SECURITY STANDARDS—GOVERNMENT AND COMMERCIAL

L. Kirk Barker and Larry D. Nelson

L. Kirk Barker *is a member of technical staff and* ***Larry D. Nelson*** *is a supervisor in the Government Communications Systems Department of AT&T Bell Laboratories in Holmdel, New Jersey. Mr. Barker joined the company in 1986 and is working on computer and network security for government and commercial applications. He has a B.S. in computer science from Texas A&M University and an M.S. in computer science from the University of Illinois—Champaign/Urbana. Mr. Barker is secretary of the American National Standards Committee X9E9 (Wholesale Financial Security) and is rapporteur of the Institute of Electrical and Electronics Engineers Committee 802.10 (802 LAN Security). Mr. Nelson joined AT&T in 1965 and is responsible for systems engineering support and standards and strategy* (continued on page 18)

Computer security standards are needed to reduce the cost of security products and to allow for interoperability and evaluation. Several national and international groups are trying to standardize approaches to information security for certain applications. This paper describes and compares three types of standards activities: United States government standards, financial standards, and standards developed for the International Standards Organization Open Systems Interconnection Basic Reference Model.

Introduction

Information security protects against the unauthorized disclosure or modification of data stored in or transmitted by an automated processor, but it does not address the inadvertent acts of authorized users (e.g., user mistakes). (See Table I for a list of security definitions.) Discussions of physical and procedural security are beyond the scope of this paper.

Security standards provide a common measure for evaluation so that users do not have to perform independent security assessments. In the future, the security of products may be tested by the government. In such a situation, users could assume security was appropriate if their work conformed to a government standard. Security testing of this sort might be comparable to safety testing currently performed on food, drugs, and other products.[1]

Standards also allow for compatibility among vendors' products. Compatibility serves as a convenience to customers and increases competition, which eventually lowers the cost of products. Unless security is inexpensive and convenient, it will be used only for very sensitive applications, and many applications will remain unprotected.

Standards for information security are not easy to establish, even within the limited areas described in this paper. User requirements are diverse; in fact, one user's requirements may conflict with another's.

This article surveys some of the major security standards activities. Security requirements are included in many different standards, so this article does not attempt to provide an exhaustive list of all

Table I. Security Definitions

Term	Definition	Caveats	Example
Disclosure	Allowing some entity to derive the meaning of data.		Passive wire-tap
Modification	Alteration of data.	It is not necessary to read data to alter it. Protection against modification, beyond detection, is usually not possible because it is rarely possible to keep someone from cutting the transmission medium, or inserting enough noise to alter data.	Active wire-tap
Message integrity	Prevention against unauthorized modification of a message.		Sequencing or message authentication codes.
Confidentiality	Prevention of information disclosure to unauthorized parties.		Encryption
Multilevel security	Allows data with different sensitivity levels to exist simultaneously on the same computer and allows access by users with different security clearances.	Applicability to commercial market questionable.	UNIX® System V/MLS*
Mandatory access control	Restricts users and data flow based on the clearance of the user and sensitivity level of the data.		See Bell and LaPadula†
Discretionary access control	Allows users to give access to other users independent of the receiving user's attributes.		Access control lists

*See paper by Flink and Weiss, pp. 53-64 in this issue of the *AT&T Technical Journal.*
†D. E. Bell and L. J. LaPadula, *Secure Computer Systems: Unified Exposition and Multics Interpretation*, MTR-2997, Revision 1, MITRE Corporation, Bedford, Massachusetts, March 1976.

Panel 1. Acronyms in This Paper

ANSI	American National Standards Institute
CCITT	International Telegraph and Telephone Consultative Committee
COMSEC	communication security
DES	Data Encryption Standard
DoD	U.S. Department of Defense
ECMA	European Computer Manufacturers Association
FIPS	Federal Information Processing Standards
GOSIP	Government OSI Profile
GSA	General Services Administration
ISO	International Standards Organization
KMC	key management center
NBS	National Bureau of Standards
NCSC	National Computer Security Center
NSA	National Security Agency
OSI	open systems interconnection
PIN	personal identification number
SDNS	Secure Data Network System
TC	Technical Committee

standards activities involving security.

