinsically incompatible with Network Address Translation (NAT). See Chapter 5.

Question 16

The correct answer is B. Registers are considered temporary storage units within a CPU. A CPU consists of registers, an arithmetic/logic unit (ALU), and control circuitry. Answers A, C, and D are incorrect because the I/O buffers, control circuitry, and the ALU are not considered temporary storage units in the CPU. See Chapter 4.

Question 17

The correct answer is A. The Biba model, which was published in 1977, was the first model developed to address integrity. Its goal is to prevent unauthorized users from making changes to the system and addresses only one goal: integrity (outsiders). Answer B is incorrect because although the Clark-Wilson model is based on integrity, it was not the first model. Answer C is incorrect because the Brewer and Nash model is based on confidentiality. Answer D is incorrect because the Chinese Wall is another name for the Brewer and Nash model. See Chapter 4.

Question 18

The correct answer is B. Bell-LaPadula was the first model to address confidentiality. It was developed in the 1970s and was considered groundbreaking because it supported multilevel security. Although it is well suited for the DoD and government, it is not well suited for modern commercial entities. Answer A is incorrect because the Biba model is an integrity model. Answer C is incorrect because the Graham-Denning model was not the first confidentiality-focused model to be developed. Answer D is incorrect because the Clark-Wilson model is another example of an integrity model. See Chapter 4.

Question 19

The correct answer is B. Dynamic application security testing (DAST) is a blackbox testing technique that involves inspecting an application at runtime for vulnerabilities. Answer A is incorrect because interactive application security testing (IAST) involves placing an agent within an application and performing all its analysis in the app in real time and anywhere in the development process. Answer C is incorrect because runtime application security protection (RASP) works inside an application but is more a security tool than a testing technique. RASP is designed to control an application's execution. Answer D is incorrect because static application security testing (SAST) is considered whitebox testing and helps developers find security vulnerabilities in the application source code earlier in the software development lifecycle. See Chapter 4.

Question 20

The correct answer is C. Compartmented security mode requires all subjects to have a clearance for most restricted information and a valid need to know. Answer A is not correct because a dedicated security mode would require a clearance for *all* information; this question requires a security clearance for most, not all, information. Answer B is not correct because a system high security mode must have a clearance for all information and a valid need to know for some information. This scenario requires a clearance for most restricted information and a valid need to know. Answer D is not correct because with a multilevel mode, some subjects do not have clearance for all information, and each subject has a need to know for all information he or she will access. CISSP candidates must know the four different security modes of operation. See Chapter 4.

Question 21

The correct answer is B. During the actual exam expect to see some enhanced questions that feature figures or diagrams. There are two methods by which PKI revocation can be handled. The first is through use of a CRL, which is generated and published periodically or after a certificate has been revoked. The second method is to use OCSP, which does not mandate encryption, discloses that a particular network host used a specific certificate, and generally places less burden on client resources. It does not contain more information. See Chapter 4.

Question 22

The correct answer is D. The foreign key refers to an attribute in one table whose value matches the primary key in another table. Answer A is incorrect because a field is the smallest unit of data within a database. Answer B is incorrect because aggregation refers to the process of combining several low-sensitivity items, with the result that these items produce a higher-sensitivity data item. Answer C is incorrect because a composite key is two or more columns that are together designated as the computer's primary key. See Chapter 9.

Question 23

The correct answer is A. Bluetooth uses frequency-hopping spread spectrum (FHSS). FHSS functions by modulating the data with a narrowband carrier signal that hops in a random but predictable sequence from frequency to frequency. Bluetooth can be susceptible to Bluejacking and other forms of attack. Answer B is incorrect because 802.11a uses orthogonal frequency-division multiplexing. Answer C is incorrect because 802.11b uses direct-sequence spread spectrum (DSSS) technology. Answer D is incorrect because LiFi uses light to transmit data and position between devices. See Chapter 5.

Question 24

The correct answer is C. Virtual Extensible LAN (VXLAN) is a technology designed to provide the same Ethernet Layer 2 network services as a VLAN but with greater extensibility and flexibility. VXLAN supports the virtualization of a data center network while addressing the needs of multi-tenant data centers by providing the necessary segmentation on a large scale. Answer A is incorrect because a virtual LAN (VLAN) is any broadcast domain that is partitioned from one or more existing LANs. A virtual LAN is administered like a physical LAN. Answers B and D are incorrect because a trunk is simply a link between two switches that carries the data of more than one VLAN and CDMA is a method for cellular phone transmission. See Chapter 5.

Question 25

The correct answer is C. Twenty-four DS0 lines are bundled to make one T1. A T1 line has a composite rate of 1.544 Mbps. Answers A, B, and D are incorrect because 18-, 21-, and 32-DS0 line bundles do not exist. See Chapter 5.

Question 26

The correct answer is A. Microsegmentation is a security technique that breaks data centers and cloud environments into segments down to the individual workload level. Answer B is incorrect because while firewalls were the original segmentation model their aggressive use would not allow for efficient network operations. Answer C is incorrect because zero trust is based on the principle of maintaining strict access controls and not trusting anyone regardless if they are outside or already inside the network perimeter. Answer D is incorrect because a SDWAN manages a LAN or service provider's core network and is programmable by the user to deliver bandwidth on demand. See Chapter 5.

Question 27

The correct answer is B. Transaction persistence means that the state of a database's security is the same before and after a transaction occurs, and there is no risk of integrity problems. Answer A is incorrect because it does not define transaction persistence. Answer C is incorrect because transaction persistence does not state that the database should be the same before and after a transaction. Answer D is incorrect because even though databases should be available to multiple users at the same time without endangering the integrity of the data, that is not a definition of transaction persistence. See Chapter 9.

Question 28

The correct answer is C. Aggregation is the capability to combine data from separate sources to gain information. Answer A is incorrect because metadata is data about data. Answer B is incorrect because inference attacks occur when authorized users infer information by analyzing the data they have access to. Answer D is incorrect because deadlocking is a database stalemate. See Chapter 9.

Question 29

The correct answer is B. A TOC/TOU attack can occur when the contents of a file change between the time the system security functions check the contents of the variables and the time when the variables are actually used or accessed. This is a form of asynchronous attack. Answer A is incorrect because the description describes an asynchronous attack. Answer C is incorrect because the example does not describe a DCOM attack. Answer D is incorrect because a pass the hash attack is an attack in which an attacker authenticates to a remote server or service by using the underlying NTLM or Lanman hash of a user's password. See Chapter 4.

Question 30

The correct answer is D. Hearsay evidence is not based on personal knowledge but is information that was told to a witness by another person. It is inadmissible in a court of law. Answer A is incorrect because best evidence is the preferred type of evidence. Answer B is incorrect because secondary evidence is admissible and is usually a copy of original evidence. Answer C is incorrect because conclusive evidence is also admissible. See Chapter 8.

Question 31

The correct answer is B. Cipher Block Chaining (CBC) builds a dependency between the blocks of data. To find the plaintext of a particular block, you need to know the ciphertext, the key, and the ciphertext for the previous block. This feature makes CBC unique. Answer A is incorrect because electronic code book is fast but not chained or secure. Answer C is incorrect because Cipher Feedback (CFB) can be used to emulate a stream cipher and features a feedback function. Answer D is incorrect because Output Feedback (OFB) can also emulate a stream cipher and can pregenerate the key stream, independently of the data. See Chapter 4.

Question 32

The correct answer is B. 2DES, or Double DES, is no more secure than single DES and is susceptible to meet-in-the-middle attacks. Answers A, C, and D are incorrect because none of these forms of DES are susceptible to meet-in-the-middle attacks. See Chapter 6.

Question 33

The correct answer is D. Elliptic curve cryptosystem (ECC) is an asymmetric cryptosystem created in the 1980s to make and store digital signatures in a small amount of memory. Answer A is incorrect because DES is a symmetric algorithm. Answer B is incorrect because SHA1 is a hashing algorithm. Answer C is incorrect because Diffie-Hellman is used for key exchange. See Chapter 4.

Question 34

The correct answer is D. The purpose of the red team is to penetrate security. Red teams are sometimes called tiger teams or penetration testers. Answers A, B, and C are incorrect because individuals from all those groups should be involved in the contingency planning process. See Chapter 9.

Question 35

The correct answer is A. Attackers can attack ARP by flooding a switch and other devices with bogus MAC addresses or through ARP poisoning. Answer B is incorrect because although spanning tree is a valid attack, it is typically used for DoS. Answer C is incorrect because name server poisoning is another type of DNS attack. Answer D is incorrect because a reverse lookup is a term associated with DNS, not ARP. See Chapter 5.

Question 36

The correct answer is B. EAP is a strong form of authentication that uses more advanced methods of authentication besides passwords. Answers A, C, and D are incorrect because none of these methods use more advanced forms of authentication, such as digital certificates. See Chapter 5.

Question 37

The correct answer is C. RFC 1918 specifies the addresses that are to be used for private address schemes. Addresses 172.16.0.0 to 172.63.255.255 are not part of the specified range; therefore, answer C is the correct choice. Answers A, B, and D are incorrect because RFC 1918 specifies 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255. See Chapter 5.

Question 38

The correct answer is D. Stealing email is not difficult because it is plaintext and easily sniffed. Email is one of the most popular Internet applications and deserves protection. Although answers B and C are incorrect, they describe potential vulnerabilities in standard email. Answer A is incorrect because encryption is not difficult. See Chapter 5.

Question 39

The correct answer is A. Instant messaging (IM) has the capability for scripting, which is one reason it is dangerous for an organization. Answers B, C, and D do not properly answer the question because they are all reasons IM is vulnerable. IM can bypass corporate firewalls, most versions lack encryption, and IM uses insecure password management. See Chapter 8.

Question 40

The correct answer is D. The Distributed Component Object Model (DCOM) allows applications to be divided into pieces and objects to be run remotely over the network. Potential vulnerabilities exist because of the way ActiveX is integrated with DCOM. Answer A is incorrect because Java is not associated with DCOM and is primarily used as a simple, efficient, general-purpose language. Answer B is incorrect because CORBA is a set of standards that addresses the need for interoperability between hardware and software. Answer C is incorrect because Enterprise JavaBeans (EJB) is designed for enterprise networks. See Chapter 9.

Question 41

The correct answer is C. Pretty Good Privacy (PGP) uses a web-like model because there are no certificate authorities (CAs); there are only end users. Anyone who uses PGP must determine whom to trust because, without a CA, there is no centralized or governing agency to control and validate other users. Answer A is incorrect because PKI does not use a web of trust. Answer B is incorrect because IGMP is used for multicast router group management. Answer D is incorrect because Domain Keys Identified Mail (DKIM) is an email authentication technique that allows the receiver to check that an email was indeed sent and authorized by the owner of the domain. See Chapter 5.

Question 42

The correct answer is B. Entrapment is considered the act of tricking a person to commit a crime in order to bring criminal charges against him or her. Although entrapment is illegal, enticement usually is not. Answer A is incorrect because inducement is the act of bringing about the desired result. Answer C is incorrect because a honeypot is a trap set to detect or slow attempts at unauthorized use of information systems. Answer D is incorrect because enticement is the act of influencing by exciting hope or desire. See Chapter 7.

Question 43

The correct answer is A. The G8 is a group of economically advanced nations that have agreed to work together to solve economic problems. The G8 has now grown to 20 members and is also known as the G20. Answer B is incorrect because mutual legal assistance treaties (MLATs) are agreements that U.S. law-enforcement agencies have with law-enforcement agencies in other nations to fight computer crime and terrorism. MLATs are created to improve the effectiveness of judicial assistance and to regularize and facilitate cooperation. Answer C is incorrect because SWAT is a term used for special weapons and tactics police teams. Answer D is incorrect because UN Resolution 1154 deals with weapons inspections in Iraq. See Chapter 8.

Question 44

The correct answer is A. The five main types of BCP testing strategies are checklist, structured walkthrough, simulation, parallel, and full interruption. Therefore, answers B, C, and D are incorrect because the question asked which is not a valid type. Answer A is correct because partial interruption is not one of the five valid types. See Chapter 8.

Question 45

The correct answer is D. Business, facility and supply, user, technical, and data are the five primary categories in a business continuity plan. Answers A, B, and C are incorrect because they do not describe the five categories. See Chapter 7.

Question 46

The correct answer is B. APIs provide developers the ability to bypass traditional web pages and interact directly with the underlying service. Answer A is incorrect because SOAP does not allow direct access to the underling service. SOAP allows communication via the Internet between two programs on the same or different platforms. Answer C is incorrect as OAuth is an authentication protocol. Answer D is incorrect as REST is a software architectural style which uses a subset of HTTP. See Chapter 9.

Question 47

The correct answer is D. Hosts use Internet Group Management Protocol (IGMP) to report multicast group memberships to neighboring multicast routers. Security problems exist with IGMP because anyone can start a multicast group or join an existing one. Answer A is incorrect because ICMP is used for logical errors and diagnostics. Answer B is incorrect because Routing Information Protocol (RIP) is a broadcast-based routing protocol. Answer C is incorrect because although 224.0.0.1 is a multicast address, it is not a protocol used for multicast management. See Chapter 5.

Question 48

The correct answer is D. VoIP is very time sensitive and, as such, should be based on an isochronous design. This means that the entire system must be engineered to deliver output with exactly the same timing as the input. Answer A is incorrect because VoIP does not use time-division multiplexing. Answer B is incorrect because VoIP uses UDP, not TCP, for the voice portion of a call. Some implementations of VoIP can use TCP for setup and call control. Answer C is incorrect because VLANs are not used for timing and delay problems, but are used to separate VoIP traffic from general traffic to make it more secure from sniffing. See Chapter 5.

