Data security in computer networks is becoming increasingly important owing to the expanding role of distributed computation, distributed databases, and telecommunication applications such as electronic mail and electronic funds transfer. There are several proprietary network architectures, including Arpanet, IBM's Systems Network Architecture, and Digital Equipment Corporation's Digital Network Architecture, as well as architectures for specialized applications. The International Standards Organization has proposed an architecture with the capability of universal networking as a first step toward protocol standardization. This model is called the reference model of open systems interconnection, or OSI (Figure 1).

In an OSI-based network, encryption can be done in any of the seven layers. The communication subnet consists of switches, multiplexers, or concentrators connecting transmission links. Since these links can be easily accessed, there might be a need for encryption on each data link. One can also choose to encrypt data above the network layer, i.e., the host-host layer, which constitutes an example of end-to-end encryption. The higher the layer at which encryption is performed, the greater security it provides to the user. However, data link encryption can mask traffic characteristics, and that by itself may be of interest to an unauthorized party; therefore, a combination of data link and end-to-end encryption techniques appears desirable.

When designing a computer network, several sources of data insecurity need to be considered. Prominent among these are spurious message injection, message reception by unauthorized receivers, transmission disruption, and rerouting data to fake nodes. To maintain security against these hazards, a combination of en-
Security in networks differs in several aspects from security in a centralized computer system. This is because (1) the switching nodes and concentrators are distributed physically and cannot be considered secure, and (2) the network protocols, if not properly designed, can be used by an intruder to gain access to the network data or have it misrouted.

This special issue of Computer describes many developments in the above-mentioned aspects of data security in networks. In the first article, Selim G. Akl surveys digital signatures. A digital signature is a message-dependent quantity that can be computed only by the sender using private information, and it can be used for

---

**Figure 1. The International Standards Organization's open systems interconnection model for a network connection.**

**Figure 2. The encryption model.**

---

Encryption algorithms on the data and appropriate protocols for message exchanges is utilized. These techniques also facilitate the handling of other problems in computer communication networks, such as key distribution, authentication, privacy, digital signatures, network mail, and transaction verification.

There are two approaches to encryption. The first requires use of a secret transformation (key) to encrypt data that is then sent over a public channel. At the receiving station, the same key is used to convert the enciphered data back into the original form (Figure 2). The transformation key is sent to the authorized receiver over a secure channel and is therefore unavailable to other parties. This method constitutes a private-key cryptosystem.

The second approach is based on the use of separate keys at the transmitting and receiving stations—keys that cannot, in practice, be obtained from each other. Each user keeps one of these two transformations secret and publishes the other, which can then be used to transform data intended for the user. Systems employing this approach are called public-key cryptosystems.

The Data Encryption Standard of the National Bureau of Standards was adopted for use in the US in 1977. This private-key cryptosystem is the dominant system in use today and has been implemented in hardware as well. The major reason for the popularity of the DES is its speed; it takes about 100 milliseconds to implement an 8-bit microprocessor, and the time can be brought down to about 5 microseconds on a custom-built LSI device. This should be compared with Rivest-Shamir-Adleman, or RSA, the most promising public-key system, where encryption of 500-bit numbers (a block size necessary for security) using available technology takes about a half second. This speed is unacceptable for many applications. Faster implementations of the RSA cipher are being developed, however. Implementation speed is not of critical importance in some applications, such as a key-management system, and public-key algorithms are already being used for this purpose.

Public-key systems have some intrinsic advantages over private-key systems. For example, the public-key method provides solutions to problems such as key distribution, secure communication over an insecure channel without exchanging keys, digital signatures, transaction verification, and key exchange. Solving these problems with private-key methods is either more cumbersome or impossible. To exploit the advantages of public-key systems, more efficient implementations are necessary so that encryption time can be brought down to acceptable levels. At the same time, better cryptanalytic algorithms may force the use of greater block sizes for a specified level of security. Significant progress on public-key systems in recent years has led to new encryption and protection algorithms and results in cryptanalysis, such as a subexponential algorithm to obtain discrete logarithms; new algorithms to distinguish prime numbers from composite numbers; and a polynomial time algorithm to break knapsack ciphers. Important new results have also been obtained in applications to digital signatures, design of secure protocols, and implementation schemes for electronic mail.
certifying both the message and its sender. Signature schemes are of two types: those that do not need arbitrators to validate the signed message, and those that do. Both private-key and public-key encryption techniques can be used to generate digital signatures.

Since an unauthorized party can counterfeit public keys or use private keys that have been compromised, the use of public-key encryption alone does not ensure secrecy or a correct digital signature. The article by Dorothy E. Denning discusses the protection of public keys and signature keys. She shows that by using write-once devices such as optical disks, many security requirements for keys can be met.

A protocol is a set of rules to be followed by users to ensure orderly communication. Richard DeMillo and Michael Merritt describe several issues in protocol design and implementation. They argue that new cryptographic tools make it possible to design protocols for new kinds of transactions. The importance of arbitrators in the design of secure protocols is explained and some implementations are described.

An application of the RSA digital signature to electronic mail is described in the article by D. W. Davies. He suggests using a one-way function such as the Data Encryption Standard on the message followed by an RSA signature. He also considers encryption standards issues that will have to be resolved for electronic mail to flow across national borders.

Acknowledgments

I am grateful to Dennis Fife for providing considerable help in editing this issue. I would also like to thank the various reviewers who responded promptly and provided valuable feedback to the authors.

Reference