The United States government has either performed or funded much of the security research in the U.S. This research is described in the first section of this paper. As the demand for security reached the private sector, there was a need for other security standards. The American National Standards Institute (ANSI), the International Standards Organization (ISO), and the International Telegraph and Telephone Consultative Committee (CCITT) have initiated several security-related projects. (See Panel 1 for a list of acronyms used in this paper.) We also describe the security-related activities for the financial community, the first large commercial security market.

Another effort to develop security standards stemmed from work on ISO's Open Systems Interconnection (OSI) Basic Reference Model.[2] A set of security services and mechanisms conforming to this reference model has been defined and is described in the third section of this paper. Finally, we compare and contrast the different standards efforts.

U.S. Government

The government has at least three organizations that sponsor security standards. The U.S. Department of Defense (DoD) publishes DoD standards, the Department of Commerce produces Federal Information Processing Standards (FIPS), and finally, the General Services Administration produces federal standards. A description of the standards process for each organization will be briefly described, and some standards from each of the organizations introduced.

Department of Defense Standards. The DoD sponsors both DoD standards and military standards. The Department's National Computer Security Center (NCSC) has produced many publications, some of which have become standards. Projects such as the Secure Data Network System and Government Open Systems Interconnect Profile are expected to produce standards in the next few years.

National Computer Security Center. In 1978, the National Bureau of Standards (NBS) held a workshop to discuss the auditing and evaluation of computer security. Following this lead, the Office of the Secretary of Defense assigned certain computer security responsibilities to the National Security Agency (NSA). In June 1981, the DoD Computer Security Center began operation. The success of the Center and the need to transfer security information to the commercial sector resulted in the expansion of the DoD Computer Security Center to the National Computer Security Center.

One of NCSC's missions is "to develop and promulgate uniform computer security criteria and standards."[3] The NCSC distributes the following publications dealing with information security:

- *Orange Book*—A DoD standard for evaluating standalone computers for security; it outlines several different levels of secure computers as shown in Figure 1.[4]
- *Yellow Book*—A guideline that states the environments ("the external circumstances, conditions, and objects that affect the development, operation, and maintenance of a system") in which each *Orange Book* class offers adequate protection.[5]
- *Red Book*—An NCSC standard for interpreting and applying the *Orange Book* requirements to the evaluation of networks.[6]
- *Green Book*—A guideline that provides suggestions for the initialization, administration, and maintenance of password systems.[7]

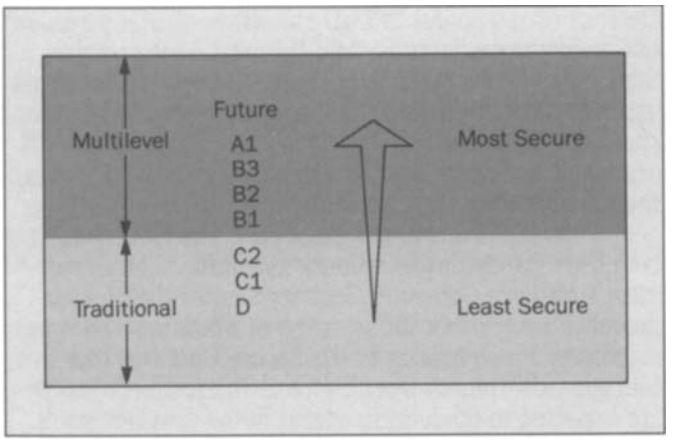

Figure 1. *Orange Book* ratings for computer security range from D to A1, with A1 being the most secure. Ratings of B1 and above include multilevel security.[4]

Documents on database security and audit guidelines, as well as information security tutorials, will be available soon.