Question 49

The correct answer is A. ATM creates a fixed channel, or route, between two points whenever data transfer begins, and it packages the data into 53-byte fixed-length cells. ATM can be used in LANs, WANs, and MANs. It supports high-bandwidth data needs. Answer B is incorrect because ISDN provides a completely end-to-end digital connection. Answer C is incorrect because Switched Multimegabit Data Service (SMDS) is a low-market-share service used to interconnect LANs. Answer D is incorrect because microsegmentation

Question 50

The correct answer is C. One issue with WEP is the initialization vector (IV), which is 24 bits, not 20. Answers A, B, and D list some of the vulnerabilities of WEP. For example, WEP uses a single shared key among all clients, which means that it authenticates groups, not devices or single users. Also, RC4 is the correct encryption type and can be implemented in 40- or 104-bit configuration, but WEP does not properly initialize it. This means the key values roll over and are predictable. Finally, a 24-bit IV vector is too short, and a 40-bit key is weak. See Chapter 5.

Question 51

The correct answer is D. The formula for annual loss expectancy is:

$$ALE \times ARO = SLE\text{, or } 0.95 \times 720 = \$684$$

Annual rate of occurrence = 95%, or 0.95

$$\text{Single loss expectancy} = (\$9 \text{ per hour} \times 8 \text{ hours per employee}) \times 10 \text{ employees} = \$720$$

Therefore, the nonprofit could expect to lose $684 by not using antivirus software. See Chapter 3.

Question 52

The correct answer is B. An evaluation that is carried out and meets evaluation assurance level (EAL) 2 specifies that the design has been structurally tested. Answers A, C, and D are incorrect because EAL 1 = functionality tested; EAL 4 = methodically designed, tested, and reviewed; and EAL 5 = semiformally designed and tested. See Chapter 4.

Question 53

The correct answer is A. Microsegmentation is a countermeasure that can be used to mitigate lateral movement. It involves breaking data centers and cloud environments into individual workload level segments to enhance security. Answer B is incorrect because zero trust is based on the concept that organizations should not automatically trust anything inside or outside its perimeters. Answer C is incorrect because port mirroring is used on a network switch to send a copy of network packets seen on one switch port to another. Answer D is incorrect because enforced governance compliance would not specifically prevent lateral movement. See Chapter 5.

Question 54

The correct answer is A. The star (*) property rule states that someone at one security level cannot write information to a lower security level. Answer B is incorrect because the simple security rule states that someone cannot read information at a higher security level. Answer C is incorrect because the simple integrity property deals with the Biba model, not Bell-LaPadula. Answer D is incorrect because the strong star rule states that read and write privileges are valid only at the level at which the user resides. See Chapter 4.

Question 55

The correct answer is B. Annual loss expectancy is calculated this way:

ALE = ARO × SLE, or 0.95 × 720 = $684

The annual savings is the ALE minus the cost of the deterrent, or $684 – $399 = $285. Therefore, answers A, C, and D are incorrect See Chapter 3.

Question 56

The correct answer is B. Physical security is considered the first line of defense against human attack. Items such as gates, guards, locks, and cameras can be used for physical defense. Answer A is incorrect because cryptography is best used to protect the integrity and confidentiality of data. Answer C is incorrect because business continuity planning should be used to prevent critical outages. Answer D is incorrect because policies are an administrative control. See Chapter 6.

Question 57

The correct answer is D. HVAC should be a closed-loop system with positive pressurization. Closed loop means that the air inside the building is filtered and continually reused. Positive pressurization should be used to ensure that inside air is pushed out. This is an important safety feature in the event that the building catches fire. Answers A, B, and C are incorrect because they do not specify both closed-loop system and positive pressurization. See Chapter 6.

Question 58

The correct answer is B. Heat-activated sensors can be either rate-of-rise or fixed-temperature sensors. Answer A is incorrect because flame-activated sensors respond to the infrared energy that emanates from a fire. Answer C is incorrect because smoke-activated sensors use a photoelectric device. Answer D is incorrect because there is no category of fire detector known as ion activated. See Chapter 8.

Question 59

The correct answer is B. Electrical fires are considered Class C fires. All other answers are incorrect. Class A fires consist of wood and paper products, Class B fires consist of liquids such as petroleum, and Class D fires result from combustible metals. See Chapter 8.

Question 60

The correct answer is D. A dry-pipe system is the preferred fire suppression method for locations that are unheated or subject to freezing. Dry-pipe systems are unique in that they use pressurized air or nitrogen. In the event of a fire, the sprinkler head opens and releases the pressurized air. Although these systems do typically use a clapper valve, the term is used here because it might be unfamiliar to many readers. The exam might also use terms that you are not familiar with. All other answers are incorrect because deluge systems release large amounts of water in a very short period of time, wet-pipe systems hold water in the pipes, and pre-action systems release water into the pipe only when a specified temperature or separate detection device triggers its release. See Chapter 8.

Answers to Practice Exam II

1. D
2. D
3. B
4. A
5. D
6. B
7. C
8. A
9. A
10. B
11. B
12. D
13. B
14. C
15. B
16. A
17. D
18. B
19. B
20. C
21. C
22. D
23. C
24. B
25. C
26. D
27. C
28. D
29. C
30. B
31. B
32. D
33. A
34. C
35. A
36. B
37. C
38. B
39. B
40. C
41. A
42. A
43. C
44. B
45. D
46. A
47. B
48. D
49. B
50. D
51. A
52. A
53. C
54. C
55. C
56. D
57. D
58. B
59. B
60. A

Question 1

The correct answer is D. A fence will not prevent a determined intruder. Although fences can deter an intruder, a determined individual could drive through the fence, cut the fence, blow up the fence, or find another way through. The best design to deter a determined intruder is 8 feet high with three strands of barbed/razor wire. See Chapter 6.

Question 2

The correct answer is D. Class D fires result from combustible metals. All other answers are incorrect: Class A fires consist of wood and paper products, Class B fires consist of liquids such as petroleum, and Class C fires are electrical fires. See Chapter 8.

Question 3

The correct answer is B. Defense in depth can be presented in many ways. It can be layers of the same control or different controls. The outer layer is physical/preventive/deterrent, the second layer is technical/preventive/detective, and the third layer is administrative/preventive. When facing this type of question, always identify which type of control you are dealing with: physical, administrative, or technical. Then determine the purpose of the control: detective, preventive, corrective, and so on. See Chapter 3.

Question 4

The correct answer is A. Magnetic strip card keys contain rows of copper strips. Answers B, C, and D are incorrect: Electronic circuit card keys have embedded electronic circuits, magnetic stripe card keys have stripes of magnetic material, and active electronic cards can transmit data. See Chapter 6.

Question 5

The correct answer is D. Hard-drive encryption offers the best defense against the loss of confidentiality. Answer A is incorrect because integrity programs validate the integrity of installed software but do not validate its confidentiality. Answer B is incorrect; reward labels might or might not encourage someone to return equipment, but they definitely will not protect data confidentiality. Answer C is incorrect because locking cables might prevent someone from removing a laptop but won't prevent someone from accessing data on the device. See Chapter 2.

Question 6

The correct answer is B. If halon is deployed in concentrations greater than 10% and in temperatures of 900°F or more, it degrades into hydrogen fluoride, hydrogen bromide, and bromine. This toxic brew can be deadly. Answers A, C, and D are incorrect because concentrations must be 10% or greater, and temperatures must reach 900°F. See Chapter 8.

Question 7

The correct answer is C. The NIST standard for perimeter protection using lighting specifies that critical areas should be illuminated with 2 foot-candles of illuminance at a height of 8 feet. Answers A, B, and D do not match the NIST standards. See Chapter 6.

Question 8

The correct answer is A. A Type I error occurs when a biometric system denies an authorized individual access. Answer B is incorrect because a Type II error occurs when an unauthorized individual is granted access. Answers C and D are incorrect because Type III and IV errors do not exist. See Chapter 6.

Question 9

The correct answer is A. When comparing biometric systems, the most important item to consider is the crossover error rate (CER). The CER is the point at which the false acceptance rate meets the false rejection rate. The CER indicates the accuracy of the biometric system. Answers B, C, and D are incorrect because there are no biometric measurements known as error acceptance rate, crossover acceptance rate, or failure acceptance rate. See Chapter 6.

Question 10

The correct answer is B. RSA's SecurID is an example of synchronous authentication. An RSA SecureID device or token uses a one-time password and a clock that synchronizes the authenticator to the authentication server during the authentication process. Each individual passcode is valid for only a very short period—normally 60 seconds or less—and is used with a username and password for two-factor authentication. Answer A is incorrect because RSA's SecurID might be part of an SSO system, but this is not an accurate answer. Answer C is incorrect because although the RSA's SecurID fob might be considered a token, it is not the best answer available out of the four. Answer D is incorrect because asynchronous authentication devices are not synchronized to the authentication server; rather, these devices use a challenge-response mechanism. See Chapter 6.

Question 11

The correct answer is B. LEAP is considered a weak version of EAP. It makes use of a modified version of CHAP and therefore does not adequately protect the authentication process. Answers A (EAP-FAST), C (PEAP), and D (EAP-TLS) are all strong versions of EAP. See Chapter 5.

Question 12

The correct answer is D. Breach of single sign-on (SSO) can enable an attacker to access many systems that are tied to SSO when authenticated only once. Answer A is incorrect because SSO does not involve a lot of maintenance and overhead. Answer B is incorrect because although SSO systems such as Kerberos do require clock synchronization, this is not the overriding security issue. Answer C is incorrect because every system has some type of flaw or drawback. See Chapter 6.

Question 13

The correct answer is B. Snort started as a signature-based IDS. Today, Snort has grown to include behavior-based features. A signature-based system examines data to check for malicious content. When data is found that matches a known signature, it can be flagged to initiate further action. Answer A is incorrect because Snort is not a behavior-based IPS. Answer C is incorrect because Snort is not a behavior-based IDS. Answer D is incorrect because although Snort is signature based, it is considered an IDS, not an IPS. IPSs are unlike IDSs in that IPSs have much greater response capabilities and allow administrators to initiate action upon being alerted. See Chapter 6.

Question 14

The correct answer is C. Asynchronous attacks are sometimes called race conditions because the attacker is racing to make a change to an object before it is used by the system. Asynchronous attacks typically target timing. The objective is to exploit the delay between the time of check (TOC) and the time of use (TOU). Answers A, B, and D are incorrect because they do not adequately describe a race condition. See Chapter 4.

Question 15

The correct answer is B. Rings of protection run from layer 0 to layer 3. Layer 2 is the location of I/O drivers and utilities. Answers A, C, and D are incorrect because layer 1 contains parts of the OS that do not reside in the kernel, layer 3 contains applications and programs, and layer 0 is the location of the security kernel. See Chapter 4.

Question 16

The correct answer is A. Multiprogramming CPUs can interleave two or more programs for execution at any one time. Answer B is incorrect because multitasking CPUs have the capability to perform one or more tasks or subtasks at a time. Answer C is incorrect because there is no type of processor known as multiapp. Answer D is incorrect because the term *multiprocessor* refers to systems that have the capability to support more than one CPU. See Chapter 4.

Question 17

The correct answer is D. The ALU portion of the CPU performs arithmetic and logical operations on the binary data. Answers A, B, and C are incorrect because I/O buffers, registers, and the control circuits do not perform arithmetic and logical operations. See Chapter 4.

Question 18

The correct answer is B. The Biba model is integrity based and does not allow a subject to write to a higher security level or read from a lower security level. Answer A is incorrect because the Bell-LaPadula model is based on confidentiality. Answer C is incorrect because the state machine model seeks to determine whether one state is valid before moving to another. Answer D is incorrect because the Clark-Wilson model is an integrity model and is designed to address integrity. See Chapter 4.

Question 19

The correct answer is B. The Lockheed Martin Cyber Kill Chain framework has seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command and controls, and actions. Therefore, answers A, C, and D are incorrect. See Chapter 7.

Question 20

The correct answer is C. Containerization has become a major trend in software development as an alternative or companion to virtualization. Containerization involves encapsulating or packaging software code and all its dependencies so that it can run uniformly and consistently on any infrastructure. Answers A, B, and D are incorrect. Microservices architecture enables rapid, frequent, and reliable delivery of large, complex applications. Serverless defines apps deployed in containers that automatically launch on demand when called. An embedded system is a combination of a computer processor, computer memory, and input/output that has a dedicated function within a larger mechanism, such as IoT or SCADA. See Chapter 5.

Question 21

The correct answer is C. The trusted computing base (TCB) is the totality of protection mechanisms within a computer system, including hardware, firmware, software, processes, and some interprocess communications. These items are responsible for enforcing security. Answer A is incorrect because rings of protection are designed to protect the operating system. Answer B is incorrect because the security kernel is the most trusted portion of the operating system. Answer D is incorrect because although resource isolation is an important part of implementing security, it is not the totality of protection mechanisms. See Chapter 4.

Question 22

The correct answer is D. Session Initiation Protocol (SIP) is an application-layer request/response protocol used for VoIP. SIP is transported by UDP, makes use of TCP, and is vulnerable to sniffing attacks. More details can be found in RFC 2543. Answer A is incorrect because there is no protocol called SKYP; the proprietary product Skype offers encryption and is used for a peer-to-peer Internet phone service. Answer B is incorrect because SLIP is used by ISPs for dialup connections. Answer C is incorrect because S/MIME is used to secure email. See Chapter 5.

