# Chapter 4

# Security Safeguards and Practices

# CONTENTS

*Page*
Findings . . . . . . . . . . . . . . . . . . . . . . . . . 51
Introduction . . . . . . . . . . . . . . . . . . . . . . . 51
Encryption . . . . . . . . . . . . . . . . . . . . . . . . 54
Encryption Algorithms . . . . . . . . . . . . 54
Message Authentication . . . . . . . . . . . 59
Public-Key Ciphers . . . . . . . . . . . . . . . . 61
Digital Signatures . . . . . . . . . . . . . . . . 63
New Technologies for Private and Secure Transactions . . . . . . . . . . . . . 68
Key Management . . . . . . . . . . . . . . . . . . 69
Voice and Data Communications Encryption Devices. . . . . . . . . . . . . . 71
Personal Identification and User Verification . . . . . . . . . . . . . . . . . . . . 72
Background . . . . . . . . . . . . . . . . . . . . . 72
Conventional Access Controls . . . . . . . 73
Biometric and Behavioral Identification Systems . . . . . . . . . . . 77
Access Control Software and Audit Trails . . . . . . . . . . . . . . . . . . . . . . . . . 83
Host Access Control Software . . . . . . 83
Audit Trails . . . . . . . . . . . . . . . . . . . . . 86
Administrative and Procedural Measures . . . . . . . . . . . . . . . . . . . . . 86
Computer Architectures . . . . . . . . . . . . . 88
Communications Linkage Safeguards . . 89
Port-Protection Devices . . . . . . . . . . . . 89
Satellite Safeguards . . . . . . . . . . . . . . . 90
FiberOptic Communications . . . . . . . . 90
Common Carrier Protected Services.. 90

## Boxes

*Box* *Page*
B. An Example of DES Encryption . . . 57
C. Application of Message Authentication to Electronic Funds Transfer . . . . . . . . . . . . . . . . . . . . . . . 60
D. Host Access Control Software . . . . . 84

## Figures

*Figure No.* *Page*
12. Common Administrative, Physical, and Technical Information Security Measures . . . . . . . . . . . . . . . . . . . . . . 52
13. DES Encryption in Electronic Codebook Mode . . . . . . . . . . . . . . . . . 56
14. Federal Standard for Authentication . . . . . . . . . . . . . . . . . . 62
15. Public-Key Ciphers . . . . . . . . . . . . . . 64
16. Digital Signatures Using a Public-Key Cipher . . . . . . . . . . . . . . . . . . . . 66
17. A Description of the Past Network Environment. . . . . . . . . . . . . . . . . . . 74
18. A Description of the Current/Future Network Development. . . . . . . . . . . . 75
19. The Mechanics of See-Through Security...,... . . . . . . . . . . . . . . . . . . 76
**20.** Biometric Identification Configuration Alternatives: Host-Based v. Stand-Alone . . . . . . . . . . . . 78
21. Example Reports From Audit Trail Software . . . . . . . . . . . . . . . . . . . . . . 87

## Tables

*Table No.* *Page*
5. Major Characteristics of Automated Biometric Identification Types . . . . . 79
6. Configurations and Applications of Biometric Devices . . . . . . . . . . . . . . . 80

## Chapter 4

# Security Safeguards and Practices

## FINDINGS

- Technical safeguards for computer and communications systems are still evolving, as are users' understanding of their needs for them. Products and systems are available for controlling access and auditing use and for encrypting data.
- Technical safeguards alone cannot protect information systems completely. Effective information security requires an integrated set of safeguard technologies, management policies, and administrative procedures.
- Information security hinges on the security of each segment of the increasingly intertwined computer and communications network.
- A number of important techniques are emerging to verify the identities of the senders of messages, authenticate their accuracy, and ensure confidentiality. Mathematical techniques using cryptography cannot only provide improved information security, but also broaden the applicability of electronic transactions in commerce.
- The Federal Government has played an important role in promoting technical standards for selected information safeguards, particularly for cryptography. Yet, the public position of the Government in general and the National Security Agency, in particular, has been inconsistent. This inconsistency is especially apparent in providing Federal leadership for the development of information security standards; e.g., in NSA's reversal of endorsements of an open encryption algorithm and of dependence on consensus agreement in developing encryption-based security standards.
- Questions are being raised about the efficacy of the NSA's developing unified sets of standards and guidelines for government-wide and private nondefense use.

## INTRODUCTION

Technology that can help promote information security can be divided into administrative, physical, and technical measures. Figure 12, which shows examples of each of these categories, demonstrates the diversity of safeguard applications and the range of approaches to improved safeguards.[1]

Like the range of threats and vulnerabilities that afflict different information systems, there is a wide range of safeguards that can help protect them. Although administrative and procedural measures are also fundamentally important to good overall security, this chapter concentrates primarily on technical safeguards. These include the following:

- *Encryption,* which can be used to encode data prior to transmission or while stored in computers, to provide an electronic

[1] 'This section examines safeguards for both computers and communications since many of the measures discussed apply to both.

**Figure 12.—Common Administrative, Physical, and Technical Information Security Measures**

***Administrative security measures:***
- Background checks for key computer employees.
- Requiring authority of two employees for disbursements.
- Requiring that employees change passwords every few months, do not use the names of relatives or friends, and do not post their passwords in their offices.
- Removing the passwords of terminated employees quickly.
- Providing security training and awareness programs.

ŽEstablishing backup and contingency plans for disasters, loss of telecommunications support, etc.
- Storing copies of critical data off-site.
- Designating security officers for information systems.
- Developing a security policy, including criteria for sensitivity of data.
- Providing visible upper management support for security.

***Physical ecurity measures:***
- Locking up diskettes and/or the room in which microcomputers are located.
- Key locks for microcomputers, especially those with hard disk drives.
- Requiring special badges for entry to computer room.
- Protecting computer rooms from fire, water leakage, power outages.
- Not locating major computer systems near airports, loading docks, flood or earthquake zones.

***Technicai security measures:***
- “Audit programs that log activity on computer systems.
- Access control systems that allow different layers of access for different sensitivities of data.
- Encrypting data when it is stored or transmitted, or using an encryption code to authenticate electronic transactions.
- Techniques for user identification, ranging from simple ones such as magnetic stripe cards to more esoteric “biometric” techniques, which rely on hand or eye scanners (just beginning to be used).
- “Kernel’ ’-based operating systems, which have a central core of software that is tamperproof and controls access within the system. *
- “Tempest” shielding that prevents eavesdroppers from picking up and deciphering the signals given off by electronic equipment •

• Generally used only in military or other national security applications in the United States.

SOURCE” U S Congress, Office of Technology Assessment, *federal Government Information Technology Management, Security, and Congressional Oversight, OTA.* CIT-297 (Washington, DC:U.S Government Printing Office, February 1966), p 61

“signature, “ and to verify that a message has not been tampered with.
- *Personal identification and user verification techniques,* which can help ensure that the person using a communications or computer system is the one authorized to do so and, in conjunction with *access control systems* and other security procedures, that authorized users can be held accountable for their actions.
- *Access control software* and *audit trails,* which protect information systems from unauthorized access and keep track of each user’s activities.
- *Computer architectures* that have been specifically designed to enhance security.
- *Communications linkage safeguards,* which hamper unauthorized access to computers through phone lines.

The systems of safeguards that are being developed fall into categories that control access to data or monitor user activities and others that protect the integrity of data, e.g., verify its accuracy. Technology is paving the way for further improvements in these and still other categories. Systems that will combine improving message integrity with preventing unauthorized activity are beginning to set the stage for major new applications with broad commercial applications.

Security is never just a “black box” of technical safeguards that can be purchased and added to computer or communications systems. Moreover, technical measures would be fruitless unless accompanied by suitable policies and administrative procedures. For security measures to be effective, they must be planned for and managed throughout the design and operation of computer and communications systems. This chapter, however, mainly discusses the technology of safeguarding information systems.

In addition, for many types of users, the combination of reasonable effectiveness and convenience are more important than extremely high security. Determining which safeguards are appropriate for a particular computer or communications system requires an analysis of such factors as the value of the information at risk, the value of the system’s reliability, and the cost of particular safeguards. Security experts disagree about how this “risk analysis” ought to be conducted and about the problems with, and validity of, risk analyses. But, some form of risk analysis-whether formal or informal, quantitative or qualitative-remains the chief means by which managers can assess their needs and evaluate the costs and benefits of various security measures.

The National Bureau of Standards (NBS) has played an important role in developing computer security standards. This role has become complicated by the recent entry of the NSA into the standards arena and by NSA efforts to develop comprehensive standards suitable for all users' needs.

There are four driving forces behind the emergence of the new safeguard technologies:

1. developments in microelectronics and information processing, such as smart cards and other hardware implementing encryption algorithms;
z. developments in cryptography, such as asymmetric and public-key ciphers;
3. developments in the mathematics underlying signal processing and cryptography; and
4. developments in software, particularly for processing biometric personal identification data.

A number of technologies exist that can verify that individual users are who they claim to be. Similarly, technologies exist to authenticate the integrity of a message and to ensure its confidentiality. These developments are being applied mainly to solve some of today's problems concerning information security.

Technologies for user verification, often intended for use in conjunction with other access control systems, include: hand-held password generators, "smart" key cards with embedded microprocessors, and a number of personal identification systems based either on biometric measurements or other individual characteristics. Message authentication techniques rely on combinations of encrypting and/or "hashing" schemes to create a code authenticating the accuracy of a message's content. A variation of this technique can provide a "digital signature" that not only authenticates the message, but also establishes the identity of its sender. Encryption methods are widely available to protect against unauthorized disclosure of messages.

What is becoming increasingly apparent, however, is that some of this same technology has far greater potential uses. One of the central observations of this chapter is that measures, particularly technical measures, are beginning to be developed that provide some of the tools likely to prove important in the long term for more secure operation of electronic information systems in uncontrolled, even hostile environments. These include environments, such as the public switched telephone network for example, where sensitive data is unavoidably exposed to risks of being improperly accessed, modified, or substituted, or where errors can be introduced by the system itself, as from normal electronic noise in communications systems. Information security technology shows promise for greatly expanding the range of applications of computer and communications systems for commerce and society. It will accomplish this by reducing the cost of many of today's paper-based business transactions, by providing legally binding contracts executed electronically, and by protecting intellectual property and the privacy of personal data stored in electronic form. (See ch. 5.)

To achieve most of the above, cryptography is critically important. There are no close substitutes for cryptography available today. Cryptography, however, is a technology in which the Government has acted somewhat inconsistently by controlling private sector activity in some ways, while occasionally stimulating it in others. Thus, the technology that is important to future applications of information security is coupled to Federal policies that can encourage or inhibit its advancement. Options for the future role of Federal policies in influencing technological developments are discussed in chapter 7.

There are two principal uncertainties in the future development of safeguards. The first is the extent to which users of computer and communications systems will, in fact, buy and use the safeguards that are available. Some of the key factors that will influence users' actions include their evolving awareness of threats and vulnerabilities, the practices of their insurance companies, the evolution of "standards of due care' related to security practices, the Federal role as a leader and shaper of the field, and news media attention to incidents of misuse. Information and communication system risk analyses, based on historical threat and vulnerability profiles, will influence the marketplace for safeguards. If the demand for safeguards increases, then the market will no doubt respond with more products and techniques. On the other hand, if many users' interest in security levels off, there may be a shakeout in the market for safeguard devices, perhaps leaving mainly those products developed for Government agencies.

The second major uncertainty is the extent to which vendors of these safeguards, in collaboration with users, will be able to develop systems that use multiple safeguards in a simple, integrated fashion. If demand for safeguards becomes a significant fraction of the overall computer and communications system market, the resulting products are more likely to be well integrated, easy to use, and low cost. For someone who needs to gain access to his or her company's mainframe computer from home, for example, appropriate safeguards might include the functions of a hand-held personal identification device, encryption of the telecommunications link, passwords, dial-back modems, and audit logs at both the microcomputer and the host computer. Using such a combination would be tremendously cumbersome at present, requiring multiple pieces of hardware, software, and passwords. Thus, a major challenge for the industry is to develop systems that allow the various safeguards to work together and to become virtually invisible to the user, as well as cost-effective.

# ENCRYPTION

Encryption is the most important technique for improving communications security. It is also one of several key tools for improving computer security. Good-quality encryption is the only relatively sure way to prevent many kinds of deliberate misuse in increasingly complex communications and computer systems with many access points. Of course, encryption is not a panacea for information security problems. It must be used in concert with other technical and administrative measures, as described below. In particular, effective key management is crucial.

## Encryption Algorithms

The various techniques for encrypting messages, based on mathematical algorithms, vary widely in their degree of security. The choice of algorithms and the method of their development have, in fact, been among the most controversial issues in communications and computer security. (See ch. 6.) The various algorithms currently available differ along the following dimensions:

- *The mathematical sophistication* **and** *computational complexity of the algorithm itself.*—More complex algorithms may be (though not necessarily) harder for an adversary to decrypt or break.
- *Whether the algorithm is for a symmetric cipher or an asymmetric one.* —Symmetric ciphers use the same key for encryption and decryption, while asymmetric ciphers use different but related keys.
- *The length of the key used to encrypt and decrypt the* message.–Each algorithm uses a series of numbers known as a key that can change with each message, with each user, or according to a fixed schedule. Generally, for an algorithm of a given complexity, longer keys are more secure. One of the important factors in selecting keys is to make sure that they cannot be easily guessed (e.g., using a phone number) and that they are as random as possible (so that an adversary cannot determine a pattern linking all the keys if one is discovered).
- *Whether the algorithm is implemented in soft ware (programming) or hardware (built*

*into an integrated circuit* chip).-Hardware tends to be much faster than software, although less versatile and portable from one machine to another.