Secure data network system. The Secure Data Network System (SDNS) is a program sponsored by the National Security Agency to develop standards for secure data networks. The program integrates security features into ISO's Open Systems Interconnection (OSI) Basic Reference Model[2] and OSI communications protocols. The program will issue standards that may then be used by vendors involved in NSA's Commercial COMSEC Endorsement Program. (COMSEC stands for communication security.) It is too early in the development cycle to determine whether the protocols will become DoD standards. For more details, see the article by Karp, Barker, and Nelson elsewhere in this issue of the *AT&T Technical Journal*.[8]

Government OSI profile. The Government Open Systems Interconnection Profile (GOSIP)[9] is the DoD's specification for implementation of protocols conforming to the OSI Basic Reference Model.[2,10] GOSIP specifies a particular selection of possible protocols at each layer as well as the options needed for conformance. It also has a section devoted to security concerns.

Federal Information Processing Standards. The Federal Information Processing Standards are published by the National Bureau of Standards. The FIPS are written by NBS with input from other areas of the government and from the private sector. When ready for distribution, they are sent to each government agency and published in the *Federal Register*. After soliciting comments, the head of the NBS sends the standard, with NBS's recommendation, to the U.S. Secretary of Commerce, who then either signs or rejects the standard. An example of a FIPS security standard is the Data Encryption Standard (DES).[11]

Table II. ANSI Financial Security Standards*

Number	Type of Standard	Status	Date
X9.8	PIN† Management and Security	Published	1982
X9.9	Financial Institution Message Authentication	Published	1986
X9.17	Financial Institution Key Management (Wholesale)	Published	1985
X9.19	Financial Institution Retail Message Authentication	Published	1986
X9.23	Encryption Of Wholesale Financial Messages	Draft	—
X9.24	Financial Services Retail Key Management	Draft	—
X9.26	Access Security for Wholesale Financial Systems	Draft	—

*Defined by the American National Standards Institute Group X9.
†PIN = Personal identification number.

Federal Standards. Federal standards are published by the General Services Administration (GSA); however, the GSA has delegated responsibility for producing and coordinating communication standards to the National Communication System.[12] An example of a federal standard is Federal Standard 1027, regarding the use of the Data Encryption Standard in telecommunication equipment.[13]

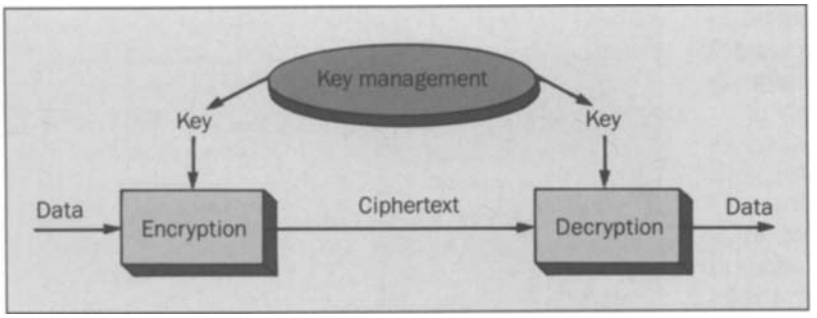

Figure 2. Symmetric key algorithm. Encryption and decryption algorithms use a secret key. Only entities with knowledge of the secret key can decrypt the information. Key management is used to distribute secret keys to authorized parties.

Financial Standards

The financial community, perhaps, the largest security-conscious commercial entity, has devoted extensive resources to information security. The financial community, as referred to in this paper, is concerned with the secure electronic transfer of money or securities. Although banks and institutional traders are the most highly visible part of this community, there are others. Some large corporations have begun to order and pay for products and services electronically. As more money and assets are transmitted electronically, the potential for computer crime increases. And thus, security procedures become more important.

