THE SECURE DATA NETWORK SYSTEM

Bennett C. Karp, L. Kirk Barker, and Larry D. Nelson

Bennett C. Karp *and* ***L. Kirk Barker*** *are members 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. Karp joined the company in 1984 and is working on information security issues in government systems. He has a B.A. in physics and mathematics from the State University of New York at Binghamton, and an M.S. and a Ph.D. in physics from the University of Pittsburgh. 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. Nelson joined AT&T in 1965 and is responsible for*

(continued on page 27)

Providing security for data communications is quite complex, especially in contrast to traditional security systems for voice communications. The Secure Data Network System (SDNS), a joint program of the U.S. government and telecommunications and computer industry representatives, is developing security standards for data networking. The SDNS program is incorporating security into the Open Systems Interconnection (OSI) framework to ensure interoperability and compatibility of equipment and services. SDNS functionality will be built into or added onto communications equipment such as personal computers, workstations, and host computers, and will provide security services such as confidentiality, integrity, authentication, access control, and sender nonrepudiation. Both real-time and store-and-forward communications will be supported.

Introduction

Data networking is becoming increasingly important to the functioning of government and industry. Information of all types is rapidly communicated among terminals and computers. Much of this information is sensitive, either by itself or in aggregate. The protection of these network communications is recognized as an important issue, especially to the U.S. government (and its contractors dealing with classified or sensitive data). In certain parts of the commercial sector, including the financial community, such protection is also important.

To meet the growing need for secure data networks, the National Security Agency (NSA) has started a program called the *Secure Data Network System* (SDNS). AT&T, along with ten other companies and several U.S. government agencies, including the National Bureau of Standards (NBS), is working to define the necessary architectures and protocols within the framework of the International Standards

Organization Open Systems Interconnection (OSI) Basic Reference Model to embody data communications with security.[1] SDNS protocols will be incorporated into the hardware as front-end devices or embedded into a host (computer) system. SDNS devices will be available for the protection of both classified data and sensitive, but unclassified, information. Key management support will be provided to SDNS devices by a centralized *key management system* (KMS). (Key management is the generation, distribution, and accounting of cryptographic keys.) SDNS will use cryptographic algorithms, developed and approved by the NSA.

How Security Complicates Data Networks

Providing security for data networks is a complex problem. Today's (and tomorrow's) data networks have been transformed because of considerations of technological evolution, efficiency, throughput, error rates, and economics. Data security must fit into this framework.

Communications rely on protocols, "a set of rules that govern the operation of functional units to achieve communication."[2] A structured set of protocols for communications is known as a computer-communications architecture, or an *architecture*. Security must be incorporated into the appropriate protocols within an architecture so that it does not adversely affect the performance of the communications functions.

The security for data networks is more complex and has a wider scope than security for traditional voice systems. Certain security services, such as *integrity* (preventing the modification or insertion of data) and *nonrepudiation* (proving to a third party that data were sent or received, i.e., a signature or receipt capability), do not generally apply to voice systems.

General-purpose security solutions must be adaptable to a wide range of equipment, systems, and applications. An end system might be a personal computer, a workstation, a minicomputer or mainframe, or a front-end processor. Security functions might be built into a switch or other network equipment. Diverse data rates and communications media can complicate security in data networks.