- *Whether the algorithm is* **open to** *public scrutiny. -Some* nongovernment experts argue that users have more confidence in an algorithm if it is publicly known and subject to testing. NSA and others, on the other hand, assert that the algorithm is one of three essential pieces of information an adversary must have to decrypt a message (along with the key and access to the message itself) and that secret algorithms are thus more secure.[2] A related argument is that if an algorithm is publicly known, standardized, and widely used, it becomes a more attractive target for cracking than algorithms that are seldom used. The Data Encryption Standard (DES, see below) is one of the few working algorithms that is open to public scrutiny. Most of the other privately developed and all of the NSA-developed algorithms currently in use have been kept secret.

DES is probably the most widely known modern encryption algorithm. (See app. C for background on its development.) Based on an algorithm developed by IBM, DES was issued as a Federal standard in 1977. Although publicly known and subject to scrutiny for more than 10 years, most experts are confident that it is secure from virtually any adversary except a foreign government. The level of security is gradually weakening, however, because of the decreasing cost of computer power and the possibility of using many computing devices in parallel to crack the algorithm.

DES has four approved modes of operation, specified in FIPS Publication 81 ("DES Modes of Operation, " Dec. 2, 1980). The modes vary in their characteristics and properties. The four modes are the electronic codebook (ECB), cipher block chaining (CBC), cipher feedback (CFB), and the output feedback (OFB) modes. (See app. C.) The CBC and CFB modes can be used for message authentication. The ECB mode, the simplest to understand, is illustrated in figure 13 and box B. One property of this mode, however, is that the same plaintext will always produce identical ciphertext for a given encryption key. This characteristic makes the ECB mode less desirable, especially for repetitive messages or messages with common content (e.g., routing headers or logon identifications) because a known plaintext cryptographic attack is more easily mounted, i.e., where both the encrypted and unencrypted text are available to the cryptanalyst.

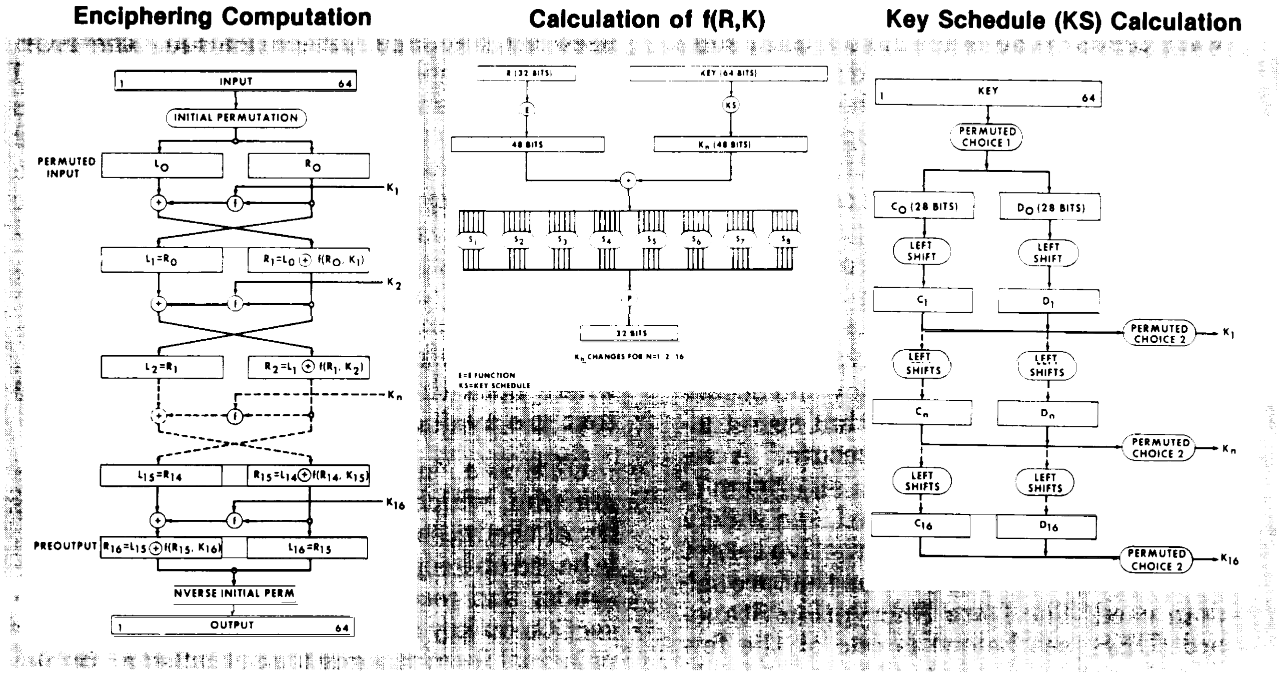
DES is a "private key" cryptographic algorithm, which means that the confidentiality of the message, under normal conditions, is based on keeping the key secret between the sender and receiver of the message. (See the section on key distribution, below.) The other principal form of algorithm is called a' 'public key" system, which uses two keys that are mathematically related—one that each user publishes and one that he keeps secret. Using a public key system, many people can encrypt messages sent to a particular correspondent (using his or her public key), but only that correspondent can decrypt messages because the decryption key is (in principle) kept secret. These algorithms are discussed in more detail below, and also in appendixes C and D.

The development of encryption algorithms has been a rather idiosyncratic, scattered process, and is likely to continue to be. The academic community of cryptographic researchers is a growing and active one, although its numbers are relatively small compared to some other scientific fields.[3] Only a handful of people in the United States outside NSA have attempted seriously to create, validate, and implement new high-quality encryption algorithms. Most algorithms currently in use can be traced to the work of a few individuals. Cryptographic research requires a high level of ability in specialized areas of mathematics and/or computer science. Different skills are required

[2] Ted Goeltz, "Why Not DES?" *Computers* ***and Security***, vol. 5, March 1986, pp. 24-27.

[3] R Rivest, Massachusetts Institute of Technology, personal communication with OTA staff, Feb. 4, 1987.

Figure 13.—DES Encryption in Electronic Codebook Mode



SOURCE: NBS FIPS Publication 74, Apr. 1, 1961, pp. 21-23.

to develop operational safeguards than for theoretical research.

Despite the relatively small size of the scientific community, cryptography has been a controversial science. For example, there have been controversies concerning attempts by NSA to control Federal research funding as well as the publication and patenting of private sector and academic results in cryptographic research during the past decade for reasons of national security.[4] NSA does not at present have the legislated authority to require prepublication review of independent, nongovernment research.

However, following the controversy sparked in part by secrecy orders imposed in 1978 on two patent applications for cryptographic inventions, NSA, in concert with some academic researchers, instituted a voluntary review for cryptography manuscripts.[5] Through this process, researchers may submit manuscripts to NSA prior to their publication, giving NSA the opportunity to request suppression of sensitive material. Although many researchers and research institutions take part in this voluntary process, others do not, considering it a threat to the free exchange of scientific ideas.[e]

The voluntary review service is similar to the one proposed by the Public Cryptography Study Group of the American Council on Education (ACE), which was assembled in 1980 at the request of NSA. The group accepted the premise that "some information contained in cryptology manuscripts could be inimical to the national security of the United States. " It recommended a voluntary rather than statutory solution to this problem.[7] However,

‘Tom **Ferguson**, "Private Locks, Public Keys, and Stats Secrets: New Problems in Guarding Information with Cryptography, " Harvard University Center for Information Policy **Re**search, Program on Information Resources Policy, April 1982.

sues. **Congress, House Committee** on **Government Operations**, "The Government's Classification of **Private** Ideas," Thirty-Fourth Report (House Report No. 96-1540), 96th Cong., 2d **sess.,** Dec. *22, 1980.*

[6] **See:** "Brief U.S. Suppression of Proof Stirs Anger, " ***The New York Times,*** Feb. 17, 1987, p. C3

"'Report of the Public Cryptography Study Group, " ***Academe,*** vol. 67, December 1981, pp. 372-382.

## Box B.—An Example of DES Encryption

The Electronic Codebook (ECB) mode is a basic, block, cryptographic method which transforms 64 bits of input to 64 bits of output as specified in FIPS PUB 46. The analogy to a codebook arises because the same plaintext block always produces the same ciphertext block for a given cryptographic key. Thus a list (or codebook) of plaintext blocks and corresponding ciphertext blocks theoretically could be constructed for any given key. In electronic implementation the codebook entries are calculated each time for the plaintext to be encrypted and, inversely, for the ciphertext to be decrypted.

Since each bit of an ECB output block is a complex function of all 64 bits of the input block and all 56 independent (non-parity) bits of the cryptographic key, a single bit error in either a ciphertext block or the non-parity key bits used for decryption will cause the decrypted plaintext block to have an average error rate of 50 percent. However, an error in one ECB ciphertext block will not affect the decryption of other blocks, i.e., there is no error extension between ECB blocks.

If block boundaries are lost between encryption and decryption (e.g., a bit slip), then synchronization between the encryption and decryption operations will be lost until correct block boundaries are reestablished. The results of all decryption operations will be incorrect until this occurs.

Since the ECB mode is a 64-bit block cipher, an ECB device must encrypt data in integral multiples of 64 bits. If a user has less than 64 to encrypt, then the least significant bits of the unused portion of the input data block must be padded, e.g., filled with random or pseudo-random bits, prior to ECB encryption. The corresponding decrypting device must then discard these padding bits after decryption of the chapter text block.

The same input block always produces the same output block under a fixed key in ECB mode. If this is undesirable in a particular application, the CBC, CFB or OFB modes should be used. An example of the ECB mode is given in table B1.

Table **B1 .—An Example of the Electronic Codebook (ECB) Mode**

The ECB mode in the encrypt state has been selected.

Cryptographic key = 0123456789abcdef

The plaintext is the ASCII code for “Now is the time for all. ” These seven-bit characters are written in hexadecimal notation (0, b7, b6,..,, b1).

| Time | Plaintext | DES input block | DES output block | Ciphertext |
|---|---|---|---|---|
| 1 | 4e6f772069732074 | 4e6f772069732074 | 3fa40e8a984d4815 | 3fa40e8a984d4815 |
| 2 | 68652074696 d6520 | 68652074696 d6520 | 6a271787ab8883f9 | 6a271787ab8883f9 |
| 3 | 666 f7220616c6c20 | 666 f7220616c6c20 | 893d51ec4b563b53 | 893d51ec4b563b53 |

The ECB mode in the decrypt state has been selected.

| Time | Ciphertext | DES input block | DES output block | Plaintext |
|---|---|---|---|---|
| 1 | 3fa40e8a984d4815 | 3fa40e8a984d4815 | 4e6f772069732074 | 4e6f 772069732074 |
| 2 | 6a271787ab8883f9 | 6a271787ab8883f9 | 68652074696 d6520 | 68652074696 d6520 |
| 3 | 893d51ec4b563b53 | 893d51ec4b563b53 | 666 f7220616c6c20 | 666f7220616c6c20 |

SOURCE: NBS, FIPS Publication 81, Dec. 2, 1980, pp. 12-13.

some researchers, including one member of the ACE group, felt that even voluntary restraints would affect the quality and direction of basic research in computer science, engineering, and mathematics.[8]

Currently, although some researchers feel that tensions between NSA and the research community have eased, others still consider that the prospect of NSA controls may discourage researchers, particularly academics, from pursuing problems related to cryptography. The issue continues to simmer, particularly because cryptography presents some

[8] “The Case Against Restraints on Nongovernmental Research in Cryptography: A Minority Report by Professor George 1. Davida, ” *Academe*, December 1981, pp. 379-382.

interesting mathematical problems. For example, a controversy recently arose when the U.S. Patent and Trademarks Office, at the request of the U.S. Army, placed a secrecy order—which the Army later requested be rescinded—on a patent application filed by Israel's Weizmann Institute. The patent application dealt with an area of mathematics called "zero-knowledge proof, " pioneered by Silvio Micali and colleagues at the Massachusetts Institute of Technology, that is considered to hold great promise for identification procedures ranging from credit card verification to military "friend or foe" recognition signals.[9]

Another controversy concerns NSA's decision not to recertify DES when it comes up for its 5-year review in 1987. NSA announced in 1986 that it will continue to endorse cryptographic products using DES until January 1, 1988, but not certify the DES algorithm or new DES products after that date, except for electronic funds transfer applications. However, DES equipment and products endorsed prior to January 1,1988, maybe sold and used after that date. In justifying this decision, NSA argues that DES has become too popular and widespread in use, and thus too attractive a target for adversaries seeking to crack it. Some observers have expressed concern that NSA decision implies that DES is no longer secure. However, NSA has stated that there are no known security problems or risks involved with the continued use of DES equipment.[10]

Instead of recertifying DES, NSA plans to provide and certify three classified algorithms. The new algorithms will use tamper-protected, integrated circuit modules directly in the products of qualified vendors. This decision officially affects only U.S. Government agencies and contractors, but it may discourage others from using DES except for electronic financial transactions.[11] The NSA plans affect safeguard vendors in two major ways: first, only selected U.S. vendors will be allowed to purchase the modules for incorporation into their products, and second, classified information (and the need to handle and protect such information) will be introduced into the product design process.[12] Also, some industry sources have expressed concern that the new secret algorithms are of uncertain reliability and will likely allow NSA itself to eavesdrop on their communications.[13]

In any case, industry has certain needs, most notably for easily exportable encryption devices and software-based encryption, that the new algorithms are unlikely to meet. Many experts consider software-based encryption less secure than hardware-based encryption, in part because the key might be exposed during encryption. Also, encryption using software is much slower than that using hardware or firmware devices. Nevertheless, some private sector users prefer software because it is inexpensive and compatible with their existing equipment and operations. For instance, reader surveys conducted by Security magazine in 1985 and 1986 found that about half of the respondents stated that they used encryption software.[14]

To date, there are no Federal software encryption standards and NSA has stated that it will not endorse software encryption products. Also, the new encryption modules are not

[9] The invention was made by Adi Shamir, Amos Fiat, and Uriel Feige. According to press accounts, the research had previously been cleared by NSA's voluntary review process, and NSA intervened to have the secrecy order reversed. *The New York Times,* Feb. 17, 1987: "A New Approach to Protecting Secrets Is Discovered, " p. Cl; and "Brief U.S. Suppression of Proof Stirs Anger, " p. C3.