Question 23

The correct answer is C. 802.11b uses direct-sequence spread spectrum (DSSS) technology. DSSS is a transmission method that transmits the data along with a chipping bit to increase the signal's resistance to interference. Answer A is incorrect because Bluetooth uses frequency-hopping spread spectrum. Answer B is incorrect because 802.11a uses orthogonal frequency-division multiplexing. Answer D is incorrect because 802.11ac uses MIMO-OFDM. See Chapter 5.

Question 24

The correct answer is B. A rogue AP is an unauthorized AP attached to a corporate network. Rogue APs are some of the biggest threats to a secure network. Answer A is incorrect because a connection to an unauthorized modem is not a valid answer. Answer C is incorrect because a rogue AP is not a modem. Answer D is incorrect because a connection to an unsecured network is not a rogue AP but might be considered an act of war driving. See Chapter 5.

Question 25

The correct answer is C. A Fagan inspection is to make sure that all the documentation is correct and clear for understanding, created up to standard during a code review. Usually the inspection team checks test cases, specifications, and code. Answers A, B, and D are incorrect because fuzzing is associated with misuse testing, synthetic transactions are used for stress testing, and RASP is designed to detect attacks in real time and functions to monitor the execution of the application. See Chapter 7.

Question 26

The correct answer is D. T1s use time division to break the individual DS0s into 24 separate channels. Time division is the allotment of available bandwidth based on time. It allows a T1 to carry both voice and data at the same time. Answer A is incorrect because there is no system known as channel division. Answer B is incorrect because FHSS is used by mobile devices. Answer C is incorrect because T1s do not use frequency division. See Chapter 5.

Question 27

The correct answer is C. A disaster recovery plan (DRP) focuses on how to repair and restore a data center and the information at an original or new primary site. Answer A is incorrect because a business continuity plan (BCP) is focused on the continuation of critical services. Answer B is incorrect because business continuity management (BCM) is about building a framework for a capable response. Answer D is incorrect because a business impact analysis (BIA) is a functional analysis used to identify the potential impact of an outage. See Chapter 8.

Question 28

The correct answer is D. Software escrow agreements are used to provide protection for source code in the event that the manufacturer declares bankruptcy or goes broke. The three items that are most critical in this type of agreement are where the code will be deposited, under what conditions the code will be released, and the terms of use of the source code upon its release to the user. Answer A is incorrect because government access to keys deals with the government's desire to maintain cryptographic keys used by industry. Answer B is incorrect because mutually assured destruction (MAD) is a term not associated with software protection. Answer C is incorrect because electronic vaulting is a term that describes the bulk transfer of data. See Chapter 8.

Question 29

The correct answer is C. The Safe Harbor Act is a cooperative effort between the United States and Europe to exchange information about European citizens between European firms and North American parent corporations. It was enacted because a large number of individuals have been victims of identity theft and to deal with the increase in misuses of personal information laws and agreements. Answer A is incorrect because although SB 168 deals with privacy, it is a state law that took effect in 2002, preventing businesses from using California residents' Social Security numbers as unique identifiers. Answer B is incorrect because there is no law known as the Demar Act. Answer D is incorrect because the name of the act is not Safety Shield. See Chapter 3.

Question 30

The correct answer is B. A bit copy, or physical copy, captures all the data on the copied medium and produces an exact copy that includes hidden and residual data, slack space, swap contents, deleted files, and other data remnants. It allows an examiner to perform an analysis of the copy and store the original. Answer A is incorrect because a logical copy does not completely duplicate the structure of the original media. Answer C is incorrect because Microsoft Backup is not an approved product for forensic analysis. Answer D is incorrect because although Xcopy can duplicate files, it does not provide a bit-level copy of the original medium. See Chapter 8.

Question 31

The correct answer is B. Secure Electronic Transaction (SET) was developed by MasterCard and Visa to be used on the Internet for credit card transactions. It uses digital signatures. Answer A is incorrect because SET is not used for digital signatures. Answer C is incorrect because SET is not used for key exchange, and Victor Miller and Neal Koblitz are the creators of ECC. Answer D is incorrect because SET does not use SSL. See Chapter 5.

Question 32

The correct answer is D. Knowledge discovery in databases is an artificial intelligence method used to identify useful patterns in data; it provides a type of automatic analysis. Answer A is incorrect because polyinstantiation is a technique used to prevent inference violations. Answer B is incorrect because known signature scanning is a method used to detect computer viruses. Answer C is incorrect because an application programming interface (API) is not associated with artificial intelligence. See Chapter 9.

Question 33

The correct answer is A. Although RFC 1035 does allow DNS lookups over TCP, this service is provided for only when lookups are greater than 512 bytes; typically UDP port 53 is used. Answers B, C, and D are incorrect because UDP port 69 is used for TFTP, TCP port 53 is used for zone transfers, and UDP port 161 is used for SNMP. See Chapter 5.

Question 34

The correct answer is C. Running the md5sum hashing algorithm would be the best way for Bob to verify the program. Answer A is incorrect because AES is a symmetric algorithm and will not help Bob verify the program. Answer B is incorrect because the size and date might match the information found on the developer's website, but the program still might have been altered. Answer D is incorrect because a digital signature will not verify the integrity of the program. See Chapter 6.

Question 35

The correct answer is A. IMAP is associated with email, but it is not an email security standard; it is a protocol to receive email and excels compared to POP3 when working with mail on multiple devices/clients. It also leaves a copy on the server. Answers B, C, and D are all incorrect as they specify valid email security standards: MIME Object Security Services (MOSS), Pretty Good Privacy (PGP), and Privacy Enhanced Email (PEM). See Chapter 5.

Question 36

The correct answer is B. With link encryption, the message is decrypted and re-encrypted as it passes through each successive node, using a key common to the two nodes. Answers A, C, and D are incorrect because they all describe end-to-end encryption. See Chapter 5.

Question 37

The correct answer is C. Diameter uses RADIUS as a base and is considered the next generation of authentication, authorization, and accounting services for the Internet, with over 16 million attribute/variable pair (AVP) tags for negotiation. Answer A is incorrect because TACACS is not considered a base for Diameter. Answer B is incorrect because TACACS+ is a Cisco protocol that is widely used. Answer D is incorrect because Kerberos is not associated with Diameter but is considered a single sign-on technology. See Chapter 6.

Question 38

The correct answer is B. Programmers involved in database management talk about the ACID test when discussing whether a database management system has been properly designed to handle transactions. The ACID test addresses atomicity, consistency, isolation, and durability. Answer A is incorrect because the ACID test does not deal with behavior-based IDSs. Answer C is incorrect because ACID is not related to signature-based IDSs. Answer D is incorrect because the ACID test is not related to the strength of a cryptographic function. See Chapter 9.

Question 39

The correct answer is B. Redundant array of inexpensive tape (RAIT) is used to back up systems by means of a tape array that stripes the data across the tape. Answer A is incorrect because RAID is not typically used for backup. Answer C is incorrect because JBOD (just a bunch of disks) offers no backup or fault tolerance. Answer D is incorrect because SOAR (Security Orchestration, Automation, and Response) is not a type of tape backup but is used to respond to security events through playbooks and requires little to no human intervention. See Chapter 8.

Question 40

The correct answer is C. RC4 is a stream cipher. It has been implemented in products such as SSL and WEP. Answer A is incorrect because DES is a block cipher with a 56-bit key size. Answer B is incorrect because Camellia is a block cipher developed by Mitsubishi with a default 128-block size. Answer D is incorrect because Twofish is a 256-bit key size block cipher. See Chapter 4.

Question 41

The correct answer is A. Electronic Code Book (ECB) is fast and simple but is also the weakest mode of DES. Answer B is incorrect because Cipher Block Chaining (CBC) is not the weakest mode of DES. Answer C is incorrect because Cipher Feedback (CFB) is more secure than ECB and OFB. Answer D is incorrect because Output Feedback (OFB) is not the weakest, but it can't detect integrity errors as well as CFB. See Chapter 4.

Question 42

The correct answer is A. The statement "access and use of the Internet is a privilege and should be treated as such by all users" is part of RFC 1087, which is titled "Ethics and the Internet." Answer B is incorrect because the statement is not part of the (ISC)^2 Code of Ethics. Answer C is incorrect because the statement is not part of the Ten Commandments of Computer Ethics. Answer D is incorrect because RFC 1109 addresses network management, not ethics. See Chapter 7.

Question 43

The correct answer is C. The waterfall method is the oldest and one of the most well-known methods for developing software systems. It was developed in the 1970s and is divided into phases, each of which involves a list of activities that must be performed before the next phase can begin. Answer A is incorrect because the spiral model is a combination of the waterfall and prototyping methods. Answer B is incorrect because the clean room software development method focuses on ways to prevent defects rather than ways to remove them. Answer D is incorrect because the V-shaped waterfall model is an extension to the original waterfall model. See Chapter 9.

Question 44

The correct answer is B. A multipartite malware is not one of the techniques used by fileless malware. Answer A, C, and D are incorrect as all three are techniques used by fileless malware. Fileless infector can execute in one of several ways including windows registry manipulation, memory code injection, and script-based techniques. See Chapter 9.

Question 45

The correct answer is D. HTTPS uses TCP and port 443. Answer A is incorrect because port 80 is used for HTTP, answer B is incorrect because port 110 is used for POP3, and answer C is incorrect because port 111 is for Network File Service. See Chapter 5.

Question 46

The correct answer is A. Hierarchical databases link records in a tree structure so that each record type has only one owner. Hierarchical databases date from the information management systems of the 1950s and 1960s. Answer B is incorrect because network databases were not the first. Answer C is incorrect because although relational databases are the most widely used, they were not the first. Answer D is incorrect because object-oriented databases were not the first; they were designed to overcome some of the limitations of relational databases. See Chapter 9.

Question 47

The correct answer is B. The IEEE divides the OSI data link layer into sublayers. The upper half is the Logical Link Control (LLC) layer, and the lower half is the Media Access Control (MAC) layer. The LLC layer is based on HDLC; the MAC layer is where 802.3 addressing is performed. Answers A, C, and D are incorrect because none of these are sublayers of the data link layer. See Chapter 5.

Question 48

The correct answer is D. An access control matrix is used to associate the relationships and rights of subjects and objects. Answer A is incorrect because MAC uses security labels on objects and clearances for subjects. Answer B is incorrect because RBAC would be based on roles and containers, not users.

Answer C is incorrect because LBAC is based on the interaction between any combination of objects and subjects. LBAC provides upper and lower limits for a user. See Chapter 6.

Question 49

The correct answer is B. Subjects are the active entities, and objects are the passive entities. A subject does not have to be a person; it can be an application. However, in this scenario, the subject—the active entity—is the list of names. Answers A, C, and D are incorrect. Subjects are active, objects are passive, the mode of access is read or write. See Chapter 6.

Question 50

The correct answer is D. A service set ID (SSID) is used to identify an 802.11 network. An SSID is a 32-bit character string that acts as a shared identifier and that some describe as a very weak password. The SSID is used to differentiate one WLAN from another. Answer A is incorrect because a security ID (SID) is an identifier used in conjunction with Microsoft domains. Answer B is incorrect because a broadcast name is not a means of identifying a WLAN. Answer C is incorrect because Kismet is a Linux software program used to sniff wireless traffic. See Chapter 5.

Question 51

The correct answer is A. Threat intelligence leverages threat history and includes threat feeds, indicators of compromise (IoCs), and other pieces of threat actor activities that security analysts analyze and enrich. This information is used to look for persistent threats and zero-day exploits. Answers B, C, and D are incorrect because IDP, SIEM, and UEBA use machine learning, algorithms, and statistical analyses to detect deviations from established patterns. These anomalies may indicate potential or real threats. See Chapter 9.

Question 52

The correct answer is A. An evaluation that is carried out and meets evaluation assurance level (EAL) 1 specifies that the design has been functionality tested. Answers B, C, and D are incorrect because EAL 2 = structurally tested; EAL 4 = methodically designed, tested, and reviewed; and EAL 5 = semi-formally designed and tested. See Chapter 4.

Question 53

The correct answer is C. Clark-Wilson does not provide for the confidentiality of information; Clark-Wilson deals with integrity. Answers A, B, and D are all incorrect because the question asks which aspect Clark-Wilson does *not* address. See Chapter 4.

Question 54

The correct answer is C. A data custodian is responsible for maintaining and protecting a company's assets and data at a macro level. Answer A is incorrect because the user is the individual who uses the documentation. Answer B is incorrect because the data owner is responsible for protecting the data. Answer D is incorrect because the auditor makes periodic reviews of the documentation and verifies that it is complete and that users are following its guidelines. See Chapter 2.

Question 55

The correct answer is C. Single loss expectancy (SLE) × Annualized rate of occurrence (ARO) is the formula used to determine ALE. Answers A, B, and D are incorrect because these formulas are not used to calculate ALE. See Chapter 3.

Question 56

The correct answer is D. A qualitative assessment ranks the seriousness of threats and sensitivity of assets into grades or classes, such as low, medium, and high. It is performed by experts or external consultants and is based on risk scenarios. Although purely quantitative risk assessment is not possible, purely qualitative risk analysis is. Answers A, B, and C are incorrect because they do not adequately describe qualitative risk assessment. See Chapter 3.

Question 57

The correct answer is D. Facilitated Risk Analysis Process (FRAP) is an example of a qualitative assessment technique. It is not used for BCP, quantitative assessment, or DRP; therefore, answers A, B, and C are incorrect. See Chapter 3.