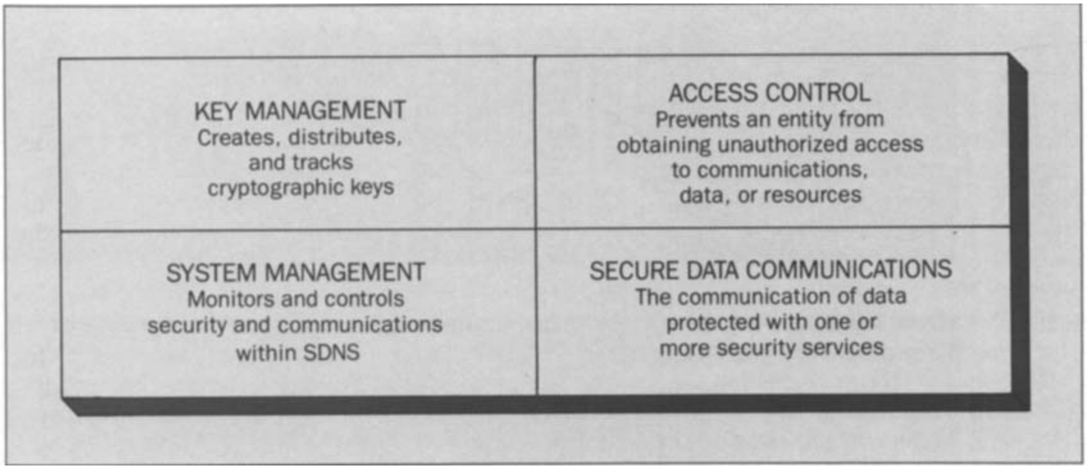
Finally, the distinction between data processing (i.e., computers) and communications is not clear. For example, a user could be logged on to one computer system and accessing a database on another system. The problem of authenticating the first system and user to the second (remote) computer and controlling access to the database is closely related to the security of the communications between the two systems. It is not possible for the second system to rely on any of the communications it receives from the first system if the communications between the systems are unprotected. If the first computer is unsecured, the second system may not be able to determine the true identity of the user on the first machine. And, if the second system itself is unsecured, it can not protect the database no matter how secure the inter-computer communications. The point is that the security of the end systems affects the security approach for the network.

Standards

Standards are necessary for interoperability in data networking, with or without security. The International Standards Organization (ISO) and other bodies are working to meet this need for standards; the OSI Basic Reference Model and the specific protocols developed under ISO are evidence of progress in this area. (See the preceding article on standards by Barker and Nelson in this issue of the *AT&T Technical Journal.*[3])

Incorporating security into data networking requires an effort parallel to ISO and other standard-setting bodies. ISO has begun work on incorporating security into the OSI Basic Reference Model.[1] SDNS is relying on a more sophisticated system for key management than is defined by ISO. In addition, some security requirements, such as tamper resistance, formal proofs, and denial of service, are outside the scope of the OSI framework.

Security must fit into the existing structure of data networking. A separate set of standards for security would limit the applicability of security, curtail interoperability, and increase development costs. The SDNS program is designed to incorporate security into existing or emerging international standards.



KEY MANAGEMENT
Creates, distributes, and tracks cryptographic keys

ACCESS CONTROL
Prevents an entity from obtaining unauthorized access to communications, data, or resources

SYSTEM MANAGEMENT
Monitors and controls security and communications within SDNS

SECURE DATA COMMUNICATIONS
The communication of data protected with one or more security services

Figure 1. The four functional areas within the Secure Data Network System (SDNS) that combine to provide information security.

The SDNS Approach

To meet the need for data networking security, NSA has joined with other federal agencies and eleven major telecommunications/computer companies in the SDNS program. The program's objectives are to:

- Develop a security architecture and supporting protocols in an OSI framework and develop a user-friendly key management system (KMS)
- Produce a family of affordable, interoperable types of equipment that implement SDNS functionality.

The SDNS program is establishing methods and working to establish standards for secure data networking. By including major vendors of telecommunications and computers in the program, the SDNS architectures and protocols are expected to gain widespread acceptance. The National Bureau of Standards and the Defense Communications Agency also are participating in SDNS.

Achieving interoperability is an important objective of SDNS. That is, SDNS devices operating at the same layer of the OSI Model and providing the same security services should be interoperable. (For further discussion of layers as defined in the OSI Model, see Figure 3 in Reference 3.) Minimum essential requirements for interoperability and security are being determined under the SDNS program.