[10] Harold E. Daniels, Jr., National Security Agency, letter N/2338 to DataPro Research Corp., Dec. 23, 1985.

[11] The Treasury Department has embarked on a major plan using DES to authenticate electronic funds transfers. For these applications, Treasury will certify the DES and DES-based equipment. See ch. 5.

[12] S. Lipner, Digital Equipment Corp., personal communication with OTA staff, Dec. 24, 1986. See ch. 5 for a description of vendor eligibility requirements.

[13] IEEE Subcommittee on Privacy, meeting at OTA, July 8, 1986.

[14] These data were reported in: Kerrigan Lyndon, "protecting the Corporate Computer, *Security World,* Oct. 1985, pp. 35-56; and Susan A. Whitehurst, "How Business Battles Computer Crime, " *Security,* October 1986, pp. 54-60. Of the 1985 survey respondents, 48 percent reported using data encryption software compared to only 19 percent reporting use of data encryption hardware. Of the 1986 respondents, 47 percent reported using encryption software; the percentage using encryption hardware was not reported.

exportable. NSA has not yet announced whether it will provide exportable modules for use by the private sector. Thus, the NSA decision not to recertify DES has cast doubt on the reliability of the algorithm without providing a replacement that can meet the full range of users' needs. Chapter 6 discusses Federal policy in more detail.

OTA's analysis suggests that there are certain kinds of algorithms not widely available that would substantially increase the range of applications for which encryption would be useful. These include algorithms that are very fast (require little processing time), secure enough to ensure confidentiality for relatively short periods (e.g., days or months for financial transactions, as opposed to years or decades for defense and intelligence information), and easily implemented in software, especially software for microcomputers. In addition, because of the widespread acceptance of DES for unclassified information, some experts argue that it would be fruitful to develop an improved version of that algorithm that would lengthen the key while using the same essential scheme. However, the commercial market for cryptographic safeguards is still new and small, and it has thus far been dominated by DES. Although a number of firms—mostly NSA contractors or spinoffs of these–are reportedly working on new encryption algorithms and products for the commercial market, " as of early 1987 public-key systems are the only area of encryption algorithm development in which substantial nongovernment research and development is evident. Developing a new algorithm may take anywhere from 5 to 20 person-years, so many firms—except, perhaps, large firms that ordinarily devote such substantial resources to long-term research and development—may hesitate to invest in a new cryptographic product for a market that, so far, has been shaky. "

## Message Authentication

An "authentic" message is one that it is not a replay of a previous message, has arrived exactly as it was sent (without errors or alterations), and comes from the stated source (not forged or falsified by an imposter or fraudulently altered by the recipient). [17] Encryption in itself does not automatically authenticate a message. It protects against passive eavesdropping automatically, but does not protect against some forms of active attack. [18] Encryption can be used to authenticate messages, however, and the DES algorithm is the most widely used cryptographic basis for message authentication.

As the use of electronic media for financial and business transactions has proliferated, message authentication techniques have evolved from simple pencil-and-paper calculations to sophisticated, dedicated hardware processors capable of handling hundreds of messages a minute. In general, the various techniques can be grouped together according to whether they are based on public or, at least in part, on secret knowledge.

Public techniques share a common weakness: they check against errors, but not against malicious modifications. Therefore, fraudulent messages might be accepted as genuine ones because they are accompanied by "proper" authentication parameters, based on information that is not secret. Using secret parameters, however, message authentication cannot be forged unless the secret parameters are compromised. A different secret parameter is usu-

' "S. Lipner, Digital Equipment Corp., personal communication with OTA staff. Dec. 24, 1986.

"'Peter Schweitzer and Whitfield Diffie, personal communications with OTA staff, June 2, 1986.

[17] For a thorough discussion of message authentication and the various techniques used to authenticate messages, see Davies & Price, *Security for Computer Net works: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfers*, Ch. 5, (New York, NY: J. Wiley, 1984). The descriptions of authentication techniques in this section follow Davies & Price closely.

[18] "Passive attack" is described as eavesdropping and "active attack" as the falsification of data and transactions through such means as: 1 ) alteration, deletion, or addition; 2) changing the apparent origin of the message; 3) changing the actual destination of the message; 4) altering the sequence of blocks of data or items in the message: 5) replaying previously transmitted or stored data to create a new false message; or 6) falsifying an acknowledgment for a genuine message. See Davies & Price, pp. 119-120,

ally required for each sender-receiver pair. The logistics for distributing this secret information to the correct parties is analogous to key distribution for encryption (see below).

If privacy as well as authentication is required, one scheme for encrypting and authenticating a message involves sequential use of DES with two different secret keys: one to calculate the authenticator (called the message authentication code or MAC) and one to encrypt the message. Even the use of a message authentication code and encryption do not safe guard against replay of messages or malice on the part of one of the corresponding parties, so various message sequence numbers, date and time stamps, and other features are usually incorporated into the text of the message. Box C discusses the use of message authentication in financial transactions. Figure 14 shows a data authentication code (synonymous with message authentication code) based on the DES algorithm.

### Box C.—Application of Message Authentication to Electronic Funds Transfer

Developments in the banking industry provide a good example of how important information should be safeguarded, both because of the large amounts of money involved and because of the early use of new safeguard technology by segments of this industry.[1] Roughly $668 billion per day was transferred over the FedWire and Clearing House Interbank Payment System (CHIPS) networks alone in 1984, representing a 48 percent increase over 1980. [Z] The fully-automated, online, FedWire system handled 49.5 million domestic transactions in 1986, with an average value of $2.5 million each, for a total of $124.4 trillion. In the same year, CHIPS handled $125 trillion in domestic and international payments for its member banks.[3]

During recent decades, the financial community has made increasing use of computer and communications systems to automate these fund transfers and other transactions. Typically, the computer systems of these financial institutions are interconnected with local and long distance public and private communications networks, over which the bankers have only limited control over potential fraud, theft, unauthorized monitoring, and other misuse. Their customers have an expectation of privacy and banks have the obligation to restrict details of financial transactions to those who need to know.

Wholesale and retail banking systems have somewhat different requirements for safeguards for funds transferred electronically. Wholesale bankers' requirements include message authentication and verification, as well as confidentiality of some communications; retail banking requirements additionally include authentication of individual automatic teller machines, confidentiality of customers' personal identification numbers, and communications security between the automatic tellers and the host computer. These needs are in sharp contrast with those of the defense-intelligence establishment, where confidentiality is the primary concern.

During the past decades, various technical methods have been adopted to reduce errors and to prevent criminal abuse relating to electronic fund transfers. Among these are parity checks, checksums, testwords, and pattern checks.[4] Some of these methods are widely used in various banking networks to verify that user inputs are correct and detect errors rather than protect against criminal activity.

‘Wholesale banking transactions are characterized by large dollar amounts per average transaction (e.g., about $3 million) and daily volumes of transactions that number in the thousands or tens of thousands. Retail banking transactions amounts might average $50 and number in the hundreds of thousands.

‘“Electronic Funds Transfer Systems Fraud, ” U.S. Department of Justice, Bureau of Justice Statistics, NCJ-1OO461, April 1986.

‘Information on FedWire and CHIPS from F. Young, Division of Federal Reserve Bank Operations, personal communication with OTA staff, Feb. 12, 1987.

‘For a brief description of testwords (or test keys) in banking transactions, see M. Blake Greenlee, “Requirements for Key Management Protocols in the Wholesale Financial Services Industry, ” *IEEE Communications Magazine,* vol. 23, No. 9, September 1985, One of the major, traditional drawbacks of encryption systems is that of key distribution. Each pair of communicating locations generally requires a matched, unique set of keys or codes, which have to be delivered in some way–usually by a trusted courier–to these users each time the keys are changed. (An alternative is to use a prearranged code book, which can be compromised, as has been well publicized in recent spy trials.) The key distribution problem rapidly becomes onerous as the number of communicators increases.[5] The discovery of the public-key algorithm, noted earlier, may alleviate some of the key distribution problems—for example, to distribute the secret keys to large networks of users.

In the late 1970s, the financial community was quick to realize the potential of the new cryptographic-based message authentication codes as a replacement for testwords. These codes allow major improvements in safeguards against both errors and intentional abuse, and facilitate the potential of future transaction growth. Thus, this community has pioneered industrywide technical standards both in the United States and worldwide.

The message authentication code is a cryptographically derived check sum based on processing the electronic fund transfer message with the DES algorithm (called the Data Encryption Algorithm in the financial services community) and a secret key.[6] The sender calculates the code and appends it to the message. The receiver calculates a code independently based on the same message, algorithm, and secret key. Most new bank authentication systems in use or in planning utilize DES to calculate the codes. If the code calculated by the receiver is identical to that sent with the message, then there is a high level of assurance that the originator is authentic and that the content of the received message is identical to that transmitted by the sender, with no alterations of any kind. Also, some banks authenticate and encrypt their wholesale electronic fund transfers whenever practical and in countries where encryption is legally permissible.[7]

[5] The number of pairs of separate keys needed in a network of "n" communicators, each pair of which requires unique keys, is n(n - 1 ) 2. Thus, a network of 5 communicators requires 10 separate pairs of keys, while a network of 100 communicators requires 4,950 pairs of keys. These numbers pale when considering that 10,000 banks send fund transfers worldwide, the largest of which have thousands of keying relationships.

[6] For a thorough discussion of the properties of message authentication techniques, see R.R. Jueneman, S.M. Matyas, and C'. H. Meyer. "Message Authentication, " *IEEE Communications Magazine,* vol. 23, No. 9, September 1985.

[7] C. Helsing, Bank of America, personal communication with OTA staff, December 1986.

## Public-Key Ciphers

A symmetric cipher is an encryption method using one key, known to both the sender and receiver of a message, that is used both to encrypt and decrypt the message. Obviously, the strength of a symmetric cipher depends on both parties keeping the key secret from others. With DES, for example, the algorithm is known, so revealing the encryption key permits the message to be read by any third party.

An asymmetric cipher is an encryption scheme using a pair of keys, one to encrypt and a second to decrypt a message.[19] A special class of asymmetric ciphers are public-key ciphers, in which the encrypting key need not be kept secret to ensure a private communication.[20] Rather, Party A can publicly announce his or her encrypting key, PKA, allowing anyone who wishes to communicate privately with him or her to use it to encrypt a message. Party A's decrypting key (SKA) is kept secret, so that only A or someone else who has obtained

[19] "See Davies & Price, ch. 8, for a more complete discussion of asymmetric and public-key ciphers. A discussion of the underlying principles of public-key ciphers, including examples of the RSA and knapsack algorithms, is given in Martin E. Hellman: "The Mathematics of Public-Key Cryptography. " *Scientific American,* vol. 241, No. 2, August 1979, pp. 146-157. A pictorial example of the RSA public-key method can be found in *Understanding Computers/COMPUTER SECURITY* (Alexandria, VA: Time-Life Books, 1986), pp. 112-117.

[20] The public-key concept was first proposed by Whitfield Diffie and Martin Hellman in their pathbreaking paper. "New Directions in Cryptography, " *IEEE Trans. Inform. Theory, IT-22, 6,* November 1976, pp. 644-654.

## Figure 14.—Federal Standard for Authentication

### The DAA Authentication Process

A cryptographic Data Authentication Algorithm (DAA) can protect against both accidental and intentional, but unauthorized, data modification.

A Data Authentication Code (DAC) is generated by applying the DAA to data as described in the following section. The DAC, which is a mathematical function of both the data and a cryptographic key, may then be stored or transmitted with the data. When the integrity of the data is to be verified, the DAC is generated on the current data and compared with the previously generated DAC. If the two values are equal, the integrity (i.e., authenticity) of the data is verified.

The DAA detects data modifications which occur between the initial generation of the DAC and the validation of the received DAC. It does not detect errors which occur before the DAC is originally generated.

### Generation of the DAC

The Data Authentication Algorithm (DAA) makes use of the Data Encryption Standard (DES) cryptographic algorithm specified in FIPS PUB 46. The DES algorithm transforms (or encrypts) 64-bit input vectors to 64-bit output vectors using a cryptographic key. Let D be any 64-bit input vector and assume a key has been selected. The 64-bit vector, O, which is the output of the DES algorithm when DES is applied to D, using the enciphering operation, is represented as follows.

O = e(D)

The data (e.g., record, file, message, or program) to be authenticated is grouped into contiguous 64-bit blocks: D1, D2 ..., Dn. If the number of data bits is not a multiple of 64, then the final input block will be a partial block of data, left justified, with zeros appended to form a full 64-bit block. The calculation of the DAC is given by the following equations where .+ represents the Exclusive-OR of two Vect ors.