Question 58

The correct answer is B. The U.S. Department of Defense data classification standard classifies data as unclassified, sensitive, confidential, secret, and top secret. Answer A is incorrect because ISO 17799 is an international security standard policy. Answer C is incorrect because RFC 2196 is the Site Security Handbook and does not address data classification standards. Answer D is incorrect because there is no CDCS standard. See Chapter 2.

Question 59

The correct answer is B. Risk rejection is the least prudent course of action because it means that individuals have decided that risk does not exist and are ignoring it. Answer A is incorrect because risk reduction occurs when a countermeasure is implemented to alter or reduce the risk. Answer C is incorrect because risk transference involves transferring risk to a third party. Answer D is incorrect because risk acceptance means that risk is analyzed, but the responsible individuals have decided that they will accept the risk. See Chapter 4.

Question 60

The correct answer is A. Risk management requires that vulnerabilities be examined, that loss expectancy be calculated, that a probability of occurrence be determined, and that the costs of countermeasures be estimated. Only then can it be determined whether the value of an asset outweighs the cost of protection. Answer B is incorrect as typically you would not spend more on the countermeasure than the value of the asset. Answer C is incorrect as you would not typically implement a countermeasure regardless of the price. Answer D is incorrect as the risk must be evaluated before you can assess if insurance should or should not be used. Answer D is incorrect as it is possible for the cost of protection to outweigh the value of an asset. See Chapter 3.

This page intentionally left blank

Glossary

802.11 standard A legacy set of wireless LAN standards developed by Working Group 11 of the IEEE LAN/MAN Standards Committee. 802.11 is known for its use of WEP and RC4.

802.11i standard One of the replacements for 802.11. 802.11i uses WPA and AES.

A

Acceptable use policy (AUP) A policy that defines what employees, contractors, and third parties are authorized to do on an organization's IT infrastructure and its assets. AUPs are common for access to IT resources, systems, applications, Internet access, email access, and so on.

Access control A control that monitors the flow of information between a subject and an object. It ensures that only the operations permitted are performed.

Access control list (ACL) A table or list stored by a router to control access to and from a network by helping the device determine whether to forward or drop packets that are entering or exiting it.

Access creep The result of employees moving from one position to another within an organization without losing the privileges of the old position but gaining additional access in the new position. Thus, over time, employees build up much more access than they should have.

Access point spoofing The act of pretending to be a legitimate access point in order to trick individuals to pass traffic using the fake connection so that it can be captured and analyzed.

Accountability The traceability of actions performed on a system to a specific system entity or user.

Accreditation Management's formal acceptance of a system or an application.

ACID test A test that addresses atomicity, consistency, isolation, and durability. Programmers involved in database management use the ACID test to determine whether a database management system has been properly designed to handle transactions.

Active fingerprint An active method of identifying the operating system of a targeted computer or device that involves injecting traffic into the network.

Address Resolution Protocol (ARP) A protocol used to map a known IP address to an unknown physical address.

Ad hoc mode A mode that makes it possible for an individual computer to communicate directly with other client units, with no access point required. Ad hoc operation is ideal for small networks of no more than two to four computers.

Administrative law A body of regulations, rules, orders, and decisions to carry out regulatory powers, created by administrative agencies.

Advanced Encryption Standard (AES) The encryption standard that was originally known as Rijndael and serves as the replacement to DES.

Aggregation Collection of data from disparate sources.

Algorithm A mathematical procedure used for solving a problem. Commonly used in cryptography.

American Standard Code for Information Interchange (ASCII) A standard code for transmitting data, consisting of 128 letters, numerals, symbols, and special codes, each of which is represented by a unique binary number. An ASCII word typically is 8 bits of binary data.

Annualized loss expectancy (ALE) A quantifiable measurement of the impact that a threat will have on an organization if it occurs. ALE is used to calculate the possible loss that could occur over a one-year period. The formula is SLE × ARO = ALE.

Anomaly detection A type of intrusion detection that looks at behaviors that are not normal with standard activity. These unusual patterns are identified as suspicious.

Appender A virus infection type that places the virus code at the end of the infected file.

Applet A small Java program that can be embedded in an HTML page. Applets differ from full-fledged Java applications in that they are not allowed to access certain resources on the local computer, such as files and serial devices (modems, printers, and so on), and they are prohibited from communicating with most other computers across a network. An applet can make an Internet connection only to the computer from which the applet was sent.

Application A software program designed to perform a specific task or group of tasks, such as word processing, communication, or database management.

Application controls A category of controls used to verify the accuracy and completeness of records made using manual or automated processes. Controls used for applications include encryption, batch totals, and data input validation controls.

Application layer The highest layer of the seven-layer OSI model. The application layer is used as an interface to applications or communications protocols.

Application programming interface (API) A set of system-level routines that can be used in an application program for tasks such as basic input/output and file management. In a graphics-oriented operating environment such as Microsoft Windows, high-level support for video graphics output is part of the Windows graphical API.

Arithmetic logic unit (ALU) A device used for logical and arithmetic operations within a computer.

Artificial intelligence (AI) Computer software that can mimic the learning capability of a human.

Assembler A program that converts the assembly language of a computer program into the machine language of the computer.

Assessment An evaluation and/or valuation of IT assets based on predefined measurement or evaluation criteria. It is not typically necessary for an accounting or auditing firm to conduct an assessment, such as a risk or vulnerability assessment.

Asset Anything of value owned or possessed by an individual or a business.

Asymmetric algorithm A routine that uses a pair of different but related cryptographic keys to encrypt and decrypt data.

Asymmetric encryption In cryptography, a form of encryption in which an asymmetric key algorithm is used with a pair of cryptographic keys to encrypt and decrypt. The two keys are related mathematically: A message encrypted by the algorithm using one key can be decrypted by the same algorithm using the other. In a sense, one key locks the data, and a different key is required to unlock it.

Asynchronous Transfer Mode (ATM) Communication technology that uses high-bandwidth, low-delay transport technology and multiplexing techniques.

Asynchronous transmission A method whereby data is sent and received 1 byte at a time.

Attenuation A weakening of a signal that increases as the signal travels farther from the source.

Attribute-based access control (ABAC) A modern access control methodology in which access rights are granted by means of policies made up of attributes mapped to subjects and objects.

Audit An examination typically done by an accounting or auditing firm that conforms to a specific and formal methodology and definition for how an investigation is to be conducted, with specific reporting elements and metrics being examined (such as a financial audit according to public accounting and auditing guidelines and procedures).

Audit trail A set of records that collectively provide documentary evidence of processing that is used to aid in tracing from original transactions forward to related records and reports and/or backward from records and reports to their component source transactions.

Authentication A method of verifying that someone is who he or she purports to be. Authentication involves verifying the identity and legitimacy of an individual to access the system and its resources. Common authentication methods include passwords, tokens, and biometric systems.

Authorization The process of granting or denying access to a network resource based on a user's credentials.

Authorization creep A phenomenon that occurs when employees not only maintain old access rights but gain new ones. It results in too much access over time.

Availability One of the three items considered part of the security triad, in addition to confidentiality and integrity. It is a measure of the degree to which data or systems are available to authorized users.

B

Backdoor A piece of software that allows access to a computer without using the conventional security procedures. Backdoors are often associated with Trojans.

Back Orifice A backdoor program that infects the end user with a Trojan and gives the attacker the ability to remotely control the user's system.

Backup A copy of programs, databases, and other files that is made so that information can be restored in the event that it is lost due to, for instance, a computer failure, a natural disaster, or a virus infection.

Bandwidth The range of frequencies, expressed in hertz (Hz), that can pass over a given transmission channel. The bandwidth determines the rate at which information can be transmitted through the circuit.

Baseband The name given to a transmission method in which the entire bandwidth (the rate at which information travels through a network connection) is used to transmit just one signal.

Baseline A consistent or established base used to establish a minimum acceptable level of security.

Bayesian filter A technique used to detect spam. A Bayesian filter gives a score to each message based on the words and numbers in a message. These filters are often used by antispam software to filter spam based on probabilities. Messages with high scores are flagged as spam and can be discarded, deleted, or placed in a folder for review.

Bell-LaPadula A formal security model based on confidentiality that is defined by two basic properties:

- Simple security property (ss property): This property states that a subject at one level of confidentiality is not allowed to read information at a higher level of confidentiality. It is sometimes referred to as "no read up."
- Star (*) security property: This property states that a subject at one level of confidentiality is not allowed to write information to a lower level of confidentiality. Also known as "no write down."

Benchmark A standard test or measurement used to compare the performance of similar components or systems.

Binary code A sequence of 0s and 1s used by computer systems as the basis of communication.

Biometrics A method of verifying a person's identity for authentication by analyzing a unique physical attribute of the individual, such as a fingerprint, retina, or palm print.

Blackbox testing A form of testing in which the tester has no knowledge of the target or its network structure.

Block cipher An encryption scheme in which data is divided into fixed-size blocks, each of which is encrypted independently of the others.

Blowfish A form of symmetric block encryption designed in 1993.

Blu-ray disc A storage medium designed as a replacement for DVDs. Blu-ray is a high-density optical disk that can hold audio, video, or data.

Bluejacking The act of sending unsolicited messages, pictures, or information to a Bluetooth user.

Bluesnarfing The theft of information from a wireless device through a Bluetooth connection.

Bluetooth An open standard for short-range wireless communications of data and voice between both mobile and stationary devices. Used in cell phones, PDAs, laptops, and other devices.

Bollard A heavy round post used to prevent vehicles from ramming buildings or breaching physical security.

Botnet A term used to describe a collection of robot-controlled workstations.

Brewer and Nash model A security model developed to prevent conflict of interest (COI) problems.

Bridge A Layer 2 device for passing signals between two LANs or two segments of a LAN.

Broadband A wired or wireless transmission medium capable of supporting a wide range of frequencies, typically from audio up to video frequencies. It can carry multiple signals by dividing the total capacity of the medium into multiple independent bandwidth channels, with each channel operating on only a specific range of frequencies.

Broadcast A type of transmission used on local and wide area networks in which all devices are sent the information from one host.

Brute-force attack A method of breaking a cipher or an encrypted value that involves trying a large number of possibilities. Brute-force attacks function by working through all possible values. The feasibility of brute-force attacks depends on the key length and strength of the cipher and the processing power available to the attacker.

Buffer An amount of memory reserved for the temporary storage of data.

Buffer overflow In computer programming, a problem that occurs when a software application somehow writes data beyond the allocated end of a buffer in memory. Buffer overflow is usually caused by software bugs and improper syntax and programming that open or expose the application to malicious code injections or other targeted attack commands.

Bus A common channel shared among multiple computer devices.

Bus LAN configuration A LAN network design that was developed to connect computers used for 10BASE-5 and 10BASE-2 computer networks. All computers and devices are connected along a common bus or single communication line so that transmissions by one device are received by all.

Business case A document developed to establish the merits and desirability of a project. It contains the information necessary to enable approval, authorization, and policy-making bodies to assess a project proposal and reach a reasoned decision, as well as justify the commitment of resources to a project.

Business continuity plan (BCP) A document that describes how an organization will resume partially or completely interrupted critical functions within a predetermined time after a disaster or disruption occurs. The goal is to keep critical functions operational.

Business impact analysis (BIA) A component of a business continuity plan that looks at all the components that an organization relies on for continued functionality. It seeks to distinguish which components are more crucial than others and require more funds in the wake of a disaster.

C

Caesar cipher A basic ROT3 cipher that works by means of a substitution. Each letter is replaced with another letter from a fixed number of letters down the alphabet. A Caesar cipher is easily cracked.

Capability Maturity Model (CMM) A structured model designed by Carnegie Mellon's Software Engineering Institute to improve and optimize the software development lifecycle.

Carrier-sense multiple access with collision avoidance (CSMA/CA) An access method used by local area networking technologies such as Ethernet.

Carrier-sense multiple access with collision detection (CSMA/CD) An access method used by local area networking technologies such as token ring.

Catastrophe A calamity or misfortune that causes the destruction of a facility and/or data.

Central processing unit (CPU) One of the central components of a computer system, which carries out the vast majority of the calculations performed by the computer. It can be thought of as the "brain" of a computer or as a manager or boss that tells what the other components of the system should be doing at a given moment.

Certificate A digital file that uniquely identifies its owner. A certificate contains owner identity information and its owner's public key. Certificates are created by certificate authorities.

Certificate authority (CA) An entity in the PKI infrastructure that issues certificates and reports status information and certificate revocation lists.

Certificate Practice Statement (CPS) A detailed explanation of how a certificate authority manages the certificates it issues and associated services such as key management. The CPS acts as a contract between the CA and users, describing obligations and legal limitations and setting the foundation for future audits.

Certificate revocation list (CRL) A certificate authority's list of invalid certificates, such as compromised, revoked, or superseded certificates. The CRL is used during the digital signature verification process to check the validity of a certificate from which a public verification key is extracted.

Certification The technical review of a system or an application.

Challenge-Handshake Authentication Protocol (CHAP) A protocol for securely connecting to a system. CHAP functions as follows: (1) After the authentication request is made, the server sends a challenge message to the requestor. The requestor responds with a value obtained by using a one-way hash. (2) The server checks the response by comparing the received hash to a hash calculated locally by the server. (3) If the values match, the authentication is acknowledged; otherwise, the connection is terminated.

Channel service unit/data service unit (CSU/DSU) A telecommunications device used to terminate telephone company equipment, such as a T1, and prepare data for a router interface at the customer's premises.

Ciphertext The form of data after it has been encrypted; contrast with the form before encryption, called plaintext.