To address the need for security, the financial community is currently developing many security standards. Table II contains some of the standards and work items of the American National Standards Institute. The ANSI groups responsible for financial security are American Standard Committees (ASC) X9 and X12. ASC X9 develops financial services standards; ASC X12 develops standards for business transactions. These committees have met jointly and are now working together to develop security standards for these transfers. International responsibility for financial security standards is distributed between ISO Technical Committee (TC) 68 and Technical Committee 154.

The following are the areas of concern to the financial community:

1. *Message Integrity.* Financial standards use a cryptographic checksum, or *message authentication code,* to provide this service. The ANSI X9.9-1986 and ISO 8730 standards define the process.
2. *Confidentiality.* The financial community uses the Data Encryption Algorithm (DEA X3.92-1981), which is equivalent to the Data Encryption Standard, to protect data.[11] Financial institutions use encryption to protect personal identification numbers (PINs) (ANSI X9.8-1982) and messages (ANSI X9.23–Draft).
3. *Access Security*—There is currently an effort in ANSI X9E.9 to develop a standard (ANSI X9.26–Draft) to protect computer sign-on information, such as passwords.
4. *Key management*—Key management is an essential element of any system that relies on cryptography. Figure 2 shows a typical encryption/decryption process and the relationship of key management. The financial community relies on a key management center (KMC) to distribute keys to subscribers that have a need to communicate. The center is able to audit and assign liability based on a subscriber's knowledge of the key. A subscriber constitutes any entity that relies on the KMC to provide keys for communication. This is a necessary feature for the financial community. Communication among key management centers is being studied so that subscribers of different centers can communicate securely.

The financial area is also working on the protection of financial transaction cards, cryptographic service messages, and efforts to secure business transactions.

OSI-Related Standards

The potential disclosure of trade secrets and corporate plans or finances, as well as deliberate sabotage of projects by hackers or corporate spies, is the catalyst for security among general business customers. Computers and communication facilities must prevent unauthorized

personnel from using or damaging the services provided. Because all valid users do not necessarily share the same privileges, some type of access control policy is usually required. In addition, the confidentiality and integrity of user data must often be ensured.

There is significant international activity to standardize security. The recent expansion of international communication has hastened the development of international standards for information movement and management. The following section outlines some of the developing work on international information security for the OSI Basic Reference Model. ANSI efforts corresponding to this work are primarily performed in ANSI X3, but the discussion of the ISO work encompasses most of the work done in ANSI X3.

iso. The OSI Basic Reference Model has been accepted internationally as the data communication standard. The model separates communication services into seven layers (shown in Figure 3) and defines the interfaces between layers. By standardizing these interfaces, vendors can offer products that are compatible with those of other vendors. This should allow more competition and enhance maintenance of the communication entities.

Part 2 of the OSI Basic Reference Model (developed by Joint Technical Committee 1) operates under the same concept of layering that the Basic Reference Model uses, and thus includes security while maintaining the advantages of interoperability.[10] (Both ISO 7498 and ISO 7498-2 define the model, not the protocols. As such, they lay the foundation for interoperability, but do not define what is necessary to provide it.) Part 2 distinguishes security services (e.g., confidentiality) from the mechanisms (e.g., encryption) that provide services. This is a useful abstraction because it allows the communicating entity to request a service and not be involved with its implementation. The services described by ISO 7498-2 are shown in Table III. As noted earlier, more recent DoD standards adhere to the OSI framework and use the abstractions presented in ISO 7498-2.

ISO 7498-2 allows placement of some services at most layers of the OSI model; however, the services have different implications at different layers. For example, authentication at Layer 7 (the Application layer) refers to user or process authentication, while at Layer 3 (the Network layer), it may provide host authentication. In addition to developing ISO 7498-2, Joint Technical Committee 1 is defining frameworks for certain security services, including authentication, access control, nonrepudiation, security audit,[15] and integrity. Security management is also being addressed.[16]