01 = e(DI)
02 = e(D2 ı? 01)
03 = e(D3 ı@ 02)

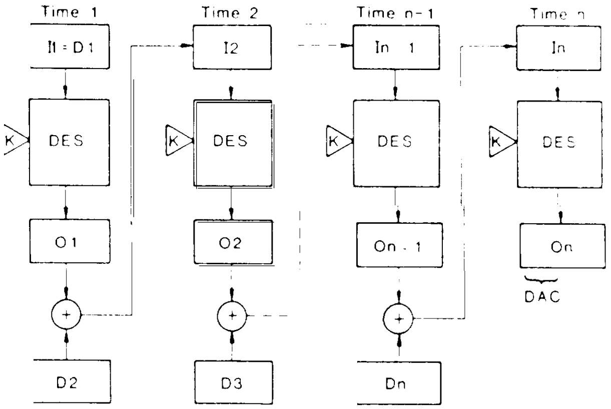
.

.

On = e(Dn ⊕ On-1)

The DAC is selected from On. Devices which implement the DAA shall be capable of selected the leftmost M bits of On as the DAC, where 16 < M < 64 and M is a multiple of 8. A block diagram of the DAC generation is given below, along with an example. The Cipher Block Chaining Mode (CBC) with Initialization Vector (IV) = O and the 64-bit Cipher Feedback Mode with IV = D1 and data equal to D2, D3, . . ., Dn (see FIPS PUB 81) both yield the required DAC calculation.

### Block Diagram of the DAC Generation



D = Data Block   O = Output Block   K = DES Key
= Input Block   DES = Data Encryption Standard   ⊕ = Exclusive-OR

### An Example of the DAA

Cryptographic Key = 0123456789abcdef

The text is the ASCII code for "7654321 Now is the time for." These 7-bit characters are written in hexadecimal notation 0,b7,b6, . . .,b1).

Text =
37363534333231204e6f77206873207468652074696d6520666f7220

| IME | PLAIN TEXT | DES INPUT BLOCK | DES OUTPUT BLOCK |
|---|---|---|---|
| 1 | 3736353433323120 | 3736353433323120 | 21fb193693a16c28 |
| 2 | 4e6f772069732074 | 6f946e16fad24c5c | 6c463f0cb7167a6f |
| 3 | 68652074696d6520 | 04231f78de7b1f4f | 956ee891e889d91e |
| 4 | 666f722000000000 | f3019ab1e889d91e | f1d30f6849312ca4 |

A 32-bit DAC = f1d30f68 is selected.

SOURCE: NBS FIPS Publication 113, May 30, 1985, pp. 3-6.

his or her decrypting key can easily convert messages encrypted with PKA back into plaintext.[21] Knowing the public encrypting key, even when the encrypted message is also available, does not make computing the secret decrypting key easy, so that in practice only the authorized holder of the secret key can read the encrypted message.

If the encrypting key is publicly known, however, a properly encrypted message can come from any source. There is no guarantee of its authenticity. It is thus crucial that the public encrypting key be authentic. An imposter could publish his or her own public key, PKI and pretend it came from A in order to read messages intended for A, which he or she could intercept and then read using his or her own SKI. Therefore, the strength of the public-key cipher rests on the authenticity of the public

[21] For A and B to have private two-way communication, two pairs of keys are required: the "public" encryption keys $PK_A$ and $PK_B$, and the secret decryption keys $SK_A$ and $SK_B$.

key. A variant of the system allows a sender to authenticate messages by "signing" them using an encrypting key, which (supposedly) is known only to him or her. This very strong means of authentication is discussed further in the section on digital signatures below.

The RSA public key is one patented system available for licensing from RSA Data Security, Inc. It permits the use of digital signatures to resolve disputes between a sender and receiver. The RSA system is based on the relative difficult y of finding two large prime numbers, given their product. The recipient of the message (and originator of the key pair) first randomly selects two large prime numbers, called p and q, which are kept secret. The recipient then chooses another (odd) integer e, which must pass a special mathematical test based on the values of p and q. The product, n, of p times q and the value of e are announced as the public encryption key. Even though their product is announced publicly, the prime factors *p* and q are not readily obtained from n. Therefore, revealing the product of *p* and *q* does not compromise the secret key, which is computed from the individual values of *p* and *q*.[22] Current implementations of the cipher use keys with 200 or more decimal digits in the published number N. A more complete description of the RSA system, including a discussion of its computational security, is given in appendix D.

Figure 15 shows a simple illustrative example of a public-key cipher based on the RSA algorithm. This simplified example is based on small prime numbers and decimal representations of the alphabet. It is important to bear in mind, however, that operational RSA systems use much larger primes.

The RSA system was invented at the Massachusetts Institute of Technology (MIT) in 1978 by Ronald Rivest, Adi Shamir, and Leonard Adelman. The three inventors formed RSA Data Security, Inc. in 1982 and obtained an exclusive license for their invention from MIT, which owns the patent. The firm has developed proprietary software packages implementing the RSA cipher on personal computer networks. These packages, being sold commercially, provide software-based communication safeguards, including message authentication, digital signatures, key management, and encryption. The firm also sells safeguards for data files and spread sheets transmitted between work stations, electronic mail networks, and locally stored files. The software will encrypt American Standard Code for Information Interchange (ASCII), binary, or other files on an IBM personal computers or compatible machines, and runs on an IBM PC/AT at an encryption rate of 3,500 bytes per second.

A number of public-key ciphers have been devised by other industry and academic researchers. Stanford University, for instance, holds four cryptographic patents, potentially covering a broad range of cryptographic and digital signature applications. Some of these patents have been licensed to various companies for use in their products.[2s]

## Digital Signatures

Encryption or message authentication alone can only safeguard a communication or transaction against the actions of third parties. They cannot fully protect one of the communicating parties from fraudulent actions by the other, such as forgery or repudiation of a message or transaction. Nor can they resolve contractual disputes between the two parties. Paper-based systems have long depended on letters of introduction for identification of the parties, signatures for authenticating a letter or contract, and sealed envelopes for privacy. The contractual value of paper documents hinges on the recognized legal validity of the signature and the laws against forgery.

[22] Certain special values of (p)(q) can be factored easily—when p and q are nearly equal, for instance. These special cases need to be avoided in selecting suitable keys. Furthermore, it is important to remember that this cipher system is no more secure than the secrecy of the private key.

[23] The companies include the Harris Corp., Northern Telecom, VISA, Public Key Systems, and Cylink. Lisa Kuuttila, Stanford Office of Technology Licensing. personal communication with OTA staff, Sept. 29, 1986.

## Figure 15.—Public-Key Ciphers

This example is adapted from one used in *Understanding Computers/Computer Security*, © 1986 Time-Life Books, Inc.

### A. Converting a message to numbers

Prescribed numeric values

| 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 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | • | , | . |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |

Converting the message

| S | E | L | L | • | 1 | 0 | 0 | • | S | H | A | R | E | S | • | O | F | • | A | B | C | D | • | I | N | D | U | S | T | R | I | E | S | • | J | O | H | N | • | S | M | I | T | H |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 19 | 5 | 12 | 12 | 37 | 28 | 27 | 27 | 37 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

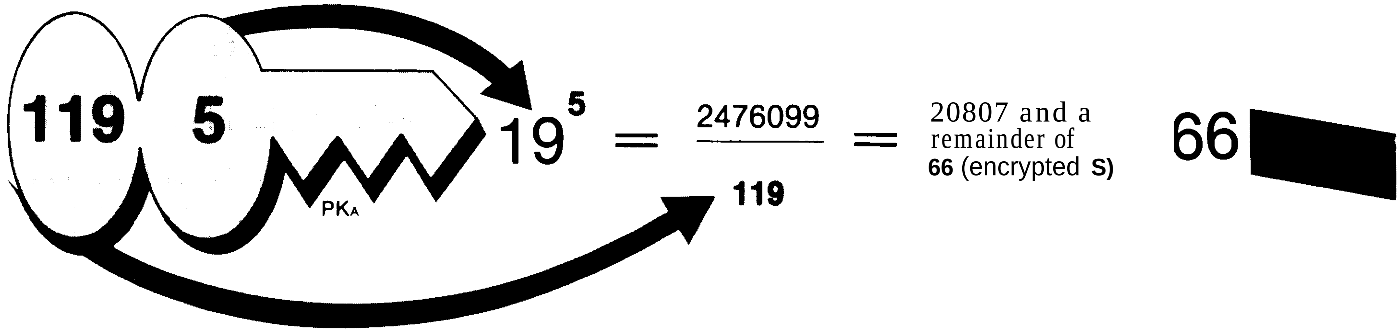
Before a message can be encrypted by the public-key method, it must be blocked and each block assigned a numerical value. Blocks may vary in size, from one character to several; and numerical values may be assigned in many ways, within constraints imposed by the system, In the example used here, each character is treated as a block, and a simple number-assigning system is used: A = 1, B = 2, C = 3, D = 4, and so on (tab/e *at top)*.

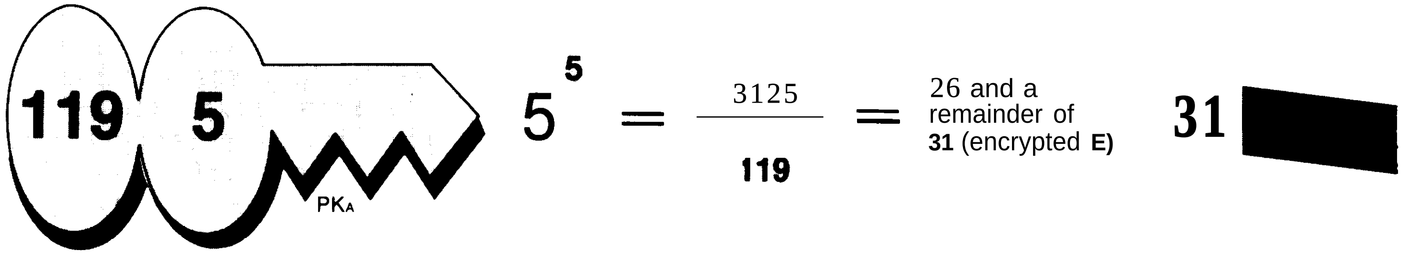
### C. The Arithmetic of locking and unlocking: the sender, user B, uses PKA to encrypt a message to user A.

The number 19, assigned to the letter S, is raised to the fifth power (multiplied by itself five times), as dictated by the second part of PKA (5).

The result of 19 raised to the fifth power—2,476,099—is divided by the first part of PKA, the number 119.

The division yields the number 20,807 and a remainder of 66. Only the remainder is important. It is the value of the encrypted letter S.


119
5
PKA
$19^5 = \frac{2476099}{119} =$
20807 and a remainder of 66 (encrypted S)
66


119
5
PKA
$5^5 = \frac{3125}{119} =$
26 and a remainder of 31 (encrypted E)
31

The next letter of the message, E, has the assigned value 5. Using the second part of PKA, this number is raised to the fifth power,

The result of multiplying 5 by itself five times—3,125—is divided by the other part of PKA 119.

The division yields the number 26 and a remainder of 31. Again, only the remainder is significant. it is the value of the encrypted letter E.

## B. Creating user A's keys.

1, Each user has a public and a private key, and each key has two parts To create user A's keys, two prime numbers, customarily designated P and Q, are generated by an operator at a central computer or key generation center (To quallfy, a prime number must pass a special mathematical test ) Here. P is 7, Q is 17.

2, In this slmpllfled example, the two primes are multiplied, and the result—N—will be the first part of both keys, N is 119

3. Next, an odd number is chosen, in this case, 5. (This number—designated E—must also pass a special mathematical text.) It forms the second part of the publlc key. PKA.

4. To create the second part of the private key, the numbers are multlpl!ed P minus 1 (6, In this case) times Q minus 1 (16) times E minus 1 (4) The result is 384

5, Next, 1 is added to the result of the previous step, yleldlng 385

6. The sum is divided by E (5). The result of the division, 77 (designated D), is the second part of SKA

*1* P = *7, Q = 17*

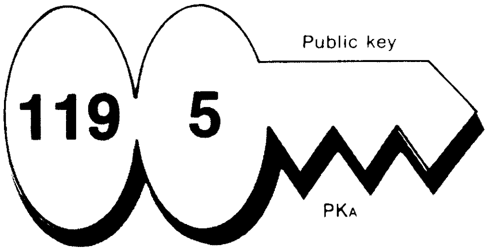
*2 7* x 17 = 119 = N

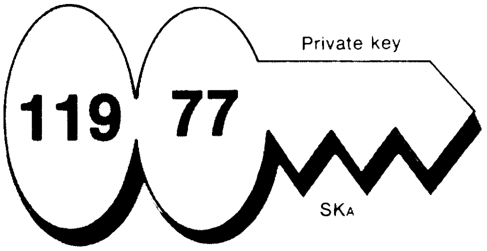
3 E = 5

4 6 X 16 X 4 = 384

5 384 + 1 = 385

6 385 ÷ 5 = 77 = D





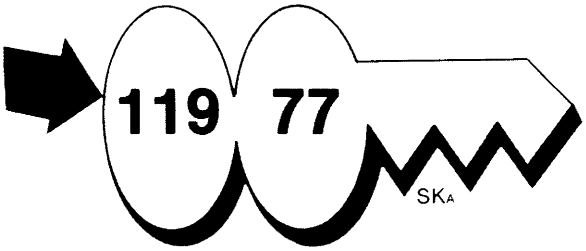
At the end of the procedure user A has a public key (119 5) and a private key (119 77) In reality, these numbers would be many digits long.

## D. The recipient, user A, uses his private key, SKA, to decrypt the message.

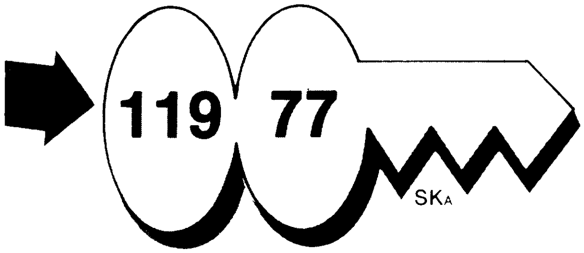
Decryptlon, using SKA, follows the same steps First, 66—the encrypted S— is raised to the 77th power, as dictated by the second part of the key, SKA.