Civil law A type of law that usually pertains to the settlement of disputes between individuals, organizations, or groups and having to do with the establishment, recovery, or redress of private and civil rights. Civil law is not criminal law. It is also called tort law and is mainly for redress or recovery related to wrongdoing.

Clark-Wilson model An integrity-based security model focused on the integrity properties of real-world data; it uses CDIs, UDIs, and TPs.

Client/server Describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfills the request. Clients rely on servers for resources such as files, devices, and processing power.

Clipping level The point at which an alarm threshold or trigger occurs.

Cloning A process that occurs when a hacker copies the electronic serial numbers from one cell phone to another, thereby duplicating the cell phone.

Closed-circuit television (CCTV) A system of television cameras used for video surveillance, in which all components are directly linked via cables or other direct means. Also, a system comprising video transmitters that can feed the live or recorded video to one or more receivers. CCTV is typically used in banks, casinos, shopping centers, airports, and anywhere that physical security can be enhanced by monitoring events. Placement is typically at locations where people enter or leave a facility or at locations where critical transactions occur.

Closed system A system that is not "open" and, therefore, is a proprietary system. Open systems employ modular designs, are widely supported, and facilitate multivendor, multitechnology integration.

Cloud computing The use of a network of remote servers hosted on the Internet, rather than local servers, to store, manage, and process data.

Coaxial cable A cable composed of an insulated central conducting wire wrapped in another cylindrical conductor (the shield). The whole thing is usually wrapped in another insulating layer and an outer protective layer. A coaxial cable has great capacity to carry vast quantities of information. It is typically used in high-speed data and cable TV applications.

COBIT A framework that was designed by ISACA to aid in information security best practices. COBIT is an acronym for Control Objectives for Information and Related Technology.

Cohesion The extent to which a system or subsystem performs a single function.

Cold site A location that contains no computing-related equipment except for environmental support, such as air conditioners and power outlets, and a security system made ready for installing computer equipment.

Collision A problem that occurs when a hashing algorithm, such as MD5, creates the same value for two or more different files.

Combination lock A physical lock that can be opened by turning dials in a predetermined sequence.

Committed information rate (CIR) The data rate guaranteed by a Frame Relay data communications circuit.

Community cloud Cloud infrastructure that is shared between several sources.

Compact disc (CD) An optical disc that can store video, audio, and other data. CDs were originally designed for digital audio.

Compensating control An internal control designed to reduce risk or weakness in an existing control.

Compiler A computer program that translates a computer program written in one computer language (called the source language) into an equivalent program written in another computer language (called the object, output, or target language).

Completely connected (mesh) configuration A type of network configuration in which all devices are connected to all others with many redundant interconnections between network devices.

Computer-aided software engineering (CASE) The use of software tools to assist in the development and maintenance of software. Tools used in this way are known as CASE tools.

Computer incident response team (CIRT) An organization developed to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve the ability of organizations to respond to computer and network security issues.

Concurrency control In computer science, a method used to ensure that database transactions are executed in a safe manner (that is, without data loss). Concurrency control is especially applicable to database management systems, which must ensure that transactions are executed safely and that they follow the ACID rules.

Confidentiality One of the three parts of the security triad, in addition to integrity and availability. Confidentiality is a measure of how well data and systems are protected against access by unauthorized persons.

Confidentiality agreement An agreement that employees, contractors, or third-party users must read and sign prior to being granted access rights and privileges to an organization's IT infrastructure and assets.

Content delivery network (CDN) A high-availability, high-performance network used to serve content to end users from multiple data centers.

Contingency planning The process of preparing to deal with calamities and non-calamitous situations before they occur in order to minimize the effects.

Continuity The state or quality of being continuous or unbroken, without interruption.

Cookie A message from a website given to an individual's web browser on a workstation device. The workstation browser stores this text message in a text file, and the message is sent back to the web server each time the browser goes to that website.

Copyright Legal protection given to authors or creators that protects their expressions on a specific subject against unauthorized copying. It is applied to books, paintings, movies, literary works, and any other medium of use.

Corporate governance The method by which a corporation is directed, administered, or controlled. It includes the laws and customs affecting that direction, as well as the goals for which the organization is governed. How objectives of an organization are set, the means of attaining such objectives, how performance-monitoring guidelines are determined, and ways to emphasize the importance of using resources efficiently are significant issues of corporate governance.

Corrective controls Controls designed to resolve problems soon after they arise.

Coupling The extent of the complexity of interconnections with other modules.

Covert channel An unintended communication path that allows a process to transfer information in such a way that it violates a system's security policy.

Cracker A hacker who acts in an illegal manner. The term is derived from "criminal hacker."

Criminal law A type of law pertaining to crimes against the state or conduct that is detrimental to society. Violations of criminal statutes are punishable by law and can include monetary penalties and jail time.

Critical path methodology (CPM) A methodology that helps in determining what activities are critical and what dependencies exist among the various activities.

Criticality The quality, state, degree, or measurement of the highest importance.

Crossover error rate (CER) A comparison measurement for different biometric devices and technologies that measures their accuracy. The CER is the point at which FAR and FRR are equal or cross over. The lower the CER, the more accurate the biometric system.

Cryptographic key A string of bits used by a cryptographic algorithm during the encryption or decryption process.

Cryptology The science of secure communications.

D

Data analytics The process of reviewing data for the purpose of making conclusions about the information.

Data breach The exposure of sensitive information to unauthorized individuals.

Data communications The transmission or sharing of data between computers via an electronic medium.

Data custodian A data owner who has the responsibility for maintaining and protecting an organization's data.

Data dictionary A catalog of all data held in a database, or a list of items that includes data names and structures.

Data Encryption Standard (DES) A symmetric encryption standard based on a 64-bit block. DES processes 64 bits of plaintext at a time to output 64-bit blocks of ciphertext. DES uses a 56-bit key and has four modes of operation. Because DES has been broken, AES is now the standard.

Data leakage Any type of computer information loss. It can involve removal of information by CD, floppy disk, USB thumb drive, or any other method.

Data owner A person, usually a member of senior management, in an organization who is ultimately responsible for ensuring the protection and use of the organization's data.

Data security The science and study of methods of protecting data in computer and communications systems against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

Data structure A logical relationship among data elements that is designed to support specific data-manipulation functions.

Data warehouse A large collection of data from a variety of sources used to make business decisions and support business intelligence activities.

Database A collection of data that is organized and stored on a computer and can be searched and retrieved by a computer program.

Database administrator (DBA) A person (or group of people) responsible for maintenance activities related to a database, including backup and recovery, performance, and design.

Database management system (DBMS) An integrated set of computer programs that provides the capabilities needed to establish, modify, make available, and maintain the integrity of a database.

Deadman door A linked pair of doors that allows one person to enter the first door and then, after it is closed, allows the person to exit the second door. Deadman doors are used to control access and are also known as a mantrap.

Decentralized computing A type of computing in which activities and computer processing are distributed to different locations.

Decision support system (DSS) A software application that analyzes business data and presents it so that users can make business decisions more easily.

Decryption The process of converting encrypted content into its original form, which is often plaintext. Decryption is the opposite of encryption.

Defense in depth Multilayered security in which the layers may be administrative, technical, or logical.

Demilitarized zone (DMZ) The middle ground between a trusted internal network and an untrusted external network. Services that internal and external users must use, such as HTTP, are typically placed in a DMZ.

Denial of service (DoS) A type of attack that occurs when an attacker consumes the resources on a computer or network for things it was not intended to be doing, thus preventing normal use of the computer or network resources for legitimate purposes.

Destination NAT (DNAT) A type of network translation that alters the destination address in an IP header. DNAT can also change the destination port in the TCP/UDP headers. The purpose of DNAT is to redirect incoming packets with the destination of a public address/port to a private IP address/port inside a network.

Destruction The act of destroying data so that it is denied to legitimate users.

Detective controls Controls that identify and correct undesirable events.

Device lock A physical lock used to secure laptops and other devices from theft.

DevOps The concept of blending development and operations together so that developers, programmers, engineers, and others can work together to build more secure software faster.

Dial back A procedure established for positively identifying a terminal that is dialing in to a computer system. It works by disconnecting the calling terminal and reestablishing the connection by the computer system dialing the telephone number of the calling terminal. Dial back can be used for personal identification.

Dictionary attack A type of cryptographic attack in which the attacker uses a word list or dictionary list to try to crack an encrypted password. A newer technique is to use a time/memory trade-off, such as in rainbow tables.

Digital certificate A certificate, typically issued by a trusted third party, that contains the name of a user or server, a digital signature, a public key, and other elements used in authentication and encryption. An X.509 certificate is the most common type of digital certificate.

Digital signature An electronic signature that can be used to authenticate the identity of the sender of a message. A digital signature is usually created by encrypting the user's private key and is decrypted with the corresponding public key.

Digital watermark A hidden indicator of copyright information added to a document, picture, or sound file.

Direct-sequence spread spectrum (DSSS) A technique used to scramble wireless signals.

Disaster A natural or human-caused event such as fire, flood, or storm that causes equipment failure that negatively affects an industry or a facility.

Disaster tolerance The amount of time that an organization can accept the unavailability of IT facilities and services.

Discretionary access control (DAC) An access policy that allows the resource owner to determine access.

Diskless workstation A thin client that has no hard drive or local operating system. The system boots from a centralized server and stores files on a network file server.

Distributed denial of service (DDoS) An attack that is similar to DoS, except that it is launched from multiple distributed agent IP devices.

DNSSEC A secure version of DNS that provides authentication and integrity.

Domain Name System (DNS) A hierarchy of Internet servers that translate alphanumeric domain names into IP addresses and vice versa. Because domain names are alphanumeric, they are easier to remember than IP addresses.

Downloading The process of transferring information from one computer to another computer and storing it there.

Downtime report A record that tracks the amount of time a computer or other device is not operating because of a hardware or software failure.

Dropper A Trojan horse or program designed to drop a virus into an infected computer and then execute it.

Due care The standard of conduct taken by a reasonable and prudent person. When you see the term *due care*, think of the first letter of each word and remember "do correct" because due care is about performing the ongoing maintenance necessary to ensure the proper level of security.

Due diligence Reasonable examination and research. When you see the term *due diligence*, think of the first letter of each word and remember "do detect."

Dumb terminal A computer workstation or terminal that consists of a keyboard and screen but that has no processor of its own. It sends and receives data to and from a large central computer or server.

Dumpster diving The practice of rummaging through the trash of a potential target or victim to gain useful information.

Dynamic Host Configuration Protocol (DHCP) A protocol that dynamically assigns IP addresses to host devices.

E

Eavesdropping The unauthorized capture and reading of network traffic.

Echo reply The second part of an ICMP ping message, officially a Type 0.

Echo request The first part of an ICMP ping message, officially a Type 8.

eDiscovery The process of searching electronic data for evidence for a civil or criminal case.

Edit control A control that detects errors in the input portion of information. A manual or automated process can be used to check for and allow the correction of data errors before processing.

Editing The process of reviewing for possible errors and making final changes, if necessary, to information in a database.

Electronic Code Book (ECB) A symmetric block cipher that is considered the weakest form of DES. With ECB, the same plaintext input results in the same encrypted text output.

Electronic serial number (ESN) A number that is used to identify a specific cell phone when it is turned on and requests to join a cell network.

Email bomb A hacker technique that involves flooding the email account of a victim with useless emails.

Email/interpersonal messaging Instant messages, usually text, sent from one person to another, or to a group of people, via computer.

Encapsulation of objects A technique used by layered protocols that involves adding header information to the protocol data unit (PDU) from the layer above. Think of data encapsulated in a TCP header followed by an IP header as an example.

Encryption The process of turning plaintext into ciphertext.

Encryption key A sequence of characters used by an encryption algorithm to encrypt plaintext into ciphertext.

Endpoint security A client/server approach to network security that places security controls on end hosts, such as laptops, tablets, and smartphones.

End-user computing The use or development of information systems by the principal users of the systems' outputs or by their staffs.

End-user licensing agreement (EULA) A software license that a software vendor creates to protect and limit its liability and hold the purchaser liable for illegal pirating of the software application. The EULA typically has language in it that protects the software manufacturer from software bugs and flaws and limits the liability of the vendor.

Enterprise architecture A blueprint that defines the business structure and operation of an organization.

Enterprise resource planning (ERP) A software system used for operational planning and administration and for optimizing internal business processes. The best-known supplier of ERP systems is SAP.

Enterprise vulnerability management The overall responsibility and management of vulnerabilities within an organization and how that management of vulnerabilities will be achieved through dissemination of duties throughout the IT organization.

Entity relationship diagram (ERD) A diagram that helps map the requirements of and define the relationship between elements when designing a software program.

Ethernet A network protocol that defines a specific implementation of the physical and data link layers in the OSI model. Ethernet is a local area network standard that provides reliable high-speed communications (a maximum of 100 Mbps) in a limited geographic area (such as an office complex or a university complex).

Ethical hack A term used to describe a type of hack conducted to help a company or an individual identify potential threats to the organization's IT infrastructure or network.

Ethical hacker Ethical hackers must obey rules of engagement, do no harm, and stay within legal boundaries. A security professional who legally attempts to break into a computer system or network to find its vulnerabilities.

Evasion The performance of activities to avoid detection.

Evidence Information gathered by an auditor during the course of an audit that stands as proof to support the conclusions of an audit report.

Exception report A report that uses data selection based on a very specific set of circumstances to identify process exceptions. Reports that identify items with negative quantities of a product are examples of exception reports.

Exclusive-OR (XOR) A logical operation that results in true only if one, but not both, of the operands is true.