The emerging standards for data networking are being followed closely by the SDNS program. Security is being incorporated into the OSI seven-layer model. Particular attention is being paid to the OSI Security Architecture[4] and emerging protocol standards. The Transport layer security protocol being defined by SDNS, for example, is defined as an addendum to the ISO Transport Protocol (TP4).[5]

SDNS will offer the user a variety of the security services defined in the OSI Security Architecture, including:

- Data confidentiality—Keeping information secret
- Data integrity—Preventing undetected modification
- Peer-entity authentication—Identifying the far-end user, process, or processing element, and determining the attributes of such
- Access control—Restricting communications or access to data, based on authentication information
- Sender nonrepudiation—Digital signatures.

The actual set of services used is determined on a call or session basis.

SDNS uses cryptographic and key management algorithms developed and approved by NSA. These algorithms have been specified for use in SDNS, although the architecture is not dependent on any particular algorithm; other functionally equivalent algorithms could be used in an alternative, SDNS-like system.

SDNS will rely on a centralized *key management center* (KMC). This system will provide cryptographic keying material in a user-friendly manner. Users will not need to interact with the KMC on a session basis.

Because different networks have varying policies and controls, SDNS will provide the tools to solve the network security problem, rather than dictate a particular solution. Implementations of SDNS must address all aspects of security and consider the complexities of interconnecting end systems with different levels of security.

SDNS will have two types of equipment available: *Type I* equipment protects all levels of information including classified; *Type II* is restricted to the protection of unclassified data. Controls for Type II equipment are less strict than for Type I.

SDNS Architecture

Secure data networking consists of the four functional areas shown in Figure 1. Each of these areas is supported by protocols, many of which are being defined within the SDNS program.

SDNS provides security services at several layers of the OSI Basic Reference Model. Figure 2 shows the protection provided and the SDNS implementation at each layer. In addition to electronic mail, other applications not in real-time, such as file transfer, will also be addressed.

One SDNS device uses KMS-supplied keying material to establish secure communications with a compatible SDNS device. As part of the session setup, a unique traffic key is generated that can be used to provide data confidentiality and data integrity services. Each SDNS device verifies the identity and security credentials of the other, and access control privileges for the ensuing communications are determined. If the devices can not communicate for security reasons (e.g., the hosts are single-security-level computers that operate at different security levels), then the SDNS devices do not allow secure communications. If the session is allowed, a negotiation process is used to determine additional access control restrictions and to establish which security services will be used.

Once the session is begun, the two hosts are able to communicate, subject to the access control restrictions established earlier and with the protection of the selected security services. In transmitting data, SDNS devices take