The result of the previous step is divided by 119, the first part of SKA, which is identical to the first part of user A's public key.

The remainder resultlng from the divislon is 19—the original number assigned to the letter S. Thus, the decryption of the first one-letter block of the message is complete



$66^{77} = \dfrac{1237...}{119} =$ 1069 . . . and a remainder of **19** (numerical equivalent of) S



$31^{77} = \dfrac{6836\ ...}{119}$ - 5745 . . . and a remainder of **5** (numerical equivalent of) E

The number 31 —the encrypted letter E—Is raised to the 77th power, as dictated by the second part SKA

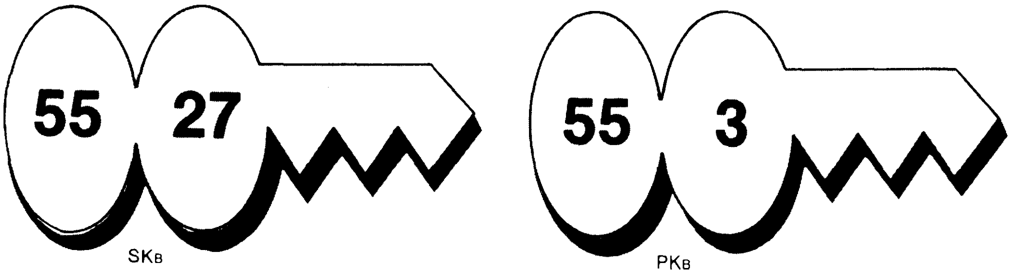
The result of multiplying 31 by itself 77 times is divided by 119. the other part of the private key SKA

The remainder from the dvision is 5—the orlglnal value assigned to the letter E Each letter block will be decrypted in the same way,

SOURCE Adapted from *Computer Security* (Alexandria, VA Time-Life Books, 1986} pp 112-115

### Figure 16.—Digital Signatures Using a Public-Key Cipher

This example uses the same key pair (PKA, SKA) generated for user A In figure 15. In this example, the sender (user B) uses his private key (SKB) to “sign” a message intended for user A and then “seals'” it by encrypting, the message with user A’s public key (PKA).



User B’s private key

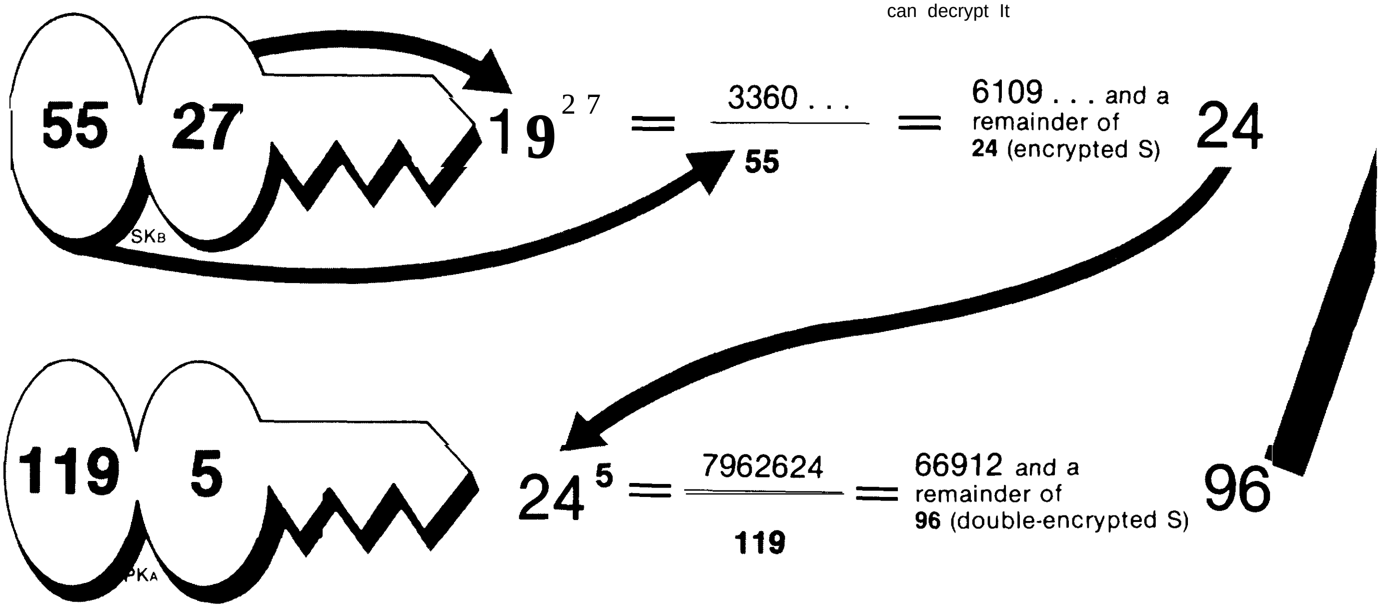
User B’s public key.

When user A receives the signed and sealed message, he uses hls SKA to unseal the message and the sender’s PKB to unsign it,

To begin the encryption technique called signing, the value of the letter S (l9)—Is raised ‘to the 27th power, as dictated by the second part of SKB.

The result of raising 19 to the 27th power IS divided by 55, the first part of SKB.

The divis!on yields a very large number, which is disregarded, and a remainder of 24. This completes the signing process for the letter S; only user B’s public key PKB can decrypt It


55
27
SKB
$19^{27} = \frac{3360\ldots}{55} =$
6109 . . . and a remainder of 24 (encrypted S)
24
119
5
PKA
$24^{5} = \frac{7962624}{119} =$
66912 and a remainder of 96 (double-encrypted S)
96

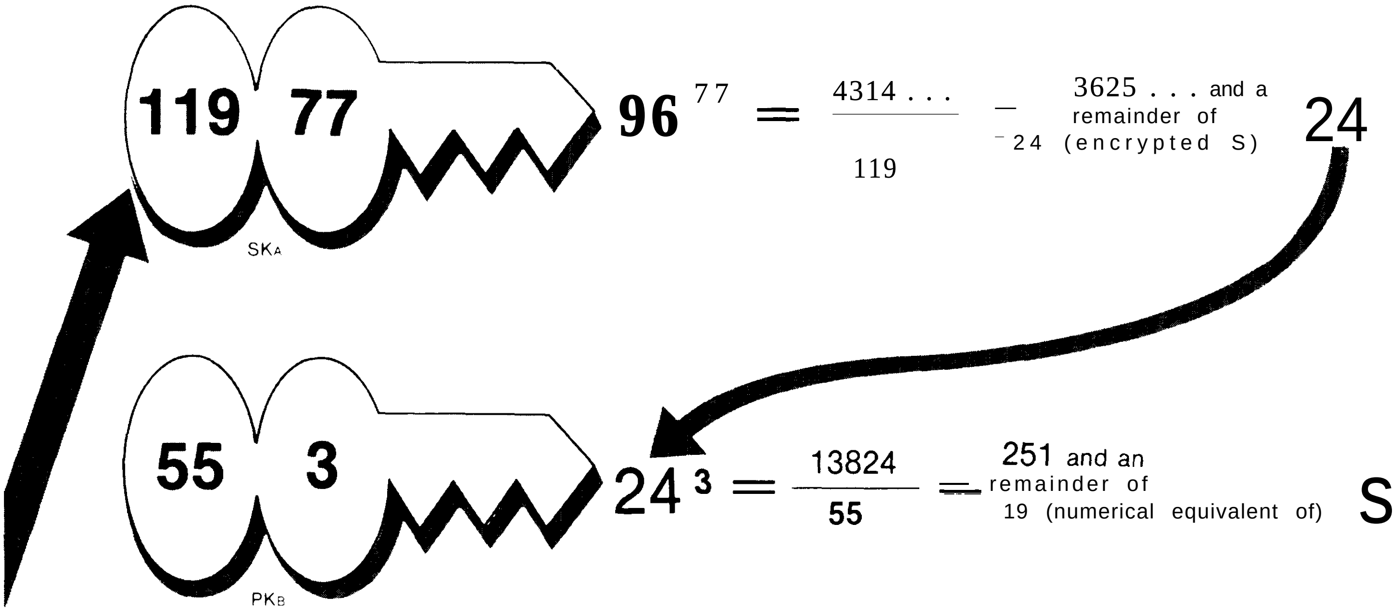
To seal the message for secrecy, the result of the first encryption, 24 in this case, is raised to the fifth power, as dictated by the second part of the receiver’s public key, PKA,

The result of raising 24 to the fifth power is divided by 119, the other part of PKA,

The division yields a number (disregarded) and a remainder of 96-the twice-encrypted S. It will be sent when the rest of the message has undergone the same double encryption, To decrypt a .slgned-and-sealed message, user A raises the number 96—the double-encrypted S—to the 77th power, as dictated by one part of hls private key, SKA

The result of the prevtous step IS divided by 119, the other part of SKA,

The division yields a very large number (disregarded) and a remainder of 24—the cipher imposed on the letter S by the sender's private key, SKB.


119
77
SKA
$96^{77} = \frac{4314\ldots}{119}$
— 3625 . . . and a remainder of
24 (encrypted S)
24
55
3
PKB
$24^{3} = \frac{13824}{55}$
= 251 and an remainder of
19 (numerical equivalent of)
S

To decrypt this digital signature, the number 24 IS raised to the third power, as dictated by one part of the sender's public key, PKB

The result of raising 24 to the third power IS divided by 55, as determined by the other part of PKB

The division yields a number (disregarded) and a remainder of 19—the numerical equivalent assigned to the letter S by the system, Performing the same steps on the rest of the transmission reveals the plaintext,

SOURCE Adapted from Computer *Security* (Alexandra, VA Time.Life Books, 1986), pp 116.117

Equivalent functions for electronic documents can be provided by using an asymmetric cipher, such as the RSA cipher, to create a digital signature for a document.[24] This can both authenticate their contents and also prove who sent them because only one party is presumed to know the secret information used to create the signature. If privacy is required, encryption can be used in addition to the digital signature. However, the "proof" of the signature hinges on the presumption that only one party knows the secret signing key. If this secret information is compromised, then the proof fails.

The equivalent of a letter of introduction is still necessary to verify that the correct public key was used to check the digital signature—an adversary might try to spoof the signature system by substituting his or her own public key and signature for the real author ’s. This letter of introduction could be accomplished by several means. The system offered by RSA Data Security, Inc., provides "signed key server certificates" by attaching the corporation's own digital signature to its customers' public keys. Thus, customers can attach their certified public keys to the messages they sign. Note that although a public-key cipher system is used to set up the digital signature system, the actual text of the message can be sent in plaintext, if desired, or it can be encrypted using DES or the public-key cipher.[25]

Figure 16 continues the simplified example in figure 15 to illustrate the digital signature technique.

[24] Other public-key ciphers using different one-way functions could provide the mechanism for a form of digital signature; however, none are commercially available at present. Also, it is possible to use a symmetric cipher such as DES in an asymmetric fashion—at least two signature functions of this type have been described-but these functions are more inconvenient to use than the RSA method and require more administrative effort. See Davies & Price, ch. 9, for a general treatment of digital signatures and alternative methods.

[25] For example, if the author wishes to keep the text of the message private, so that only the intended recipient can read it, he or she can encrypt the signed message, using the recipient's public key. Then, the recipient first uses his or her own secret key to decrypt the signed message and then uses the sender's public key to check the signature. In practice, the RSA digital signature system is used to transmit a DES key for use in encrypting the text of a message because DES can be implemented in hardware and is much faster than using the RSA algorithm to encrypt text in software.

## NEW TECHNOLOGIES FOR PRIVATE AND SECURE TRANSACTIONS

The public-key and digital signature systems described above have important uses for key exchange and management, for authenticating messages and transactions, and for permitting enforceable "electronic contracts" to be made, including electronic purchase orders and other routine business transactions. Digital signatures might also be used in equally secure transaction systems that preserve the privacy of individuals. This would be accomplished by permitting transactions to be made pseudonymously (using digital signatures, which would correspond to digital pseudonyms that could differ for each type of transaction) .2’ That is, transactions could be made without revealing the identity of the individual, yet at the same time making certain that each transaction is completed accurately and properly.

‘('See, for example, David Chaum, "Security Without Identification: Transactions Systems To Make Big Brother Obsolete, " *Communications ofthe ACM, vol. 28, No.* 10, October 1985.

Digital signatures could prevent authorities from cross-matching data from different types of transactions or using computer profiling to identify individuals who have a particular pattern of transactions. Database matching is a technique that uses a computer to compare two or more databases to identify individuals in common (e.g., Federal employees who have defaulted on student loans). Computer profiling uses inductive logic to determine indicators of characteristics and/or behavior patterns that are related to the occurrence of certain behavior (e.g., developing a set of personal and transactional criteria that make up a profile of a drug courier).[27]

Public-key systems make it possible to establish a new type of transaction system that protects individual privacy while maintaining the security of transactions made by individuals and organizations. This new system would cre ate a security relationship between individuals and organizations in which an organization and the individuals it serves cooperatively provide mutual protection, allowing the parties to protect their own interests.