Expert system A class of computer programs developed by researchers in artificial intelligence during the 1970s and applied commercially throughout the 1980s. In essence, an expert system is a program made up of a set of rules that analyze information (usually supplied by the user of the system) about a specific class of problems, as well as provide analysis of the problem(s), and, depending on the design, a recommended course of user action to implement corrections.

Exploit A vulnerability in software or hardware that can be used by a hacker to gain access to a system or service.

Exposure factor A value calculated by determining the percentage of loss to a specific asset due to a specific threat.

Extended Binary Coded Decimal Interchange Code (EBCDIC) An IBM-developed 8-bit binary code that can represent 256 characters. It allows control codes and graphics to be represented in a logical format. EBCDIC was created to represent data in particular types of data processing and communications terminal devices.

Extensible Authentication Protocol (EAP) A protocol that supports multiple authentication methods, such as tokens, smart cards, certificates, and one-time passwords.

Extensible Markup Language (XML) A standard for defining, validating, and sharing documents and data distributed on the Web.

Extranet A private network that uses Internet protocols and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses. An extranet can be viewed as part of a company's intranet that is extended to users outside the company. An extranet requires security and privacy.

Extreme Programming (XP) An Agile development method.

F

Failsafe In a logical sense, the process of discovering a system error, terminating the process, and preventing the system from being compromised. The system enters a state in which no access is allowed. In a physical system, an item such as a controlled-access door that unlocks in the event of a power failure so that people can leave the facility and are not locked in.

False acceptance rate (FAR) A biometric system measurement that indicates the percentage of individuals who are incorrectly granted access. This is the worst type of error that can occur because it means that unauthorized individuals have been allowed access.

False rejection rate (FRR) A biometric device error that indicates the percentage of authorized individuals who are incorrectly denied access.

Fast infection A type of virus infection that occurs quickly.

Feasibility study A phase of the SDLC methodology that involves researching the feasibility and adequacy of resources for the development or acquisition of a system solution for a user's need.

Fiber-optic cable A medium for transmission comprising many glass fibers. Light-emitting diodes or lasers send light through the fiber to a detector that converts the light back to an electrical signal for interpretation. Advantages of this medium include huge bandwidth, immunity to electromagnetic interference, and the capability to traverse long distances with minimal signal degradation.

Fibre Channel over Ethernet (FCOE) A SAN technology that encapsulates Fibre Channel traffic over Ethernet packets.

Field In a database, the part of a record reserved for a particular type of data; for example, in a library catalog, author, title, ISBN, and subject headings would all be fields.

File Data stored as a named unit on a data storage medium. Examples include a program, a document, and a database.

File allocation table (FAT) A table or list maintained by an operating system to keep track of the status of various segments of disk space used for file storage.

File infector A type of virus that copies itself into executable programs.

File server A high-capacity disk storage device on a computer that each computer on a network can use to access files. Such computer programs can be set up to accept or not accept requests of different programs running on other computers.

File type The kind of data stored in a file.

Finger On some UNIX systems, a command that identifies who is logged on and active and that may also provide personal information about that individual.

Firewall Hardware or software used to control network connectivity and network services. Firewalls act as chokepoints for traffic entering and leaving a network and prevent unrestricted access. Firewalls can be stateful or stateless.

Firmware A computer program stored permanently in PROM or ROM or semi-permanently in EPROM. Software is "burned in" on the memory device so that it is nonvolatile (that is, so it will not be lost when power is shut off).

First-in/first-out (FIFO) A method of data and information storage in which the data stored for the longest time is retrieved first.

Flooding The process of overloading a network with traffic so that no legitimate traffic or activity can occur.

Fourth-generation language (4GL) A programming language that is easier to use than a lower-level language such as BASIC, assembly language, or Fortran. 4GL languages such as SQL and Python are also known as nonprocedural, natural, or very high-level languages.

Frame Relay A packet-switching technology that transmits data faster than the X.25 standard. Frame Relay does not perform error correction at each computer in a network. Instead, it simply discards any messages that contain errors. It is up to the application software at the source and destination to perform error correction and to control for loss of messages.

Frequency-hopping spread spectrum (FHSS) A basic modulation technique used in spread-spectrum signal transmission. FHSS makes wireless communication harder to intercept and more resistant to interference.

Function Point Analysis (FPA) An ISO-approved method of estimating the complexity of software.

Fuzzing A blackbox testing technique that involves inputting random values and examining the output while looking for failures or exceptions.

G

Gap analysis Analysis of the differences between two different states, often for the purpose of determining how to get from point A to point B. The aim is to look at ways to bridge the gap.

Gateway A device that allows for the translation and management of communication between networks that use different protocols or designs. A gateway can also be deployed in a security context to control sensitive traffic.

Gold standard Practices and procedures that are generally regarded as the best of the best.

Governance The planning, influencing, and conduct of the policy and affairs of an organization.

Graybox testing Testing that occurs with only partial knowledge of the network or is performed to see what internal users have access to.

Guidelines Recommendations, as opposed to hard-and-fast rules. Guidelines are much like standards.

H

Hardware The physical equipment of a computer system, including the central processing unit, data storage devices, terminals, and printers.

Hardware keystroke logger A form of key logger that is a hardware device. When placed in a system, it is hard to detect without a physical inspection. A logger may be plugged in to the keyboard connector or can be built in to the keyboard.

Hash A cryptographic sum that is considered a one-way value. A hash is considerably shorter than the original text and can be used to uniquely identify it. You might have seen a hash value next to applications available for download on the Internet. By comparing the hash of an application with the one on the application vendor's website, you can make sure that the file has not been changed or altered.

Hashing algorithm An algorithm that examines every bit of data while it is being condensed so that even a slight change to the data will result in a large change in the message hash. It is considered a one-way process. MD5 and SHA-1 are examples of hashing algorithms.

Hearsay Evidence based on what a witness heard someone else say, not on what the witness personally observed.

Help desk A support system designed to assist end users with technical and functional questions and problems. A help desk also provides technical support for hardware and software. Help desks are staffed by people who can either solve a problem directly or forward the problem to someone else. Help desk software provides the means to log problems and track them until they are solved. It also gives management information regarding support activities.

Heuristic filter An IDS/IPS and antispam filter technology that uses criteria based on a centralized rule database.

Heuristic scanning A form of virus scanning that looks at irregular activity by programs. For example, a heuristic scanner would flag a word processing program that attempted to format the hard drive, as that is not normal activity for a word processor.

Hierarchical database A database organized in a tree structure, in which each record has one owner. Navigation to individual records takes place through predetermined access paths.

Honeypot An Internet-attached server that acts as a decoy, luring in potential hackers in order to study their activities and monitor how they are able to break into a system.

Hot site A fully prepared and configured off-site location that is fully configured and supplied and ready for use in case of disaster.

Hub A device used for physical connectivity in networks that provides connectivity, amplification, and signal regeneration.

Human-caused threats Threats caused by humans such as hacker attacks, terrorism, or destruction of property.

Hybrid cloud A type of cloud that involves a combination of public and private cloud services. These services may be private on-premises or public cloud services.

Hypertext Markup Language (HTML) A markup language used to create documents and web pages for the World Wide Web.

I

Identity theft An attack in which an individual's personal, confidential, banking, and financial information is stolen and compromised by another individual or individuals.

For example, use of a person's Social Security number without that person's consent or permission could result in identity theft.

Impact The extent of the consequences that would result if a given event occurred.

Impact assessment A study of the potential future effects of a development project on current projects and resources. The resulting document should list the pros and cons of pursuing a specific course of action.

Independence The state or quality of being free from subjection or the influence, control, or guidance of individuals, things, or situations. Auditors and examining officials and their respective organizations must maintain independence and exercise objectivity so that opinions, judgments, conclusions, and recommendations on examined allegations are impartial and are viewed as impartial by disinterested third parties.

Indexed sequential access method (ISAM) A combination or compromise between indexed blocks of data arranged sequentially within each block; used for storing data for fast retrieval.

Inference attack A form of attack that relies on the attacker's ability to make logical connections between seemingly unrelated pieces of information.

Information-processing facility (IPF) Areas where information is processed, usually including a computer room and support areas.

Information technology (IT) The use of technology (computer systems, software, and networks) to solve organizational or business concerns.

Information Technology Security Evaluation Criteria (ITSEC) A European standard that was developed in the 1980s to evaluate confidentiality, integrity, and availability of an entire system.

Infrastructure mode A form of wireless networking in which wireless stations communicate with each other by first going through an access point.

Initial sequence number A number defined during a TCP startup session.

Input controls Computer controls designed to provide reasonable assurance that transactions are properly authorized before being processed by the computer; that transactions are accurately converted to machine-readable form and recorded in the computer; that data files and transactions are not lost, added, duplicated, or improperly changed; and that incorrect transactions are rejected, corrected, and, if necessary, resubmitted in a timely manner.

Insecure computing habits Bad habits that employees, contractors, and third-party users accumulate over time and that can be attributed to an organization's lack of security awareness training, security controls, and security policies or acceptable use policies (AUPs).

Integrated Services Digital Network (ISDN) A system that provides simultaneous voice and high-speed data transmission through a single channel to the user's premises. ISDN is an international standard for end-to-end digital transmission of voice, data, and signaling.

Integrity One of the three items considered part of the security triad, along with confidentiality and availability. Integrity is a measure of the accuracy and completeness of data or systems.

Internet An interconnected system of networks that connects computers around the world via the TCP/IP protocol.

Internet Assigned Numbers Authority (IANA) An organization dedicated to preserving the central coordinating functions of the global Internet for the public good. IANA oversees three key aspects of the Internet: top-level domains (TLDs), IP address allocation, and port number assignments. IANA is used by hackers and security specialists to track down domain owners and their contact details.

Internet Control Message Protocol (ICMP) A protocol that supports diagnostics and error control. A ping is a type of ICMP message.

Internet Engineering Task Force (IETF) A large, open, international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet's architecture and the smooth operation of the Internet. It is open to any interested individual and engineers and develops protocols for the Internet.

Internet of Things (IoT) A network of consumer devices, vehicles, building controls (such as HVAC controls) embedded with electronic sensors and network connectivity so that they have the ability to collect and exchange data.

Internet packet spoofing A technique used to gain unauthorized access to computers or in denial of service attacks. Newer routers and firewall arrangements can offer protection against IP spoofing.

Internet Protocol (IP) One of the key protocols of TCP/IP. IP is found at Layer 3 (network layer) of the OSI model.

Internet Protocol Security (IPsec) An IETF standard used to secure TCP/IP traffic. It can be implemented to provide integrity and confidentiality.

Intrusion detection A key component of security that includes prevention, detection, and response. It is used to detect anomalies or known patterns of attack.

Intrusion detection system (IDS) A network-monitoring device typically installed at an Internet ingress/egress point that is used to inspect inbound and outbound network activity and identify suspicious patterns that might indicate network or system attack from someone attempting to break in to or compromise a system.

Irregularities Intentional violations of established management policy, deliberate misstatements, or omissions of information concerning an area under audit or an organization as a whole.

ISO 17799 A comprehensive security standard that is divided into ten sections. It is considered a leading standard and a code of practice for information security management.

IT asset An asset such as hardware, software, or data.

IT asset valuation The act of putting a monetary value to an IT asset.

IT infrastructure A general term that encompasses all information technology assets (hardware, software, and data), components, systems, applications, and resources.

IT security architecture and framework A document that defines an organization's policies, standards, procedures, and guidelines for information security.

J–K

Just a bunch of disks (JBOD) A technique that is somewhat like RAID in that two or more hard drives are combined into one storage array. However, JBOD offers none of the fault tolerance advantages of RAID.

Key exchange protocol A protocol used to exchange secret keys for the facilitation of encrypted communication. Diffie-Hellman is an example of a key exchange protocol.

Kilo lines of code (KLOC) A software metric used to determine the cost of software development based solely on the length of code.

L

Last-in/first-out (LIFO) A data-processing method that applies to buffers. The last item in the buffer is the first to be removed.

Latency The delay a packet incurs in traveling from one node to another.

Lattice-based access control (LBAC) A security model that deals with confidentiality and integrity and places upper and lower bounds on subjects and objects.

Librarian An individual in an organization who is responsible for storing, safeguarding, and maintaining data, programs, and computer information.

Limit check A test of specified amount fields against stipulated high or low limits of acceptability. When both high and low values are used, the test can be called a range check.

Local area network (LAN) A group of wired or wireless computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building).

Log A system that automatically records significant events. The files that contain these records are called log files or simply logs; what is written on a log is a record.

Log on The process of identifying oneself to a computer or an online service to gain access to a system as a legitimate user. The usual requirements are a valid username (or user ID) and password.

Logic bomb A dangerous type of malware that waits for a predetermined event or amount of time to execute its payload. Typically used by disgruntled employees for insider attacks.

Lumen The amount of light one standard candle makes.

M

MAC filtering A method of controlling access on a wired or wireless network by denying access to any device whose MAC address does not match an address from a pre-approved list.

Macro infector A type of computer virus that infects macro files. I Love You and Melissa are examples of macro viruses.

Man-in-the-middle attack A type of attack in which the attacker can read, insert, and change information being passed between two parties without either party knowing that the information has been compromised.

Mandatory access control (MAC) A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (such as clearance) of subjects to access information of such sensitivity.

Mantrap See Deadman door.

Massive array of inactive disks (MAID) A large array of hard drives that are kept inactive until needed.

Master boot record infector A virus that infects a master boot record.

Materiality An expression of the relative significance or importance of a particular matter in the context of an organization as a whole.

MD5 A hashing algorithm that produces a 128-bit output.