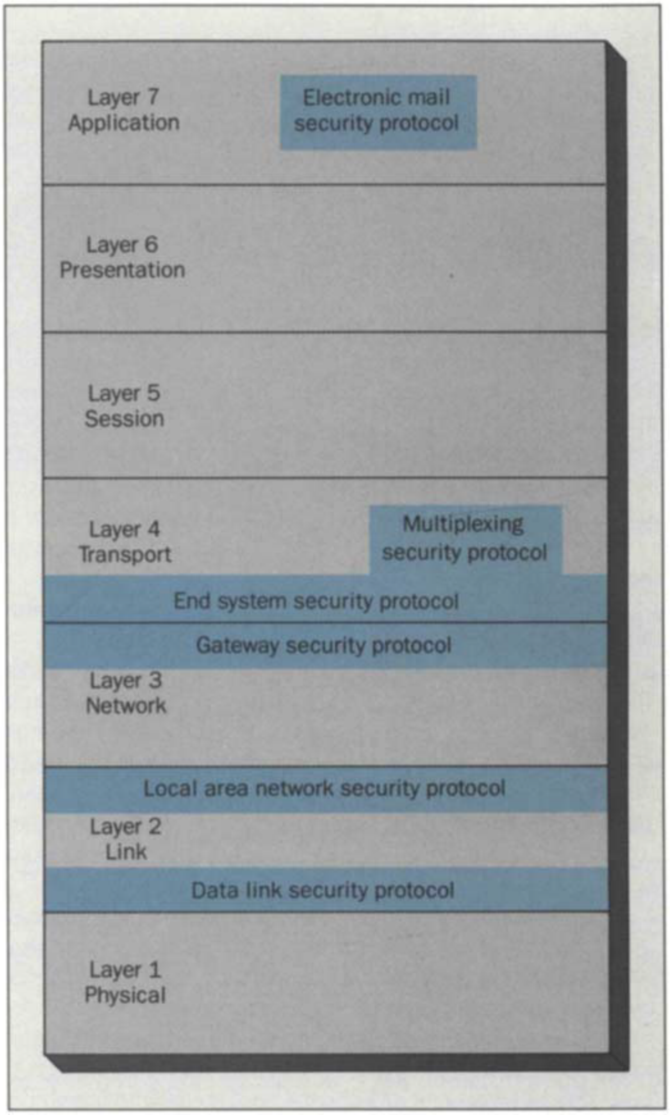

Layer 7
Application
Electronic mail security protocol
Layer 6
Presentation
Layer 5
Session
Layer 4
Transport
Multiplexing security protocol
End system security protocol
Gateway security protocol
Layer 3
Network
Local area network security protocol
Layer 2
Link
Data link security protocol
Layer 1
Physical

Figure 2. The insertion of SDNS security protocols will protect various communications entities. In the Application layer, only electronic mail is protected by the SDNS secure message protocol. At the Transport layer, there are two critical portions: the multiplexing security protocol and the end system security protocol.

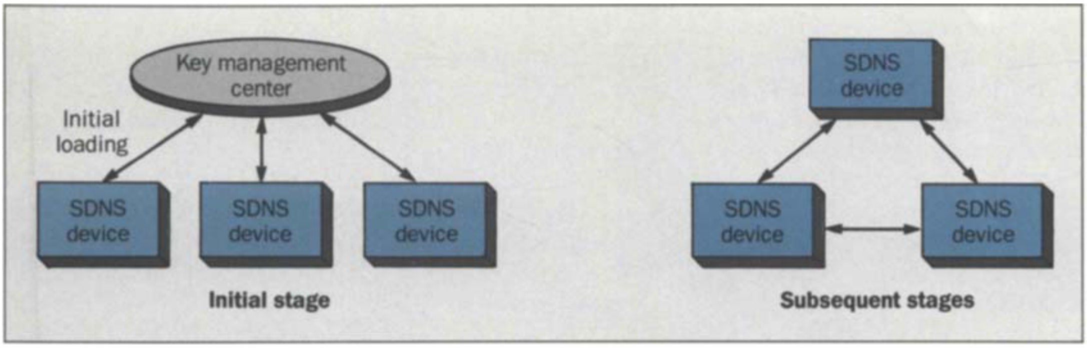


Figure 3. Once the key management center (KMC) initially loads the SDNS devices, subsequent interchanges between the components do not include the KMC.

host-supplied data, check any applicable access control restrictions, create the secured data protocol units according to the appropriate SDNS protocol, and transmit the data to the far end. The reverse process takes place when data are received.

Key Management

Key management (the generation, distribution, and accounting of cryptographic keys) is a crucial part of any distributed system that uses cryptography. Because the security of the system depends on the strength and secrecy of the keys, the keys must be generated and distributed in a way that minimizes the possibility of compromise. Accounting procedures detect any compromise that might occur. Recovery mechanisms minimize any losses that might result from a compromise, and then restore the system to full security.

Key management should be user friendly. Keying operations should not significantly impede network performance or affect operating costs. Traditional secure communications have relied on manual distribution of keys encoded onto paper tape. Such a system is unacceptable for the modern, high-capacity systems that an SDNS serves. The costs and complexity of manual distribution quickly become prohibitive as the number of users increases. Furthermore, manual key distribution forces tradeoffs in security.

SDNS uses a state-of-the-art system developed by NSA that relies on a centralized key management center (KMC). The KMC issues one or more sets of special keying material for each SDNS device when the device is put into service. The device can then operate securely; only periodic interaction with the KMC is required. Figure 3 shows this procedure. This method represents a significant advantage over a system having a *key distribution center* (KDC), which requires third-party interaction during each call setup. The time for call setup is reduced considerably with the SDNS KMC, and problems associated with a large number of users in a KDC are eliminated.