For example, instead of individuals using the same identification (e.g., Social Security numbers, which are now commonly used on drivers' licenses, insurance forms, employment records, tax and banking records, etc.), they would use a different account number or digital pseudonym with each organization they do business with. Individuals could create their pseudonyms, rather than have them issued by a central authority. A one-time pseudonym might even be created for certain types of transactions, such as retail purchases. Although individuals would be able to authenticate ownership of their pseudonyms and would be accountable for their use, the pseudonyms could not be traced by computer database matching.[28] On the other hand, the use of numerous digital pseudonyms might make it more complicated for individuals to check or review all their records.[29]

A second difference is the ownership of the "tokens" used to make transactions. Currently, individuals are issued credentials, such as paper documents or magnetic stripe cards, to use in transactions with organizations. Moreover, the information contained on the electronic credentials is usually not directly reviewable or modifiable by the individual who uses it. In the scheme described above, individuals would own the transaction token and would control the information on it.

This system illustrates how technological de velopments and organizational changes can be used to mitigate potential erosions of privacy that could result from the widespread use of multi-purpose smart cards and computer profiling. However, while the technology and organizational infrastructures for the latter, at least, are already fairly well developed, the practical development of privacy systems is just beginning.[30]

[27] For a further discussion of the implications of computer database matching and profiling, see the Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy,* OTA-CIT-296 (Washington, DC: U.S. Government Printing Office, June 1986).

[28] A formal description of a "credential mechanism for pseudonyms is given in David Chaum and Jan-Hendrik Evertse, "A Secure and Privacy-Protecting Protocol for Transmitting Personal Information Between Organizations, *Advances in Cryptology: Proceedings of Crypto 86,* A.M. Odlyzko (cd.), Springer-Verlag Lecture Notes in Computer Science, forthcoming, summer 1987.

[29] Chaum suggests using a card computer to manage this complexity while maintaining a convenient user interface. Personal communication with OTA staff, February 1987.

[30] The Center for Mathematics and Computer Science in Amsterdam has recently demonstrated a payment system and is working with European groups to develop trial systems. David Chaum, personal communication with OTA staff, February 1987.

# KEY MANAGEMENT

Key management is fundamental and crucial to encryption-based communication and information safeguards. As an analogy, one might say that:

> The safety of valuables in a locked box depends as much or more on the care with which the keys are treated than on the quality of the lock. It is useless to lock up valuables if the

key is left lying around. The key may be stolen, or worse, it may be secretly duplicated and used at the thief's pleasure.[31]

Key management encompasses the generation of encrypting and decrypting keys as well as their storage, distribution, cataloging, and eventual destruction. These functions may be handled centrally, distributed among users, or by some combination of central and local key management. Also, key distribution can be handled through various techniques: by using couriers to distribute data-encrypting keys or master (key-encrypting) keys, for instance, or by distributing keys electronically using a public-key cipher. The relative merits of each mode of key management are subject to some debate.

For example, some technical experts, including those at NSA, argue that centralized key generation and distribution, perhaps performed electronically, efficiently ensures interoperability among different users and that relatively unsophisticated users do not inadvertently use any weak keys that may exist. NSA has stated that, for reasons of security and interoperability, it plans to control key generation for the new STU-III secure telephones (see ch. 5), including those purchased by private sector users. It is also likely that NSA will control key generation for equipment using its new encryption modules.

Some critics of this plan are concerned that NSA might be required—by secret court order, perhaps—to selectively retain certain users' keys in order to monitor their communications. Others express concerns that keying material may be exposed to potentially unreliable employees of NSA contractors. At the very least, the prospect of centralized NSA key generation has generated some public controversy.

On the other hand, the National Bureau of Standards (NBS) operates on the assumption that each user organization should generate its own keys and manage its own key distribution center. In the United States, Federal standards for protecting unclassified information in Government computer systems have been developed by NBS[32] which has also worked cooperatively with private organizations such as the American Bankers Association (ABA) and the American National Standards Institute (ANSI). Additionally, ABA and ANSI have developed voluntary standards related to cryptography for data privacy and integrity, including key management. The International Organization for Standardization (IS0) has been developing international standards, often based on those of NBS and/or ANSI.[33] Standards of these types are intended to specify performance requirements (accountability for keys, assignment of liability) and interoperability requirements for communications among users.

According to some experts, it is technically possible to handle centralized key distribution so that the key-generating center cannot read users' messages. If this were done, it would provide efficient and authenticated key distribution without the potential for misuse by a centralized authority. However, whether NSA plans to use these techniques has not been made public.

In any event, a key distribution center of some sort is the most prominent feature of key management for multi-user applications. Such a center is needed to establish users' identities and supply them with the keys to be used for communications–usually, with "seed" keys used to establish individual session keys.

[31] This analogy is from Lee Neuwirth: "A Comparison of Four Key Distribution Methods, " *Telecommunications* (Technical Note), July 1986, pp. 110-115. For a detailed discussion of key distribution and key management schemes, also see ch. 6 of Davies & Price.

[32] See, for example, Federal Information Processing Standards (FIPS) Publications FIPS PUB 81, 74, and 113 published by NBS.

[33] D. Branstad, Institute for Computer Science and Technology, National Bureau of Standards. Information about NBS and standards development from personal communication with OTA staff, Aug. 6, 1986. For a general discussion of security standards based on cryptography, see: Dennis K. Branstad and Miles E. Smid, "Integrity and Security Standards Based on Cryptography, " *Computers and Security, vol.* 1, 1982, pp. 255-260.

Even in a public-key system, the initial secret keys must be computed or distributed. NBS has developed a key notarization system that provides for authenticated distributed keys and other key management functions.[34] NBS had initiated a process for developing standards for public-key systems[35] but is no longer pursuing this activity.

The traditional means of key distribution—through couriers—is a time-consuming and expensive process that places the integrity of the keys, hence the security of the cipher system, in the hands of the courier(s). Courier-based key distribution is especially awkward when keys need to be changed frequently. Recently, public-key systems for key distribution have been made available allowing encryption keys (e.g., DES keys) to be securely transmitted over public networks—between personal computers over the public-switched telephone network, for example. There continue to be new developments in public-key cryptography research.[36]

To date, the best-known commercial offering of a public-key system to secure key distribution (or other electronic mail or data transfers) is by RSA Data Security, Inc. Other public-key systems have been developed, some earlier than RSA, but to date none have yet gained wide commercial acceptance. Although RSA initially attempted to implement its algorithm in hardware, their first successful commercial offerings, introduced in 1986, use software encryption. The Lotus Development Corp., one of the largest independent software companies, has licensed the RSA patent for use in future products. RSA Data Security has also licensed the patent to numerous large and small firms and to universities engaged in research, as well as to some Federal agencies, including the U.S. Navy and the Department of Labor.[37] A new hardware implementation of several public-key ciphers (including RSA and the SEEK cipher) was offered commercially in 1986. The chip, developed by Cylink, Inc., will be used in Cylink's own data encryption products and is available to other vendors who wish to use it.[38]

## VOICE AND DATA COMMUNICATIONS ENCRYPTION DEVICES

A number of commercial products, in the form of hardware devices or software packages, are available to encrypt voice and data communications. Software-based encryption is slower than hardware encryption and many security experts consider it to be relatively insecure (because, among other reasons, the encryption keys may be 'exposed' in the computer operations). Still, some commercial users prefer software encryption because it is relatively inexpensive, does not require additional hardware to be integrated into their operations, and is compatible with their existing equipment and operations. However, this section will deal only with hardware products, in large part because only hardware products have been certified for Government use.

Since 1977, NBS has validated 28 different hardware implementations of the DES algorithm (in semiconductor chips or firmware), but NBS does not validate vendors' software implementations of the algorithm. In 1982, the General Services Administration (GSA) issued Federal Standard 1027, "Telecommunications: Interoperability and Security Requirements for Use of the DES, in the Physical Layer of Data Communications. " At present, equipment purchased by Federal agencies to protect unclassified information must meet FS 1027 specifications; vendors may submit products built using validated DES chips or firmware to NSA for FS 1027 certification. NSA has a DES endorsement program to certify products for government use, but plans to dis-

[34] Branstad and Smid, op. cit., p. 258.

[35] Ibid., p. 259.

[36] S. Goldwasser, S. Micali, and R. Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen Message Attack, MIT Laboratory for Computer Science, Rev. Apr. 23, 1986,

[37] Letter to OTA staff from Jim Bidzos, RSA Data Security, Inc., Feb. 19, 1987.

[38] See '* Cypher Chip Makes Key Distribution A Snap, " *Electronics*, Aug. 7, 1986, pp. 30-31.

continue this program on January 1, 1988. As stated earlier in this chapter, DES products endorsed prior to this date can be used indefinitely .39

Hardware encryption products use special semiconductor or firmware devices to implement one or more encryption algorithms. Online encryption (in which data is encrypted as it is transmitted and decrypted as it is received, as opposed to off-line encryption in which plaintext is first encrypted and then stored for later transmission) can be implemented in two ways. In the first method, called end-to-end encryption, synchronized encryption/decryption devices at the source and destination operate so that the transmitted information is encrypted and remains in its encrypted form throughout the entire communications path. In the second method, called link encryption, the transmitted information is also encrypted at the source, and decrypted and then reencrypted at each intermediate communications node between the source and the ultimate destination. Thus, the information is encrypted, decrypted, and reencrypted as it traverses each link along its communications path.

By late 1986, the market research firm DataPro listed about 30 vendors that were marketing commercial encryption equipment, using the DES and/or proprietary algorithms, and operating at low or high data rates (depending on the product and vendor, encryption data rates can range from about 100 bits per second up to 7 million bits per second). These vendors offer 40 or more commercial products or families of products, mostly for data encryption, although a few vendors offer products for voice encryption. Some vendors specialize in encryption-only products, while others are data communications service (turnkey) providers offering encryption products complementing the rest of their product line. Published prices range from $500 to several thousand dollars per unit, depending on data rate and other features.

[39] Harold E. Daniels, Jr., Deputy Director for Information Security, NSA, enclosure 3, page 4 in letter S-0033-87 to OTA, Feb. 12. 1987.

# PERSONAL IDENTIFICATION AND USER VERIFICATION

## Background

User verification measures aim to ensure that those who gain access to a computer or network are authorized to use that computer or network. Personal identification techniques are used to strengthen user verification by increasing the assurance the person is actually the authorized user.[40]

User verification techniques typically employ a combination of (usually two) criteria, such as something an individual has, knows, or is. Until recently, the "has" has tended to be a coded card or token, which could be lost, stolen, or given away and used by an unauthorized individual; the "knows" a memorized password or personal identification number, which could be forgotten, stolen, or divulged to another; and the "is" a photo badge or signature, which could be forged. Cards and tokens also face the problem of counterfeiting.

Now, new technologies and microelectronics, which are harder to counterfeit, are emerging to overcome the shortcomings of the earlier user verification methods. At the same time, these new techniques are merging the has, knows, or is criteria, so that one, two, or all three of these can be used as the situation dictates. Microelectronics can make the new user verification methods compact and portable. Electronic smart cards, for example, now carry prerecorded, usually encrypted, access control information that must be compared with data that the proper authorized user is required to provide, such as a memorized personal identification number or biometric data like a fingerprint or retinal scan.

[40] Purists will note that the "personal identification' systems in common use do not actually identify a person, rather they recognize a user based on pm-enrolled characteristics. The term "identification" is commonly used in the industry, however.

Merging the criteria serves to authenticate the individual to his or her card or token and only then to the protected computer or network. This can increase security since, for example, one's biometric characteristics cannot easily be given away, lost, or stolen. Moreover, biometrics permit automation of the personal identification/user verification process.

While false acceptances and false rejections can occur with any identification method, each technique has its own range of capabilities and attributes: accuracy, reliability, throughput rate, user acceptance, and cost. As with other security technologies, selecting an appropriate system often involves trade-offs. For one thing, elaborate, very accurate technical safeguards are ineffective if users resist them or if they impede business functions. The cost and perceived intrusiveness of a retina scanner might be acceptable in a high-security defense facility, for example, but a relatively low-security site like a college cafeteria might sacrifice high reliability for the lower cost, higher throughput rate, and higher user acceptance of a hand geometry reader. In banking, where user acceptance is extremely important, signature dynamics might be the technology of choice. In retail sales, a high throughput rate is extremely important and slower devices would not be acceptable.

Access control technologies will evolve for niche markets. Successful commercial products for the defense and civilian niches will look very different. As of early 1987, there were no specific performance standards for most of these user verification technologies, but it is likely that these will be developed. One incentive for the development of access control standards, at least for the Government market, is the access control objectives specified in the so-called "Orange Book. "[41] The development of user verification technologies, however, is being driven significantly by commercial needs. In the area of biometrics, vendors have formed an industry association. The International Biometrics Association is beginning to address industry issues including performance and interface standards and testing and has a standing committee on standards and technical support.

In short, the new access control technologies are moving toward the ideal of absolute personal accountability for users by irrefutably tying access and transactions to a particular individual. Some enthusiasts and industry experts foresee great and pervasive applications for some of the access control technologies, even to their evolution into nonsecurity applications, such as multiple-application smart cards (see above). However, a given set of access control technologies cannot, in themselves, fix security problems "once and for all. " Changes in information and communication system infrastructures can eventually undermine previously effective safeguards. Therefore, safeguards have a life cycle. It is the combination of attributes, of the safeguard technique, and of the system it seeks to protect that determines the useful life of a safeguard.

## Conventional Access Controls

### Password-Based Access Controls

The earliest and most common forms of user verification are the password or password-based access controls. The problem is that passwords can be stolen, compromised, or intentionally disclosed to unauthorized parties. In addition, trivial passwords can easily be guessed and even nontrivial ones can be broken by repeated attack.[42] Once stolen or com-

[41] Department of Defense Trusted Computer System Evaluation Criteria. Department of Defense Standard DOD 5200.28 - STD, December 1985. Section 7.4 of the Orange Book specifies that individual accountability must be ensured whenever classified or sensitive information is processed. This objective encompasses the use of user verification, access control software, and audit trails.