Media Access Control (MAC) The hard-coded address of a physical layer device that is attached to a network. Every network interface controller must have a hard-coded and unique MAC address. The MAC address is 48 bits long.

Message switching A strategy that enables communication channels to be used simultaneously by more than one node. At each transfer point in the connection, incoming data is stored in its entirety and then forwarded to the next point. This process continues until the data reaches its destination.

Methodology A set of documented procedures used for performing activities in a consistent, accountable, and repeatable manner.

Microsegmentation The practice of splitting up a network into many isolated segments. This activity is used with software-defined networks to integrate access control lists and increased security.

Middleware Software that "glues together" two or more types of software (for example, two applications, their operating systems, and the network on which everything works) by translating information between them and exchanging this information over a network. The interacting applications are not aware of the middleware.

Minimum acceptable level of risk The stake that an organization defines for the seven areas of information security responsibility. Depending on the goals and objectives for maintaining confidentiality, integrity, and availability of the IT infrastructure and its assets, the minimum acceptable level of risk will dictate the amount of information security.

Mobile site A portable data-processing facility transported by trailers to be quickly moved to a business location. Typically used by insurance companies and the military, these information-processing facilities can contain servers, desktop computers, communications equipment, and even microwave and satellite data links.

Modem A device used to connect a computer to an analog phone line. Modems use the process of modulation.

Modulation A process used by modems to convert a digital computer signal into an analog telecommunications signal.

Moore's law The belief that processing power of computers will double about every 18 months due to technological improvements.

Multicast The process of sending a computer packet to a group of recipients.

Multipartite virus A virus that attempts to attack both the boot sector and executable files.

N

Natural threats Threats posed by nature; for example, fire, floods, and storms.

Network Address Translation (NAT) A method of connecting multiple computers to the Internet using one IP address so that many private addresses are converted to a single public address.

Network administrator An individual responsible for the installation, management, and control of a network. When problems with the network arise, this is the person to call.

Network operations center (NOC) An organization's help desk or interface to its end users where trouble calls, questions, and trouble tickets are generated.

NIST 800-42 A document that provides guidance on network security testing. It deals mainly with techniques and tools used to secure systems connected to the Internet.

Noise Any unwanted signal, such as static, that interferes with the clarity of data being transmitted, thus creating the possibility that the receiver will receive a misconstrued message.

Non-attribution The act of not providing a reference to a source of information.

Non-repudiation A system or method put in place to ensure that an individual or a system cannot deny his/her/its own actions.

O

Off-site storage A storage facility that is not located at an organization's primary facility. The idea behind off-site storage is to protect information and prevent damage that might occur at the primary facility. Off-site storage facilities are used to store computer media, backup data, and files.

On premises At the organization's physical site. For example, computers or a data center may be run on premises rather than running at a remote data center or in the cloud.

One-time pad An encryption mechanism that can be used only once and that is, theoretically, unbreakable. One-time pads function by combining plaintext with a random pad (secret key) that is the same length as the plaintext.

Open Shortest Path First (OSPF) A routing protocol that determines the best path for routing IP traffic over a TCP/IP network. It uses less router-to-router update traffic than RIP, which it was designed to replace.

Open source Software that is released under an open-source license or to the public domain. The source code can be seen and can be modified.

Open Web Application Security Project (OWASP) A nonprofit organization that is focused on improving application security.

Operating system (OS) identification The practice of identifying the operating system of a networked device using either passive or active techniques.

Operational control A control that is used for normal daily operation of the organization. Operational controls ensure that normal operational objectives are achieved.

Outsourcing A contract arrangement between a third party and an organization for services such as web hosting, application development, or data processing.

P

Packet or packet data unit (PDU) A block of data sent over a network that transmits the identities of the sending and receiving stations for error control.

Packet filter A form of stateless inspection performed by some firewalls and routers.

Packet switching A data transmission method that divides messages into standard-sized packets for greater efficiency in routing and transport through a network.

Paper shredder A hardware device used for destroying paper and documents by shredding to prevent Dumpster diving.

Paper test A type of disaster-recovery test that reviews the steps of the test without actually performing the steps. This type of disaster-recovery test is normally used to help team members review the proposed plan and become familiar with the test and its objectives.

Parallel testing A testing mode in which a stream of data is fed into two systems to allow processing by both so that the results can be compared.

Passive (OS) fingerprint A passive method of identifying the OS of a targeted computer or device. No traffic or packets are injected into the network; attackers simply listen to and analyze existing traffic.

Password Authentication Protocol (PAP) An insecure, obsolete protocol for authentication in which cleartext usernames and passwords are used without encryption.

Patent Exclusive rights granted by the federal government to an inventor to exclude others from making, using, or selling that person's invention.

Pattern matching A method used by IDSs to identify malicious traffic. It is also called signature matching and works by matching traffic against signatures stored in a database.

Penetration test A method of evaluating the security of a network or computer system by simulating an attack by a malicious hacker but without doing harm and with the owner's consent.

Personal area network (PAN) A connection that can be made with Bluetooth between various devices.

Phishing The act of misleading or tricking an individual into providing personal and confidential information to an attacker masquerading as a legitimate individual or business.

Phreaker An individual who hacks phone systems or phone-related equipment. Phreakers predate computer hackers.

Piggybacking A method of gaining unauthorized access into a facility by following an authorized employee through a controlled access point or door.

Ping sweep The process of sending ping requests to a series of devices or to the entire range of networked devices.

Policy A high-level document that dictates management intentions toward security.

Polyinstantiation A strategy that involves preventing inference attacks by allowing different versions of information to exist at different classification levels. For example, a Navy officer without classified access might want information about a ship and discover that it has left port and is bound for Europe. A Navy officer with classified access might access the same database and discover that the ship has left port but is really bound for Asia.

Polymorphic virus A virus that is capable of change and mutation.

Port An interface used by protocols and applications to assign addresses to services. For example, port 21 is used for FTP, and port 80 is used for HTTP. Port numbers are divided into three ranges: well-known ports, registered ports, and dynamic and/or private ports. Well-known ports are those from 0 through 1023. Registered ports are those from 1024 through 49151, and dynamic and/or private ports are those from 49152 through 65535.

Post Office Protocol (POP) A commonly implemented method of delivering email from an email server to a client machine. Other methods include IMAP and Microsoft Exchange.

Prepender A virus type that adds virus code to the beginning of existing executables.

Pretexting Collecting information about a person under false pretenses.

Preventive controls Controls that reduce risk and are used to prevent undesirable events from happening.

Principle of deny all The idea of securing logical or physical assets by first denying all access and then allowing access only on a case-by-case basis.

Privacy impact analysis A review of the information held by a corporation and assessment of the damage that would result if sensitive or personal information were lost, stolen, or divulged.

Private cloud A category of cloud service that is private to a specific organization and is used only by that organization.

Probability The likelihood of an event happening.

Procedure A detailed, in-depth, step-by-step document that lays out exactly what is to be done and how it is to be accomplished.

Program Evaluation and Review Technique (PERT) A planning and control tool that represents, in diagram form, a network of tasks required to complete a project, establishing sequential dependencies and relationships among the tasks.

Protocol A set of formalized rules that describe how data is transmitted over a network. Low-level protocols define electrical and physical standards, whereas high-level protocols deal with formatting of data. TCP and IP are examples of high-level LAN protocols.

Prototyping The process of quickly putting together a working model (a prototype) to test various aspects of a design, illustrate ideas or features, and gather early user feedback. Prototyping is often treated as an integral part of the development process, where it is believed to reduce project risk and cost.

Proxy server A firewall that is used to improve performance security. A proxy server intercepts all requests to a real server to see whether it can fulfill the requests itself. It forwards to the real server any requests that it can't fulfill.

Public cloud service A cloud-based service that is available to everyone. Dropbox is an example of a public cloud service.

Public key encryption An encryption scheme that uses two keys. In an email transaction, for example, the public key encrypts the data, and a corresponding private key decrypts the data. Because the private key is never transmitted or publicized, the encryption scheme is extremely secure. For digital signatures, the process is reversed: The sender uses the private key to create the digital signature, and anyone who has access to the corresponding public key can read it.

Public key infrastructure (PKI) Infrastructure used to facilitate e-commerce and build trust. PKI consists of hardware, software, people, policies, and procedures; it is used to create, manage, store, distribute, and revoke public key certificates. PKI is based on public key cryptography.

Q

Qualitative analysis A weighted factor or nonmonetary evaluation and analysis based on a weighting or criticality factor valuation.

Qualitative assessment An analysis of risk that places the probability results into terms such as none, low, medium, and high.

Qualitative risk assessment A scenario-based assessment in which one scenario is examined and assessed for each critical or major threat to an IT asset.

Quantitative analysis A numeric evaluation and analysis based on monetary valuation.

Quantitative risk assessment A methodical, step-by-step calculation of asset valuation, exposure to threats, and the financial impact or loss that would occur if threats were realized.

Queue A group of items, such as computer jobs or messages, waiting for service.

R

Radio frequency identification (RFID) A set of components that include a reader and a small device referred to as a tag. The tag can be used to hold information for inventory, management, tracking, or other purposes. RFID provides a method to transmit and receive data over a short range from one point to another.

Record A collection of data items or fields treated as one unit.

Recovery point objective (RPO) The point in time to which data must be restored to resume processing transactions. RPO is the basis on which a data protection strategy is developed.

Recovery testing Testing aimed at verifying a system's capability to recover from varying degrees of failure.

Recovery time objective (RTO) During the execution of disaster recovery or business continuity plans, the time goal for the reestablishment and recovery of a business function or resource.

Red team A group of ethical hackers who help organizations to explore network and system vulnerabilities by means of penetration testing.

Redundant array of independent disks (RAID) A type of fault tolerance and performance improvement for disk drives that employs two or more drives in combination.

Registration authority (RA) An entity responsible for the identification and authentication of a PKI certificate. The RA is not responsible for signing or issuing certificates. The most common form of certificate is the X.509 standard.

Remote Authentication Dial-In User Service (RADIUS) A client/server protocol and software that allows remote-access servers to communicate. Used in wireless systems such as 802.1x.

Repeater A network device used to regenerate or replicate a signal. Repeaters are used in transmission systems to regenerate analog or digital signals distorted by transmission loss.

Repository A central place where data is stored and maintained. A repository can be a place where multiple databases or files are located for distribution over a network, or it can be a location that is directly accessible to users.

Required vacations A security control used to uncover misuse or illegal activity by requiring employees to use their vacation time.

Reverse engineering The process of taking apart a device or a software program and analyzing its workings in detail, usually to construct a new device or program that does the same thing without actually copying anything from the original.

Rijndael A symmetric encryption algorithm chosen for Advanced Encryption Standard (AES).

Ring topology A topology used by token ring and FDDI networks in which all devices are connected in a ring. Data packets in a ring topology are sent in a deterministic fashion from sender and receiver to the next device in the ring.

Risk The subjective measure of the potential for harm that can result from the action of a person or thing.

Risk acceptance An informed decision to suffer the consequences of likely events.

Risk assessment A process for evaluating the exposure or potential loss or damage to the IT and data assets of an organization.

Risk avoidance A decision to take action to avoid a risk.

Risk management The overall responsibility and management of risk within an organization. Risk management involves dissemination of roles, responsibilities, and accountabilities for risk in an organization.

Risk transference The process of shifting the responsibility for or burden of risk to another party or individual.

Rogue access point An 802.11 access point that has been set up by an attacker for the purpose of diverting legitimate users so that their traffic can be sniffed or manipulated.

Role-based access control (RBAC) A type of discretionary access control in which users are placed into groups to facilitate management. This type of access control is widely used by banks and casinos.

Rotation of assignment A security mechanism that involves moving employees from one job to another so that one person does not stay in one position forever. This makes it harder for an employee to hide malicious activity.

Rounding down A method of computer fraud that involves rounding down dollar amounts so that small amounts of money are stolen. For example, the value $1,199.50 might be rounded down to $1,199.00, and the extra 50 cents would be kept by the perpetrator.

Router A device that determines the next network point to which a data packet should be forwarded en route to its destination. The router is connected to at least two networks and determines which way to send each data packet, based on its current understanding of the state of the networks it is connected to. A router creates or maintains a table of the available routes and uses this information to determine the best route for a given data packet. Routing occurs at Layer 3 (the network layer) of the seven-layer OSI model.

Routing Information Protocol (RIP) A widely used distance-vector protocol that determines the best route based on hop count.

Rule-based access control A type of mandatory access control that matches objects to subjects. It dynamically assigns roles to subjects based on their attributes and a set of rules defined by a security policy.

S

Scope creep Uncontrolled change in a project's scope, which causes an assessment to drift away from its original scope and result in budget and schedule overruns.

Screen scraper A type of malware designed to capture data displayed to the screen.

Script kiddie The least skilled level of criminal hacker, who looks for easy targets or well-worn vulnerabilities.

Secure Sockets Layer (SSL) A cryptographic protocol developed by Netscape for transmitting private documents via the Internet. It works by using a private key to encrypt data that is transferred over the SSL connection. Very similar to Transport Layer Security (TLS).

Security Assertion Markup Language (SAML) An XML open standard data format for exchanging authentication and authorization data.

Security breach or security incident The result of a threat or vulnerability being exploited by an attacker.

Security bulletin A memorandum or message from a software vendor or manufacturer documenting a known security defect in software or an application. Security bulletins are typically accompanied by instructions for loading a software patch to mitigate the security defect or software vulnerability.

Security by obscurity The controversial use of secrecy to ensure security.

Security controls Policies, standards, procedures, and guideline definitions for various security control areas or topics.