In setting up a secure session, two SDNS devices exchange information. In the process, they authenticate each other's identity. The authentication information is then used to make access control decisions [e.g., the security level(s) of the data to be accessed and transmitted between the two parties]. The derived key is used as input by the cryptographic algorithm that protects the transmitted data. Figure 4 is a functional representation of this process.

Access Control

Access control is the granting and enforcement of privileges to an individual (or process) based on the information provided by an authentication mechanism. Authentication is the process that assures each communicating party of the other entity's identity and privileges. Authentication in SDNS refers to peer-entity authentication; the financial community is concerned with message authentication (i.e., verification of the integrity of the message).

Once this information is known and its accuracy guaranteed, the local system or user can make appropriate decisions about what data can be transmitted to the far

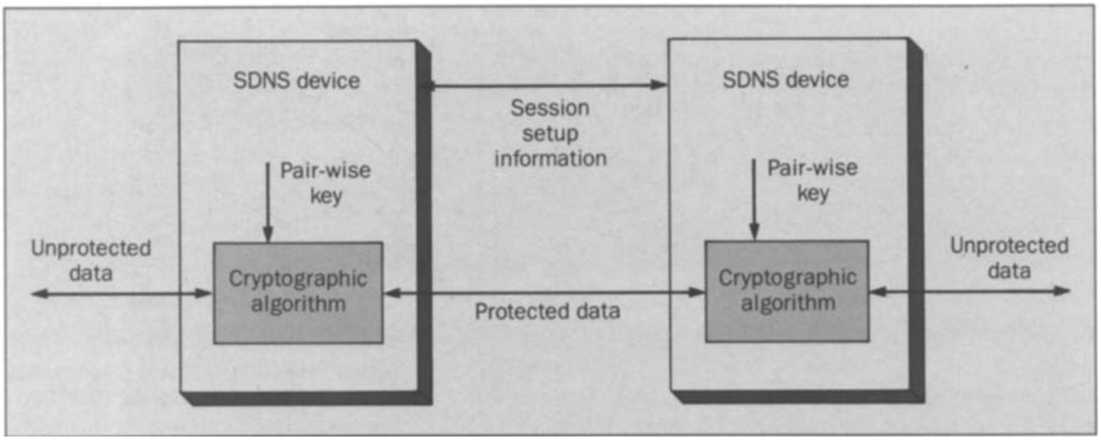


Figure 4. A key is created to authenticate users. The key can then be used to protect data transmitted among SDNS devices.

end. Thus, authentication and access control are closely related: authentication is a prerequisite of access control.

Access control is needed because users can have different privileges. In a network without access control, all users have the same privileges. Each would be able to access all network resources. Access control oversees host interconnections, access to system management databases, and access to network resources. An access control policy must be integrated into the overall security policy of the network. It is the primary means of enforcing that network policy. Authentication in SDNS occurs as part of the key management process previously described.

In an interactive exchange, once identity information has been authenticated, there are two parts to access control. (The process is slightly different for store-and-forward environments; however, the concepts are the same.) The first is the determination of what information may be communicated between peers. If no information transfer is allowable, the connection must be aborted. In SDNS, this first part of access control is referred to as *peer access approval* (PAA). PAA occurs at the time of session setup after the authenticated identity information becomes available.

In SDNS, the second part of access control, known as *peer access enforcement* (PAE), takes place over the life of the connection. The access rules determined in the first part must be enforced for every data transfer and for all attempts to use network resources. SDNS devices have the primary responsibility for PAE. They might check security labels to ensure that the access control rules are not violated. This activity is performed as part of the SDNS data transfer protocols.

The responsibility for access control is shared among SDNS devices, the host computer and its processes, and individual users. SDNS devices play an important role in enforcing the access control rules, however trust levels of the systems and users determine just how restrictive those rules need to be. Users and systems are generally trusted to some degree; security clearances or U.S. Department of Defense (DoD) *Orange Book* evaluation levels are examples of measures of trust.[6] If the host system is relatively untrusted, the SDNS device must enforce more restrictive access control rules. When the host system and its users have a higher level of trust, data having a broader range of levels of sensitivity may be processed, stored, or transmitted.