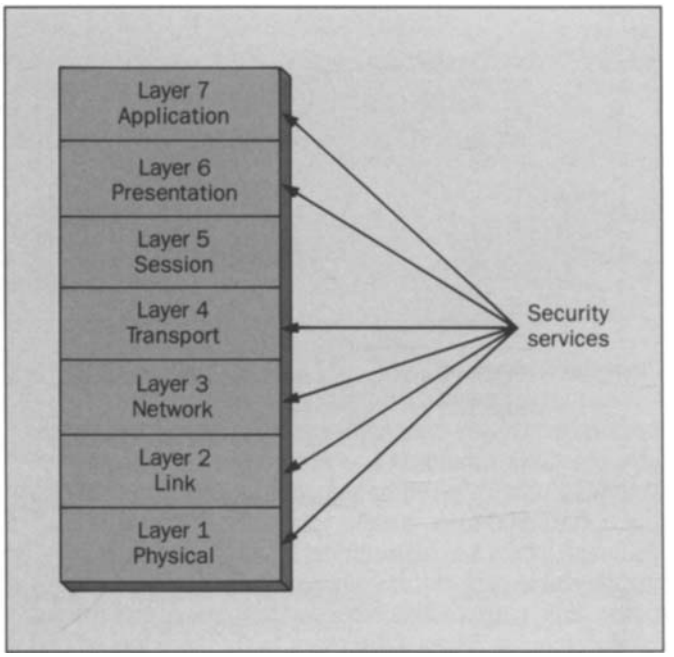

Figure 3. The OSI Basic Reference Model defines interfaces between layers to allow interoperability.[2] Some services can be placed at multiple levels; however, their effect changes depending on placement.

With these frameworks for security services, a set of models will be defined. The models will provide a method for gathering the security services into a bundled service within a layer. For example, a transaction system might require authentication and audit, but no other services. The bundle would be the combination of authentication and audit. The provisioning of a security service often affects the strength of other security services. That is, the accuracy of the audit might be dependent on the integrity of certain fields within the mes-

Table III. ISO 7498-2 Security Services*

Service	Description
Peer entity authentication	Confirms identity of entities
Data origin authentication	Corroborates source of data
Access control	Prevents unauthorized use of resources accessible via OSI†
Connection confidentiality	Protects all user data on a connection from disclosure
Connectionless confidentiality	Protects data within an SDU†† from disclosure
Selective field confidentiality	Protects selected fields within an SDU or within a connection from disclosure
Connection integrity	Detects modification, insertion, deletion, or replay of data within a sequence
Selective field connection integrity	Detects modification, insertion, deletion, or replay within a field over a connection
Connectionless integrity	Provides integrity within a single SDU
Selective field connectionless integrity	Provides integrity within selective fields within a single SDU
Nonrepudiation	Proves delivery or origin to a third party

*Source: "Information Processing Systems–OSI Reference Model–Part 2: Security Architecture," International Standards Organization, Publication No. 7498, Part 2 (to appear).
†OSI = Open Systems Interconnection.
††SDU = Service data unit.

sage. These models draw on the information in the frameworks to provide security within the dictates of the security architecture.[17]

A joint effort between ISO and CCITT has produced an authentication service contained in directories. Directories are used to store addresses and information for services such as electronic mail. Such a directory can store information and serve as the repository for authentication information.[18] The framework allows the directories to provide authentication capabilities. It describes password as well as cryptographic authentication. Joint Technical Committee 1 has other mechanisms to place security at the lower OSI layers, including the use of encryption at Layer 3 (the Network layer) and Layer 4 (the Transport layer), and authentication within the network.

Most of the standards in this section are also available as CCITT standards; however, ISO documents are listed here for simplicity.

European Computer Manufacturers Association. The ECMA, which draws its membership from European computer manufacturers, often submits standards to ISO. A group within ECMA (Technical Committee 32/Task Group 9) is defining an application-layer structure for security in open systems.[19]

Their work assumes that end users are in control of entities that communicate via *application service elements* (ASE). An ASE is part of an application entity that provides an OSI environment capability using underlying services where appropriate.[19] Examples are a file server and a print spooler. The group is concerned with secure communications between these entities—particularly in a distributed environment. The structure they have developed divides these communications into elements called "facilities," each of which has a role to play in providing total security. Combinations of facilities form a secure system. (This is similar in approach to the models referred to in the ISO work above.)