[42] Common password misuses include sharing one's password with other users (including friends or co-workers), writing down the "secret series of letters or numbers for reference and storing it in an unsecure place (examples of this abound, including writing passwords or identification numbers on the terminals themselves or on desk blotters, calendars, etc., or storing them in wallets or desk drawers), and permitting others to see the log-on/authorization code being keyed in at the terminal. Some password schemes allow users to select their own passwords; while this increases the secrecy of the passwords because they are known only by the users, trivial password choices can reduce security if the passwords are easy to guess (examples of trivial passwords would be a pet name, a birthdate, or license plate number).

promised, passwords can be disclosed widely or even posted on electronic bulletin boards, resulting in broad exposure of a system to unauthorized access. If operating system security is poor, one user who unilaterally compromises his or her own password can compromise the whole system. An even more serious weakness is that, because there may be no tangible evidence of a security breach, a compromised password can be misused over and over until either the password is routinely changed, its compromise is discovered, or other events occur (e.g., data are lost or fraudulently changed). To avoid some of these problems, many modern systems use special procedures to frustrate repeated incorrect attempts to log on.

Until the last decade or so all access points to computer systems could be physically identified, which simplified the system administrator's job of controlling access from them. In addition, users could be easily defined and their terminals had limited capabilities. A network of this type is shown in figure 17.

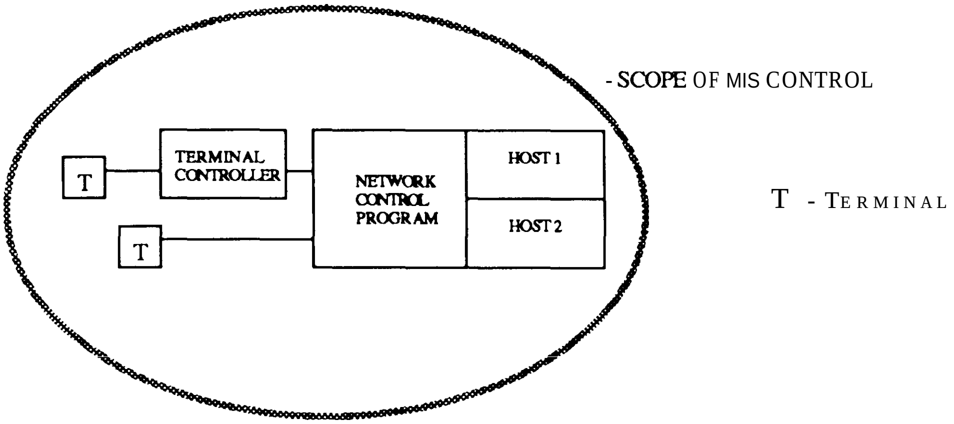
Now, new network configurations have emerged, characterized by personal computers linked to local area networks and connected by fixed and/or public switched telephone lines, as shown in figure 18. Users can readily extend the network by connecting modems to personal computers for pass-through access.

As a result, it is no longer possible to identify all access points. Communication nodes are no longer controlled exclusively by the organization when, for example, authorized users need to gain access from remote locations. While pass-through techniques facilitate access by authorized users, they can also be misused. For example, under some circumstances they can be used to defeat even such security techniques as call-back modems. With the increased number of network access points, the intrinsic weaknesses of the password further exacerbate the system's vulnerabilities.

### Token-Based Access Controls

Network evolution, therefore, has made user identification and authentication even more critical. Some of the new access-control technologies can see through the communications network to the end user to authenticate him or her—at least as the "holder' of the proper

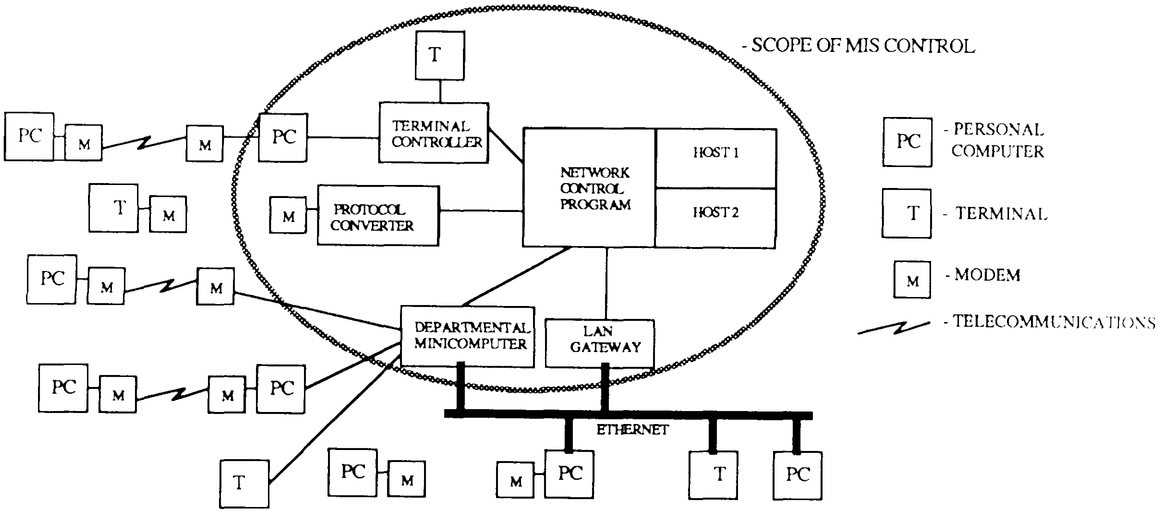
**Figure 17.—A Description of the Past Network Environment**



In the past network environment, control of all network resources resided with systems professionals. Typically, fixed-function terminals were direct-connected to the mainframe or a terminal controller. The communications parameters were specified through tables in the network control program (NCP), also under the direction of the systems group. As a result, the network was totally under the custodianship of systems professionals.

SOURCE Ernst & Whtnney, prepared under contract to OTA, November 1986

Figure 18.—A Description of the Current/Future Network Environment



In the current/future network environment, systems professionals still control direct connection to the mainframe, Through the network control program (NCP), they maintain the communications parameters that control the access through the devices directly connected to the mainframe. However, the nature of these devices is changing dramatically. Instead of fixed-function terminals, they now consist of departmental minicomputers, local area network (LAN) gateways, and personal computers, All of these devices have the capability to expand the network beyond the scope of mainframe control. This environment invalidates many of the premises upon which conventional access control mechanisms, such as passwords and call-back modems, were based.

SOURCE Ernst & Whinney prepared under contract to OTA, November 1986

token—regardless of his or her physical location. Within the limitations of current technology, token-based systems are best used in combination with a memorized password or personal identification number identifying the user to the token.

In contrast to the password, token-based systems offer significantly greater resistance to a number of threats against the password system. Many token-based systems are commercially available. By December 1986, two of these had been evaluated by NSA's National Computer Security Center (NCSC) and approved for use with the access control software packages on NCSC's Evaluated Products List. (See ch. 5 for a discussion of NSA's programs.)

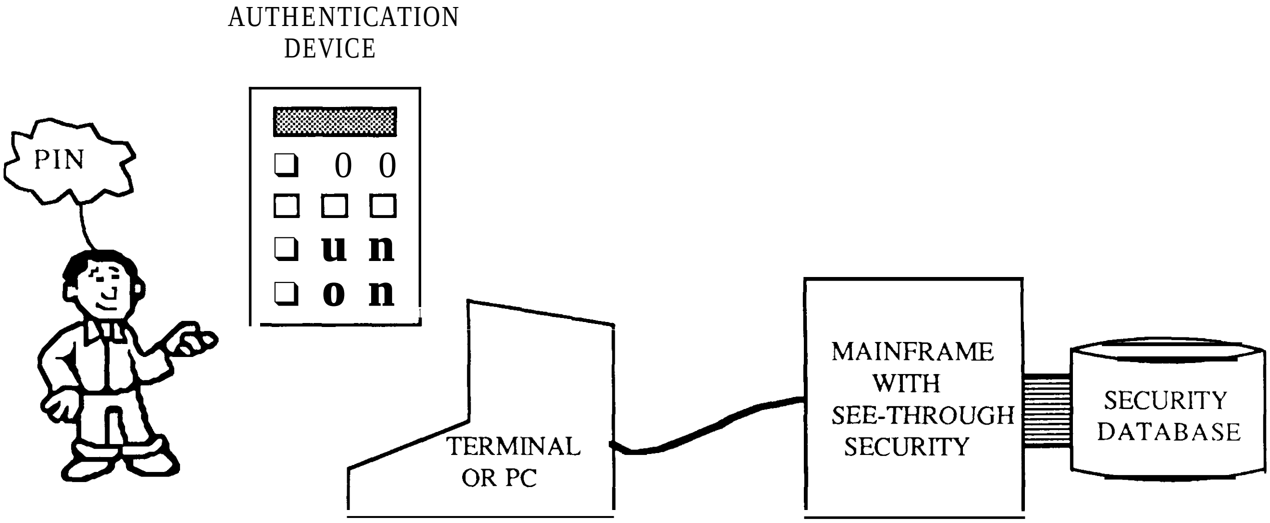
Token-based systems do much to eliminate the threat of external hackers. Under the token-based system, the password has become a one-time numeric response to a random challenge. The individual's memorized personal identification number or password to the token itself may be trivial, but the external hacker will ordinarily not have physical access to the device, which is usually designed to be tamper-resistant and difficult to counterfeit.

Hackers also have been known to make repeated tries at guessing passwords, or make use of overseen, stolen, or borrowed passwords. Repeated attack of the password to the host is also thwarted because this password is a random number and/or an encryption-based, one-time response from the token. The onetime nature of the host password also eliminates its compromise through observation, open display, or any form of electronic monitoring. As soon as a response is used, it becomes invalid. A subsequent access request will result in a different challenge from the host and a different required response from the token. An individual user can still unilaterally compromise the authentication process by giving away his or her token and memorized identification number. However, in this case, that individual no longer has access. In this way, the loss of a token serves as a warning that authentication may be compromised.

The see-through token (figure 19), used with a password, is an active device requiring complementary user action. Systems of this type currently on the market do not physically connect to a terminal, but instead provide a one-time user password for each access session. Tamper-proof electronics safeguard against reverse engineering or lost or stolen tokens. Some versions of these devices can challenge the host, effectively countering attempts at spoofing.

Two types of see-through tokens are currently available from several vendors: auto-

Figure 19.—The Mechanics of See-Through Security



Typical flow of events in a see-through security authentication session

1. User requests access to host through terminal or PC; enters user ID.
2. Host calculates random number (challenge) and transmits it to terminal.
3. User identifies himself to authentication device by entering Personal Identification Number (PIN), or through biometric identification.
4. User enters challenge from host into authentication device. Device uses the security algorithm and the user seed (both in device memory and inaccessible to the user) to calculate a numeric response.
5. User sends numeric response to host via the terminal.
6. Host calculates a response using the same challenge number, the security algorithm, and the user's seed from the security database. Host compares its response to user response, and grants or denies access.

SOURCE Ernst & Whinney, prepared under contract to OTA, November 1986 matic password generators, synchronized with the host, and challenge/response devices, using numerical key pads or optical character readers. According to some security consultants, these see-through techniques will be commonplace by the 1990s.[43]

Incorporating biometrics into these techniques will produce powerful safeguards, but there are associated risks. If biometric templates or data streams containing biometric information are compromised, the implications can be quite serious for the affected individuals because the particular measurements become invalid as identifiers. These risks can be minimized by properly designing the system so that biometric data are not stored in a central file or transmitted during the user verification procedure (as they would be in a host-based lookup mode). For many, therefore, the preferred operation for biometrics would be in a stand-alone mode, with the user carrying a biometric template in a token (like a smart card). However, tokens can be lost or stolen, and placing the biometric template on the token removes it from direct control by system security personnel. For these reasons, some installations, especially very high-security facilities using secure computer operating systems, may prefer host-based modes of operation. Figure 20 illustrates the differences between host-based and stand-alone modes for biometrics.

## Biometric and Behavioral Identification Systems

There are three major classes of biometric-based identification systems that are commercially available for user verification and access control. Since each of these systems is based on a different biometric principle, they vary widely in their technologies, operation, accuracy, and potential range of applications. The three classes are based on scans of retinal blood vessels in the eye,” hand geometry, and fingerprint identification. In addition, there are currently three classes of physiological-behavioral identification systems based on voice identification, keystroke rhythm, and signature dynamics. Most systems incorporate adaptive algorithms to track slow variations in users physical or behavioral characteristics. Although these adaptive features reduce the rate of false rejections, some can be exploited by imposters. Most systems also allow the preset factory threshold levels for acceptance and rejection to be adjusted by the user. Tables 5 and 6 illustrate some of the characteristics of biometric and behavioral technologies.

Biometrics is currently in a state of flux: technologies are advancing rapidly, firms are entering and leaving the marketplace, and new products are being tested and introduced. These technologies are being developed and marketed by a relatively large group of firms—28 at the end of 1986—some are backed by venture capital, and some are divisions of large multinational corporations. Many other companies were doing preliminary work in biometric or behavioral techniques. Therefore, these tables and the following discussions of biometric identification systems represent only a snapshot of the field.