System Management

System management is important in any large network or communications system. Its functions include fault detection and isolation, performance and status monitoring, optimizing use of network resources, and maintenance of system databases. Managing a secure network is more complicated than managing a "standard" system.

When security is added to the network, the management of the security becomes an additional system management function. Security management includes tracking of security-relevant events, ensuring that security does not have a serious impact on performance, and managing additional security-related devices.

Furthermore, the addition of security can complicate "standard" system management (i.e., system management functions that are implemented even when security features are not present in the networks). Performance monitoring could be impaired. Diagnostic tests and fault isolation could also be affected by encryption equipment embedded in the network.

SDNS system management provides monitoring and control of SDNS devices and security services for security organizations, system support organizations, and end users. System management in SDNS is responsible for the control and coordination of the security and communications functions. SDNS system management is based on the ISO system management model.

SDNS system management consists of the processes that control the communications and security functions of SDNS devices between (and within) SDNS entities.

To provide this support, six management agents have been defined within the SDNS program:

- Connection management—which arbitrates the establishment of SDNS connections
- Key management—which supports the keying operations over the life cycle of the keying materials
- Access control management—which maintains access control databases
- Audit control management—which oversees the gathering of reports and security audit information
- Health and status management—which performs non-security-related functional testing and status monitoring operations
- Operations management—which provides network support.

Secure Communications

Secure data communications are data communications protected by one or more security services. The most common applicable security services are data confidentiality and data integrity. Data confidentiality means that the data are protected from unauthorized disclosure. Encryption of data is used most often to provide this service. Data integrity means that data can not be modified, inserted, deleted, or replayed without detection. An example of a data integrity mechanism is the Message Authentication Code (MAC), used to protect wholesale electronic funds transfers in the banking industry.[7]

In the more narrow context of secure data communications, access control means that transferred data are restricted and handled according to the overall access control policy.

Nonrepudiation, either of the sender or the recipient, is a less common security service, although it can be extremely useful in certain applications. With nonrepudiation, it can be proven to a third party that the sender was the originator of the data (sender nonrepudiation) or the recipient did in fact receive the message (recipient nonrepudiation). Nonrepudiation is stronger than data-source authentication because proof to a third party is possible; the recipient (with sender nonrepudiation) can not "forge" a message and claim that it came from another user. Nonrepudiation is analogous to the use of signatures and receipts for paper communications. Sender nonrepudiation generally is provided via a digital-signature mechanism. Recipient nonrepudiation is more difficult to implement; SDNS will provide a sender, but not a recipient, nonrepudiation service.

The direct provisioning of the secure data communications capability comes from SDNS devices. These devices rely on the KMS for key management services, on system management to oversee SDNS key management and access control, and on the underlying infrastructure of people, procedures, and communications systems for communications and security support.

Relying on this support, the SDNS devices provide secure data communications capability to SDNS users. An SDNS device could either be embedded in a host computer or other communications device, or an in-line SDNS device could be used to protect host equipment that did not include SDNS functionality.

SDNS uses directory servers to support various special, secure data communications services. The most significant of these is electronic mail. The SDNS key management algorithm need not be executed in real time. A user who wants to be able to receive electronic mail securely can post the appropriate information with a directory server. Another user can retrieve that information and use it to generate a traffic key. The key is used to secure the mail message that is then sent to the first user. When the message is received, the first user is able to generate the same traffic key and thus recover the message.

Supporting Protocols

The SDNS program defines protocols that support security and communications functions. Protocols define the content and structure of the communications between entities on two different systems. An entity is something capable of sending or receiving information (e.g., an application program or file transfer package); a system is a physically distinct object that contains one or more entities (e.g., a host computer or a network node.)[8]

Protocols allow two entities to communicate, i.e., "speak the same language." A protocol defines a mutually agreeable convention for exchanging information.