Security countermeasure A security hardware or software technology solution that is deployed to ensure the confidentiality, integrity, and availability of IT assets that need protection.

Security kernel A combination of software, hardware, and firmware that makes up the trusted computing base (TCB), which mediates all access, must be verifiable as correct, and is protected from modification.

Security testing Techniques used to confirm the design and/or operational effectiveness of security controls implemented within a system. Examples include attack and penetration studies to determine whether adequate controls have been implemented to prevent breach-of-system controls and processes, and password strength testing using tools like password crackers.

Separation of duties Unique definition of the roles, tasks, responsibilities, and accountabilities for information security for the different duties of the IT staff and IT security staff.

Service-level agreement (SLA) A contractual agreement between an organization and its service provider that holds the service provider accountable for the requirements defined in the agreement.

Service set ID (SSID) A sequence of up to 32 letters or numbers that is the ID, or name, of a wireless local area network; it is used to differentiate networks.

SHA-1 A hashing algorithm that produces a 160-bit output.

Shoulder surfing The act of looking over someone's shoulder to steal the user's system credentials.

Signature scanning One of the most basic ways of scanning for computer viruses, which works by comparing suspect files and programs to fingerprints or descriptors of known viruses stored in a database.

Simple Network Management Protocol (SNMP) An application layer protocol that facilitates the exchange of management information between network devices. Version 1 uses well-known community strings or passwords of public and private.

Single loss expectancy (SLE) A monetary figure that represents an organization's cost for a single loss of a given IT asset.

Site survey The process of determining the optimum placement of wireless access points. The objective of a site survey is to create an accurate wireless system design/layout and budgetary quote.

Smurf attack A DDoS attack in which an attacker transmits large amounts of ICMP echo request (ping) packets to a targeted IP destination device using the targeted destination's IP source address. This is called spoofing the IP source address. IP routers and other IP devices that respond to broadcasts respond back to the targeted IP device with ICMP echo replies, thus multiplying the amount of bogus traffic.

Sniffer A hardware or software device that can be used to intercept and decode network traffic.

Social engineering The practice of tricking employees into revealing sensitive data about their computer system or infrastructure. This type of attack targets people and involves human manipulation. Even when systems are physically well protected, social engineering attacks are possible.

Software bug or software flaw An error in software coding or its design that can result in software vulnerability.

Software-defined networks An approach to networking that uses application programming interfaces (APIs) to converse with underlying hardware infrastructure to enable improved network performance and monitoring, making it more like cloud computing than traditional network management.

Software development lifecycle (SDLC) A method for developing software that has five main stages: analysis, design, development, implementation, and evaluation. Each stage has several components; for example, the development stage includes programming (coding, including internal documentation, debugging, testing, and documenting) and acquiring equipment (selection, acquisition [purchase or lease], and testing).

Software vulnerability standard A standard that accompanies an organization's vulnerability assessment and management policy. This standard typically defines the organization's vulnerability window and how the organization is to provide software vulnerability management and software patch management throughout the enterprise.

Source code A non-executable program written in a high-level language. A compiler or an assembler must translate the source code into an object code (machine language) that the computer can understand.

Spam Unsolicited electronic communication sent in bulk.

Spoofing Masking one's identity and pretending to be someone or something else. Common spoofing methods include ARP, DNS, and IP. Spoofing is also implemented by email in phishing schemes.

Spyware A software application that covertly gathers information about a user's Internet usage and activity and exploits this information by sending adware and pop-up ads based on the user's Internet usage history.

Stateful inspection An advanced firewall architecture that works at the network layer and can keep track of packet activity. Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection tracks each connection traversing all interfaces of the firewall and makes sure they are valid. One example is a DNS reply that has just been received in response to a DNS request.

Statistical sampling The selection of sample units from a population and the measurement and/or recording of information about these units to obtain estimates of population characteristics.

Steganography A cryptographic method of hiding the existence of a message. A commonly used method places information in pictures.

Storage area network (SAN) A high-speed subnetwork that interconnects different data-storage devices with associated data servers for a large network. SANs support disk mirroring, backup and restore, archival and retrieval of archived data, data migration from one storage device to another, and the sharing of data among different servers in a network.

Stream cipher A symmetric key cipher that encrypts data, typically one byte at a time.

Structured Query Language (SQL) A standardized relational database language for querying, manipulating, and updating information in a relational database.

Supervisory Control and Data Acquisition (SCADA) A control system architecture that is typically used for remotely monitoring and controlling industrial processes.

Supply chain management (SCM) Intercompany planning control and monitoring of central functions such as procurement, production, and sales to increase their efficiency.

Switch A device that links several separate LANs and provides packet filtering among them. A LAN switch is a device with multiple ports, each of which can support an entire Ethernet or token ring LAN. A switch operates at Layer 2 of the OSI model.

Symmetric algorithm An encryption algorithm that relies on a single key for encryption and decryption.

Symmetric encryption An encryption standard in which every party must have a copy of a shared key. A single key is used for both encryption and decryption.

SYN flood attack A DDoS attack in which the attacker sends a succession of SYN packets with a spoof address to a targeted destination IP device but does not send the last ACK packet to acknowledge and confirm receipt. This leaves half-open connections between the client and the server until all resources are absorbed, rendering the server or targeted IP destination device unavailable due to resource allocation.

Synchronized sequence number A number that is initially passed to the other party at the start of the three-step startup and is used to track the movement of data between parties. Every byte of data sent over a TCP connection has a sequence number.

Synchronous transmission A method of communication in which data is sent in blocks, without the need for start and stop bits between bytes. Synchronization is achieved by sending a clock signal along with the data and by sending special bit patterns to denote the start of each block.

System software Software that controls the operations of a computer system. It is a group of programs instead of one program. The operating system controls the hardware in the computer and peripherals, manages memory and files and multitasking functions, and is an interface between applications and the computer.

System testing The process of bringing together all the programs that a system comprises for testing purposes. Programs are typically integrated in a top-down, incremental fashion.

T

Target of engagement (TOE) The assessment or pen test target.

TCP handshake A three-step process computers go through when negotiating a connection with each other. The process is a target of attackers and others with malicious intent.

Telecommunications Systems that transport information over a distance, sending and receiving audio, video, and data signals by electronic means.

TEMPEST A method of shielding equipment to prevent the capture and use of stray electronic signals and later reconstruction of the signals into useful intelligence.

Terminal Access Controller Access Control System (TACACS) A UDP-based access control protocol that provides authentication, authorization, and accountability.

Test data Data that is run through a computer program to test the software. Test data can be used to test compliance with controls in the software.

Threat Any agent, condition, or circumstance that could potentially cause harm, loss, damage, or compromise to an IT asset or data asset.

Throughput The amount of data transferred from one place to another or processed in a specified amount of time. Data transfer rates for disk drives and networks are measured in terms of throughput. Typically, throughput is measured in kilobits per second, megabits per second, and gigabits per second.

Time-to-live (TTL) A counter used in an IP packet that specifies the maximum number of hops that a packet can traverse. When a TTL is decremented to zero, a packet expires.

Total cost of ownership (TCO) The value of the asset plus the cost of operation and the cost of all safeguards and controls.

traceroute A tool for tracing hops or computers between the source and the target computer that shows the path the packets are taking.

Trademark Legal protection for a logo, name, or characteristic that can be identified as exclusive.

Trans-border data flow The flow of data in the course of its storage or use.

Transmission Control Protocol (TCP) One of the main protocols of the Internet. It is used for reliability and guaranteed delivery of data.

Transmission Control Protocol/Internet Protocol (TCP/IP) A collection of protocols used to provide the basis for Internet and World Wide Web services.

Trapdoor function A one-way function that is the mechanism by which asymmetric encryption algorithms function.

Trojan A program that does something undocumented that the programmer or designer intended but that the end user would not approve of if he or she knew about it.

Trusted Computer System Evaluation Criteria (TCSEC) A publication of the U.S. Department of Defense, also called the Orange Book, that is designed to evaluate standalone systems. It places systems into one of four levels—A, B, C, or D—and its basis of measurement is confidentiality.

Trusted computing base (TCB) All the protection mechanisms within a computer system, including the hardware, firmware, and software responsible for enforcing a security policy.

Trusted Network Interpretation (TNI) Also known as the Red Book, a document that is part of the Rainbow Series.

Trusted Platform Module (TPM) An international standard for a secure hardware device that has integrated cryptographic keys installed. TPM uses a dedicated microprocessor.

Tumbling The process of rolling through various electronic serial numbers on a cell phone to attempt to find a valid set to use.

Tunneling A technology that enables one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network. For example, Microsoft's PPTP technology enables organizations to use the Internet to transmit data across a VPN. It does this by embedding its own network protocol within the TCP/IP packets carried by the Internet. Tunneling is also called encapsulation. Tunneling can also be used covertly, as with STUNNEL and other programs.

Turnstile A one-way gate or access control mechanism used to limit traffic and control the flow of people.

U

Uniform resource locator (URL) The global address of a web page.

Uninterruptible power supply (UPS) A device designed to provide a backup power supply during a power failure. Basically, a UPS is a battery backup system with an ultra-fast sensing device.

Universal Serial Bus (USB) A specification standard for connecting peripherals to a computer. It can connect up to 127 devices to a computer and transfers data at a slower rate, up to a maximum of 12 Mbps.

User Datagram Protocol (UDP) A connectionless protocol that provides very few error recovery services but offers a quick and direct way to send and receive datagrams.

Utility programs Standard sets of routines that assist in the operation of a computer system by performing some frequently required process, such as copying, sorting, or merging.

V

Vandalism The willful destruction of property.

Verification The process of confirming that data is correct and accurate before it is processed or entered.

Virtual local area network (VLAN) Technology typically built into a switch that allows the broadcast domain to be restricted to a specific number of switch ports. VLANs allow the segmentation of traffic that is typically done at OSI Layer 3 to be performed at OSI Layer 2.

Virtual machine (VM) An emulation of a physical machine in a virtual workspace.

Virtual private network (VPN) A private network that uses a public network to connect remote sites and users.

Virtual storage area network (VSAN) A collection of ports from a set of connected Fibre Channel switches that form a virtual fabric. These ports can be partitioned into multiple VSANs.

Virus A computer program that can generate copies of itself and thereby spread. Viruses usually require the interaction of an individual and can have rather benign results, such as flashing a message to the screen, or malicious results that destroy data, systems, integrity, or availability.

Virus hoax A chain letter designed to trick someone into forwarding it to many other people, warning of a virus that does not exist. The Good Times virus is an example.

Voice over IP (VoIP) A technology that converts voice or fax calls into data packets for transmission over the Internet or other IP-based networks.

Vulnerability The absence or weakness of a safeguard in an asset.

Vulnerability assessment A methodical evaluation of an organization's IT weaknesses in infrastructure components and assets and how those weaknesses can be mitigated by using proper security controls and recommendations.

Vulnerability management The overall responsibility for and management of vulnerabilities within an organization through dissemination of duties throughout the IT organization.

W–X–Y–Z

War chalking The process of marking on a wall or sidewalk near a building to indicate the presence of wireless access.

War dialing The process of using a software program to automatically call thousands of telephone numbers to look for any that have a modem attached.

War driving The process of driving around a neighborhood or an area, looking for wireless access points.

Warm site An alternate computer facility that is partially configured and can be made ready in a few days.

Whitebox testing A security assessment or penetration test in which all aspects of the network are known.

Wide area network (WAN) A network that spans the distance between buildings, cities, and even countries. WANs are LANs that are connected using wide area network services from telecommunications carriers.

Wi-Fi Protected Access (WPA) A security standard for wireless networks that is designed to be more secure than WEP. Developed from the draft 802.11i standard.

Wired Equivalent Privacy (WEP) A security standard based on the RC4 encryption scheme that was designed to provide the same level of security as a wired LAN. Because of 40-bit encryption and problems with the initialization vector, it was found to be insecure.

Work breakdown structure (WBS) A breakdown of a process that shows what activities need to be completed in a hierarchical manner.

Worm A self-replicating program that spreads by inserting copies of itself into other executable codes, programs, or documents. Worms typically flood a network with traffic and result in denial of service.

Wrapper A type of program used to bind a Trojan program to a legitimate program. The objective is to trick the user into running the wrapped program and installing the Trojan.

Written authorization Permission to perform penetration tests for a client. This authorization is important in ethical hacking.

Zero-day exploit An exploit for a vulnerability for which there is not yet a vendor patch.

Zone transfer A mechanism DNS servers use to update each other by transferring resource records. The transfer contains IP addresses that are mapped to the corresponding domain name. Zone transfer should be a controlled process between two DNS servers to prevent hackers from stealing an organization's DNS information.

Index

This page intentionally left blank

Pearson

Where are the companion content files?

Register this digital version of CISSP® Exam Cram, Fifth Edition to access important downloads.

Register this eBook to unlock the companion files. Follow these steps:

1. Go to **pearsonITcertification.com/account** and log in or create a new account.
2. Enter the ISBN: **9780137419555** (NOTE: Please enter the print book ISBN provided to register the eBook you purchased.)
3. Answer the challenge question as proof of purchase.
4. Click on the "Access Bonus Content" link in the Registered Products section of your account page, to be taken to
the page where your downloadable content is available.

This eBook version of the print title does not contain the practice test software that accompanies the print book.

You May Also Like—Premium Edition eBook and Practice Test. To learn about the Premium Edition eBook and Practice Test series, visit **pearsonITcertification.com/practicetest**

The Professional and Personal Technology Brands of Pearson

Addison Wesley   Cisco Press   informIT   PEARSON IT Certification   que®   SAMS