Comparing Standards

The preceding overview of standards activities shows that there are many different independent standards efforts. In comparing standards, it is useful to separate the

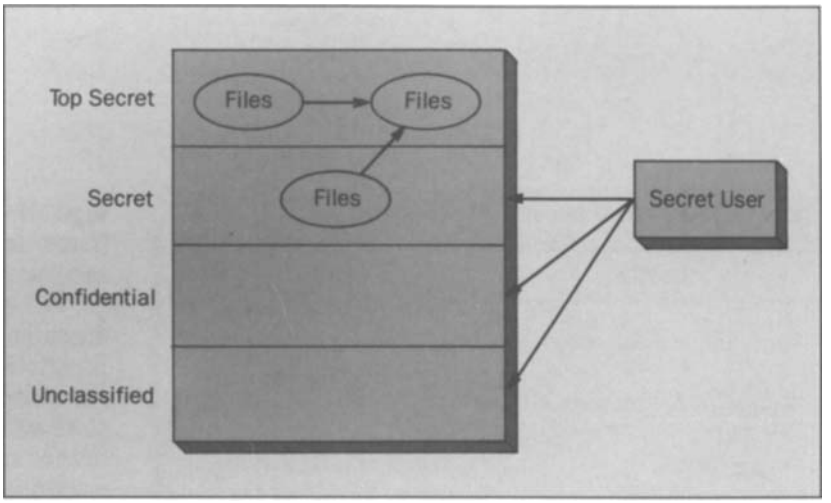

Figure 4. With multilevel security, a user can only read files whose sensitivity is less than or equal to the user's clearance. The flow of information between files is either across the same level or upward to a higher level, but never downward.

comparison into two parts:

- Differences in security standards based on functionality
- Differences in standards based on the degree of security needed.

Functionality. While both the DoD and the OSI security standards place security services at multiple layers within the OSI Basic Reference Model, financial standards place their services primarily at Layer 7 (the Application layer). A *Convener's Guide* for Technical Committee 68 states that "no reliance on security features below Layer 7 shall be allowed in TC 68 standards."[20] Thus, financial security standards can not prevent certain attacks, such as traffic flow analysis and some types of denial of service.

DoD data have marking requirements. Marking is usually a label that represents the sensitivity of data or some type of handling restriction. Strict electronic safeguards must be used to control the distribution and storage of data based on markings. Some marking requirements exist for paper documents within the commercial sector; however, most corporate policies do not require markings for electronic data.

Multilevel security can handle data with different sensitivity levels on the same computer and simultaneously permit access by users with different security clearances.[4,10] Several different models govern information flow on these computers; however, multilevel security as described here is based on the DoD version of multilevel security. Multilevel security provides one method of controlling access based on labels. As shown in Figure 4, multilevel security (1) assigns sensitivity levels for data objects (such as files) and (2) assigns clearances for active entities (such as users). The flow of information is either across the same level or upward to a higher level, but never downward.

DoD standards rely on multilevel security; no commercial security standards have this type of access and flow constraint. Some have suggested using labels such as *proprietary* to help provide commercial multilevel security; however, no widespread rules govern the distribution of this information. One does not have to be a member of a company to have access to that company's *proprietary* information. It is possible to have nondisclosure agreements, or any number of other exemptions. In the DoD, to access data marked as *secret,* one *must* be cleared at least to that level. In order to implement multilevel security, it must be possible to state concisely the rules that apply. This is practical in the DoD because of a well-defined rule base; however, it is currently impractical for commercial applications.