In a "standard" communications application (one in which security is not an explicit concern), the following are considered in developing protocols:

- Interoperability—ensuring that communications can take place between a wide variety of systems.
- Performance—ensuring that the protocols are not structured in a way that would have an adverse effect on network performance (e.g., throughput, error detection/correction).
- Expandability—ensuring that future developments can be incorporated transparently so that the protocols do not inhibit progress.

SDNS is also faced with integrating security into protocols. Our primary concern is to create a high level of security; however, it must be achieved with a minimal impact on the three areas mentioned above.

Protocols are needed in all areas of SDNS. They are used, for example, for communications between pairs of SDNS devices, between an SDNS device and the KMC, between an SDNS device and an SDNS directory server, between an SDNS device and a system-management host, and between the KMC and an SDNS directory server. Protocols are used in all four functional areas: key management, access control, system management, and secure data communications.

SDNS is compatible with the OSI Model. Under that model, protocols are defined between entities that operate at the same layer. In the areas in which ISO has defined protocols, the SDNS program is trying to take those protocols and add security. Where protocols have not yet been defined, SDNS is following the overall OSI approach.

For example, the SDNS gateways security protocol (SP3) provides secure data communications at the Network layer. It can provide data confidentiality and connectionless data integrity. Here, "connectionless" means that data integrity service applies on a per-PDU basis. (PDU stands for protocol data units.) Integrity of messages must be provided at the Transport layer or higher.

A Network layer security protocol has been defined in the SDNS program so that security can be implemented for intermediate network devices or, in particular, gateways. SP3 is defined in SDNS as a sublayer of the Network layer that resides directly below the Transport layer. Thus, SP3 is effectively at the interface between the Transport and Network layers.

SDNS Outlook

SDNS is an important step toward a secure data-networking architecture. The program integrates state-of-the-art cryptographic and key-management algorithms into the existing and evolving international standards for data communications. The communications architectures and protocols are being designed with the goals of interoperability, wide applicability, and compatibility with international standards.

User needs in both the classified and unclassified arenas are being considered. International standards and other U.S. government efforts, such as the *Red Book* and the Government Open System Interconnection Profile (GOSIP), are receiving attention.[9,10]

Specification of the initial set of protocols is currently being completed. These protocols will be tested and analyzed. Other protocols not yet given high priority must be considered. We still have a considerable systemintegration task of building and certifying SDNS devices, developing the KMC, and creating the procedures and organizations to support SDNS. If current plans are maintained, SDNS devices should be available and operational in 1991.

References

1. "Information Processing Systems—OSI Reference Model," International Standards Organization, Publication No. 7498, October 1984.
2. *American National Dictionary for Information Processing Systems,* American National Standards Committee, X3/TR-1-82, 1982.
3. L. K. Barker and L. D. Nelson, "Security Standards—Government and Commercial," *AT&T Technical Journal,* Vol. 67, No. 3, May/June 1988, pp. 9-18.
4. "Information Processing Systems—OSI Reference Model—Part 2: Security Architecture," International Standards Organization, Publication Number 7498, Part 2 (to appear).
5. "Information Processing Systems—Open Systems Interconnection—Connection Oriented Transport Protocol Specification," International Standards Organization, ISO 8073, Reference No. 8073-1986(E), 1st edition, 1986-07-15.
6. "DoD Trusted Computer Systems Evaluation Criteria," United States Department of Defense, Publication No. 5200.28, December 1985.
7. "Financial Institution Message Authentication (Wholesale)," X9.9-1986, American Bankers Association, 1986.
8. W. Stallings, *Data and Computer Communications,* Macmillan Publishing Co. Inc., New York, 1985.
9. *Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria,* Version 1, National Computer Security Center, NCSC-TG-005, July 31, 1987.
10. "Government Open System Interconnection Profile," Draft, Version 1, United States Department of Defense, April 1987.

Biographies (continued)

systems engineering support and standards and strategy 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 21, 1988)