The DoD also uses *mandatory* and *discretionary access control.* (See Table I for definitions of these terms; for a more formal definition, see the *Orange Book.*[4]) The ECMA Technical Committee 32, Task Group 9 considers the DoD policy of mandatory and discretionary access control an oversimplification of the problem. The group does consider the separation of trusted code from untrusted code a useful and necessary abstraction.[19] The reference to trusted code includes the concept of defining a *trusted computing base* that mediates all security access and contains the part of the operating system that enforces security policy.[4,10,21] It is unclear whether the ECMA's endorsement extends to the idea of *trusted functionality,* a process that is assumed to function cor-

rectly with respect to some criteria.[4,10]

Since the NCSC was created, there has been continuing debate about the applicability of its work to the general computer security problem. The DoD position is clearly stated:

. . . prevention of unauthorized access is the primary need. Others in the private sector, however, contend that far greater attention must be paid to the potential for system misuse by persons who already possess authorization.[3]

The applicability of multilevel security continues to be a popular subject for papers. The *Proceedings of the 1987 IEEE Symposium on Security and Privacy* as well as the *Proceedings of the 10th National Computer Security Conference* both contain articles questioning multilevel security.[22,23]

Degree of Security Provided. Commercial and DoD communities require encryption algorithms for confidentiality and message integrity. The choice of an algorithm for DoD applications versus commercial applications has been the subject of many heated debates. The DoD generally prefers secret algorithms because secrecy adds another barrier to breaking algorithms. The commercial sector (and some government bodies) prefer a published algorithm to permit international communication. The DoD also prefers to have many different algorithms, so that a limited amount of data is at risk if one is broken. The commercial sector prefers only one encryption algorithm to allow interoperability among vendors.

Computer logging requirements are necessary in the DoD, but the events audited, as well as the purpose of the audit, are different from those of the commercial sector. A computer audit is the logging of events into a system log file for later review. Computer audit requirements in the DoD are primarily intended to detect disclosure, whereas computer audit requirements of the financial community are intended to help assign liability.

Almost all communities require some type of confidentiality and some type of message integrity. However, communities differ in the strength of the mechanisms that they employ. For example, in some communities, a simple, cyclic redundancy check might be enough to protect against modification. In others, a cryptographic check function is needed. The DoD considers confidentiality more important than integrity because the release of information poses the greater threat. (There are exceptions, such as certain tactical environments, in which integrity is more important than confidentiality.) Commercial applications generally view integrity as equal to or more important than confidentiality.

A different underlying philosophy can also be noted between the DoD and commercial applications. The commercial sector applies a cost/benefit analysis to security. If the cost associated with losing the information is less than the cost of insuring it or protecting it, then accepting the potential loss would be a prudent business decision. To the DoD, information is often critical to national defense, so a cost/benefit analysis may not be meaningful.

Proving the authenticity of users is a ubiquitous security problem. Once again, the strength of the mechanism lies in the different needs of the application. User authentication verifies the identity of the user. A password verifies the identity of the user because no other user should be able to guess the secret password. In the retail financial communities, a 6-digit *personal identification number* (PIN) can be used. Cryptographic authentication is required for some DoD applications.

Conclusion

This paper has reviewed some of the major standards activities in information security. There are numerous activities, and more effort should be spent coordinating standards in different areas. Some coordination is occurring as government and ANSI groups attempt to make standards compatible with ISO. The concerns of ISO 7498-2 have been incorporated into DoD standards, including Part 2 of the *Red Book* and SDNS.[6] Also, Appendix A of the *Red Book* allows the division of the network policy into components, each of which supports the overall policy. This is similar to the concept that the ECMA has proposed in the division of the facilities.

There is a considerable need for security standards. Standards can reduce the cost of security products, aid interoperability, and give a meaningful evaluation of quality. At the same time, the underlying needs of users must not be ignored in establishing similar standards. It is

questionable whether multilevel security will ever be applicable to commercial communities because these groups lack the underlying classification systems and policies. Different communities have different needs and philosophies about security that must be considered when developing standards.

References

1. M. Ferris and A. Cerulli, "Certification: A Risky Business," *Proceedings of the 10th National Computer Security Conference*, September 21-24, 1987.
2. "Information Processing Systems—OSI Reference Model," International Standards Organization, Publication No. 7498, October 1984.
3. L. D. Faurer and R. H. Courtney, "Computer Security, the Defense Department, and the Private Sector—A 3-Part Dialogue about Fundamental Objectives and Needs," *Computer Security Journal*, Summer 1984.
4. "DoD Trusted Computer Systems Evaluation Criteria," United States Department of Defense, Publication No. 5200.28, December 1985.
5. "Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments," United States Department of Defense Computer Security Center, Publication No. CSC-STD-004-85, June 1985.
6. "DoD Trusted Network Interpretations," National Computer Security Center, Publication No. NCSC-TG-005, Version 1, July 1987.
7. "DoD Password Management Guideline," United States Department of Defense Computer Security Center, Publication No. CSC-STD-002-85, April 1985.
8. B. C. Karp, L. K. Barker, and L. D. Nelson, "The Secure Data Network System," *AT&T Technical Journal*, Vol. 67, No. 3, May/June 1988, pp. 19-27.
9. "Government Open Systems Interconnection Profile," Draft, United States Department of Defense, April 1987.
10. "Information Processing Systems—OSI Reference Model— Part 2: Security Architecture," International Standards Organization, Publication No. 7498, Part 2 (to appear).
11. "Data Encryption Standard," U.S. Department of Commerce, National Bureau of Standards, Federal Information Processing Standards, Publication No. 46, January 1977.
12. D. K. Branstad and M. E. Smid, "Integrity and Security Standards Based on Cryptography," *Computers and Security*, 1982, pp. 255-260.
13. "Telecommunications: General Security Requirements for Equipment Using the Data Encryption Standard," General Services Administration, Publication No. FED-STD-1027, April 14, 1987.
14. H. J. Podell and M. D. Abrams, "A Computer Security Glossary for the Advanced Practitioner," *Computer Security Journal*, Vol. IV, No. 1, Summer 1985.
15. "Proposal for the organization of work on Security within SC 21," International Standards Organization Technical Committee 97, Publication No. ISO/TC 97/SC 21 N 2025. Source: ISO/TC 97/SC 21/WG 1, June 1987. (This publication no longer reflects current direction.)
16. "Proposed Draft for Management Information Services Definition, Part 7, Security Management Service Definition," International Standards Organization Technical Committee 97, Publication No. ISO/TC 97/SC 21 N 1386. Source: ISO/ TC 97/ SC 21/WG 4, September 1986.
17. "Draft Plan for the Work on Security in SC 21," International Standards Organization, SC 21/WG 1, Ad Hoc on Security, March 1988.
18. "The Directory—Authentication Framework," International Standards Organization, Publication No. ISO DIS 9594-8 (Draft International Standard), and Draft Recommendation X.509, November 1987.
19. T. A. Parker, "Security in Open Systems—A Report on the Standards Work of ECMA's TC 32/TG 9," *Proceedings of the 10th National Computer Security Conference*, September 21-24, 1987.
20. *Convener's Security Guide*, International Standards Organization Technical Committee 68, Publication No. ISO TC 68/SC 2/WG 2 N 186, December 1987.
21. J. P. Anderson, "Computer Security Technology Planning Study," No. ESD-TR-73-51, Vol. I AD-758 206, ESD/AFSC, Hanscom Air Force Base, Bedford, Massachusetts, October 1972.
22. *Proceedings of the 1987 IEEE Symposium on Security and Privacy*, ISBN 08186-0771-8, Oakland, California, April 27-29, 1987.
23. *Proceedings of the 10th National Computer Security Conference*, September 21-24, 1987.

Biographies (continued)

development for secure/private information movement and management systems. He has a B.A. in mathematics and physics from Phillips University, Enid, Oklahoma, an M.S. in mathematics from Kansas State University, and a Ph.D. in mathematics (computer science) from The Ohio State University.

(Manuscript received April 19, 1988)