There is evidence of growing interest in biometrics on the part of some Federal agencies. According to *Personal Identification News*, defense and intelligence agencies conducted more than 10 biometric product evaluations in 1986.[45]

### Retina Blood Vessels

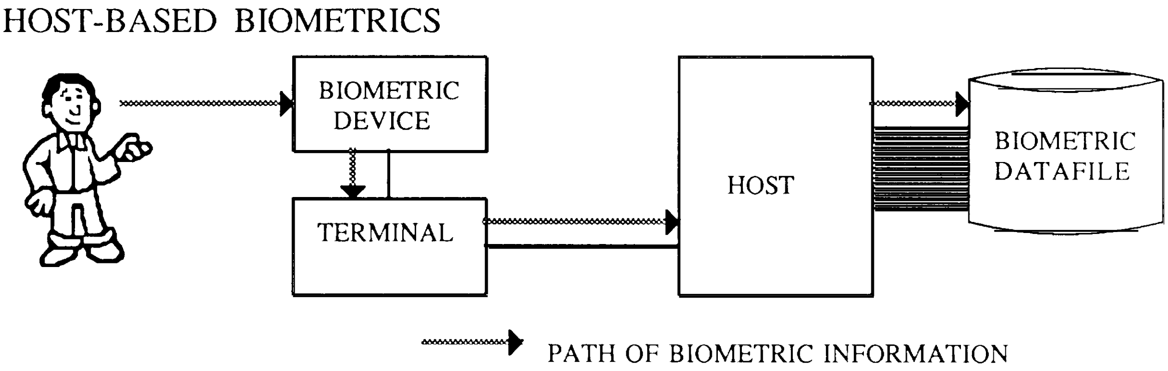
Retina-scanning technology for personal identification is based on the fact that the pattern of blood vessels in the retina is unique for each individual. No two people, not even identical twins, have exactly the same retinal vascular patterns. These patterns are very stable personal characteristics, altered only by serious physical injury or a small number of diseases, and are thus quite reliable for biometric identification. Factors such as dust, grease,

[43] Robert G. Anderson, David C. Clark, and David R. Wilson, “See-Through Securitv, ” *MIS Week*, Apr. 7, 1986.

[44] According t. *Personal Identification News*, February 1987, a patent has been issued for another type of eye system based on measurements of the iris and pupil (Leonard Flom and Aron Safir, U.S. Patent 4,641,349, Feb. 3, 1987).

“*Personal Identification News*, January 1987, p. 2.

**Figure 20.—Biometric Identification Configuration Alternatives: Host-Based v. Stand-Alone**



Description of authentication session

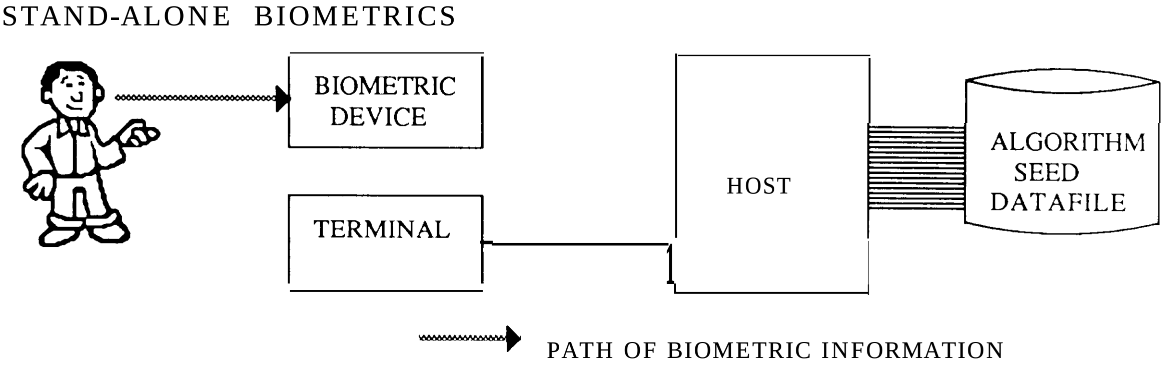
The user requests host access through the terminal, and enters his user ID. The host requests biometric authentication. The user enters the biometric information into the biometric device. The biometric data is transmitted to the host, where it is compared with the biometric data on file in the biometric datafile. Access is granted or denied.

Pros:

The user can gain access through any biometric device connected to the appropriate host. The device can be associated with terminals instead of users. An organization may require fewer devices i n this' mode, and the devices do not need to be portable.

Cons:

The biometric Information can be compromised in transmission or storage. Encrypted information can be diverted and attacked cryptologically.



Description of authentication session

The user requests host access through the terminal, and enters his user ID. The host calculates a random challenge and sends the challenge to the user terminal. The user identifies himself to the biometric see-through device through biometric input. The user then enters the random challenge into the device. The device calculates a response based on the algorithm and the user's algorithm seed. The user enters the response into the terminal for transmission to the host. The host performs the same calculations, obtaining the user's algorithm seed from the algorithm seed data file, and compares the responses. Access is granted or denied.

Pros:

No transmission or remote storage of the biometric information is required; the information is only maintained locally in the device itself. Also, the device does not need to be designed for connection to any particular terminal.

Cons:

Individual biometric devices are needed for each user, and the devices must be portable. This could result in an expensive implementation. Also, administrative issues may be more difficult to resolve in the stand-alone configuration. For example, a device malfunction may result in access denied to a user; in the host-based configuration, the user would gain access through an alternate device.

SOURCE Ernst & Whinney, prepared under contract to OTA November 1986

## Table 5.—Major Characteristics of Automated Biometric Identification Types

| | Eye retinal | Finger print | Hand geometry | Voice | Keystroke | Signature |
|---|---|---|---|---|---|---|
| Stability of measure (period) | Life | Life | Years | Years | Variable | Variable |
| Claimed odds of accepting an imposter (technically achievable without a high rate of false rejections) | 1 in billions | 1 in millions | 1 in thousands | 1 in thousands | 1 in a thousand | 1 in hundreds |
| Ease of physical damage–sources of environmentally caused false rejects | Difficult–a few diseases | Happens–cuts, dint, burns | Happens–rings, swollen fingers or joints, sprains | Happens–colds, allergies, stress | Happens–emotions, fatigue, learning curve for device | Happens–stress, position of device |
| Perceived intrusiveness of measure | Extreme to a small portion of population | Somewhat | Modest | Modest | None | Modest |
| Privacy concerns; surreptitious use of measure | Not feasible to do a scan surreptitiously | Data base can be compared to law enforcement files | Not a problem | Measurement can be transparent to user | Measurement can be transparent to user | Behavior IS already recognized as an ID function |
| Intrapersonal variation (chance of a false rejection, given training and experience in use) | Low | Low | Low | Moderate | Moderate | Moderate |
| Size of data template on current units | 35 bytes | Several hundred to several thousand bytes | 18 bytes to several hundred bytes | Several hundred bytes | Several hundred bytes | 50 bytes to several hundred bytes |
| Throughput time (note: level of security affects processing time) | 2 to 3 seconds | 4 to 5 seconds | 3 to 4 seconds | 3 to 5 seconds | Continuous process | 2 to 5 seconds |
| Cost range of products on the market (depends on configu-ration | $6,000 to $10,000 | $3,500 to $10,000 | $2,800 to $8,000 | $1,500 to $5,000 per door | $250 per terminal and up | $850 to $3,500 |
| Development goal for cost per workstation (by 1990) | $2,000 | $2,000 | $500 to $1 ,000 | $100 to $250 | $100 to $750 | $300 to $500 |
| Approximate number of patents outstanding | Less than 10 | 50 | 30 | 20 plus | Less than 10 | 100 |
| Approximate number of firms in market with products or prototypes as of summer 1986 (number with prototypes in parentheses) | 1 (0) | 3 (5) | 2 (4) | 2 (4) | 1 (1) | 3 (4) |

NOTE Other biometric PIDs under development include wrist vein, full-face. brainwave skin 011, and weight/gait devices

SOURCE Benjamin Miller prepared under contract to OTA October 1986 Oata update as of April 1987

**Table 6.—Configurations and Applications of Biometric Devices**

| | Configurations | | | | Applications | | | |
|---|---|---|---|---|---|---|---|---|
| | Off-line: reference templates stored | | | On-line: host data base | | | | |
| | In device | On mag stripe | On I.C. card | | Physical security | Computer security | Law enforcement | Financial transaction |
| Eye/retina | U | — | B | u | u | B | B | — |
| Fingerprint | D | — | u | u | u | | u | D |
| Hand geometry | B | u | — | u | u | : | — | — |
| Voice. | D | — | D | u | u | B | — | D |
| Keystroke dynamics | B | | — | B | | B | — | D |
| Signature | D | U | B | u | U | u | — | B |

U = In regular use by industry or Government
B = In Beta test use by industry or Government
D = In Development

SOURCE: Benjamin Miller, prepared under contract to OTA, October 1986. Data updated as of April 1987,

and perspiration that can make fingerprint techniques difficult do not affect retinal scanning, and injuries to the hand or fingers are more common than severe eye injuries.

At present, only one firm produces a retina-scanning identification device. One of its current models, mainly used for physical access control, was introduced in September 1984. Subjects look into an eyepiece, focus on a visual alignment target, and push a button to initiate the scan (done using low-intensity infrared light). The retinal pattern scanned is compared with a stored template and identification is based on a score that can range from – 1 to +1, depending on the degree of match. A new, low-cost version introduced at the end of 1986, uses a hand-held unit (the size of a large paperback book). It is intended for controlling access to computer terminals.

Potential applications are varied, but early purchasers are using the system for a range of uses, from physical access control to employee time-and-attendance reporting. Installations for physical access control have included a national laboratory, banks, a state prison, office buildings, and hospital pharmacy centers. According to the trade press, 300 units of the system had been shipped to end-users, original equipment manufacturers, and dealers by early 1986.[46] Some overseas users are also beginning to order the systems.

While retina scanning is fast, accurate, and easy to use, anecdotal reports suggest that the technique is perceived as being personally more intrusive than other biometric methods. Nevertheless, at the end of 1986, retinal technology accounted for the largest installed base of biometric units.[47]

### Hand Geometry

Several techniques for personal identification using aspects of hand geometry were under development or in production as of early 1986. First developed in the 1970s, more than 200 hand geometry devices are in use nationwide.

The oldest hand geometry technique was based on the length of fingers and the thickness and curvature of the webbing between them. Other techniques use the size and proportions of the hand or the distances between the joints of the fingers, infrared hand topography, palm print and crease geometry, or transverse hand geometry (viewing the sides of the fingers to measure hand thickness as well as shape). Some of these techniques combine the biometric measurement with a personal identification number. The biggest measurement problems with these devices involve people who wear rings on their fingers or whose fingers are stubbed or swollen.

The use of hand geometry systems was limited initially to high-security installations because of the cost and physical size of the

[46] *Personal Identification News*, April 1986.

[47] *Personal Identification* News, January 1987, p. 3.

equipment. However, technological advances have lowered equipment cost and size, thus extending the market to medium-security facilities, such as banks, private vaults, university food services, and military paycheck disbursing. According to vendors, users include insurance companies, a jai alai facility, engineering firms, and corporate offices. At the same time, more sophisticated systems being developed for high-security areas, such as military and weapons facilities, use a television camera to scan the top and side of the hand.

### Fingerprints

Fingerprints have been used to identify individuals since the mid-1800s.[48] Manual fingerprint identification systems were based on classifying prints according to general characteristics, such as predominant patterns of loops, whorls, or arches in the tiny fingerprint ridges, plus patterns of branches and terminations of the ridges (called minutiae). Fingerprint file data were obtained by using special ink and a ten-print card; fingerprint cross-checking with local and national records was done manually. The cross-checking process began to be automated in the late 1960s and by 1983 the Federal Bureau of Investigation (FBI) had converted all criminal fingerprint searches from manual to automated operations. [49] Some State and local law enforcement agencies are also beginning to automate their fingerprint records at the point of booking.

Several firms sell fingerprint-based systems for physical access control or for use in electronic transactions. The systems generally operate by reading the fingerprint ridges and generating an electronic record, either of location of minutia points or as a three-dimensional, terrain-like image. The scanned live print is compared with a template of the user's prerecorded print. The user is verified if the recorded and live print match within a predetermined tolerance. Alternative modes of operation use an individual password, identification number, or a smart card carrying the template fingerprint data. Costs vary according to the system configuration, but they are expected to fall rapidly as more systems are sold and as very large scale integrated (VLSI) technology is used.

By mid-1986, about 100 fingerprint-based systems had been installed, mostly in high-security facilities where physical access or sensitive databases must be reliably controlled. Some units, however, have been installed in health clubs, banks, and securities firms, either to control access or for attendance reporting. Also, firms are beginning to find overseas markets receptive. Potential applications will be wider as the price and size of the systems decrease. The bulk of near-term applications are expected to be mainly for physical access control, but work station devices are progressing.

### Voice Identification

Subjective techniques of voice identification —listening to speakers and identifying them through familiarity with their voices—have been admissible evidence in courts of law for hundreds of years.[50] More recently, technical developments in electronics, speech processing, and computer technology are making possible objective, automatic voice identification, with several potential security applications and important legal implications.[51] The sound produced by the vocal tract is an acous-

[48] For a complete discussion of fingerprint identification techniques, see: "Fingerprint Identification, " U.S. Department of Justice, Federal Bureau of Investigation (rid); and *The Science of Fingerprints,* U.S. Department of Justice, Federal Bureau of Investigation, (Washington, DC: U.S. Government Printing Office, Rev. 12/84).

[49] Charles D. Neudorfer, "Fingerprint Automation: Progress in the FB 1's Identification Division, *FBI* Law *Enforcement Bulletin*, March 1986.

[50] Historical and theoretical discussion of voice identification and its legal applications can be found in: Oscar Tosi, *Voice Identification: Theory and Legal Applications* I Baltimore, MD: University Park Press, 1979).

[51] Although courts in several jurisdictions have ruled that voiceprints are scientifically unreliable, courts in some States, including Maine, Massachusetts, and Rhode Island, consider them to be reliable evidence. A recent ruling by the Rhode 1sland Supreme Court allowed a jury to consider evidence of voiceprint comparisons and to decide itself on the reliability of that evidence, noting that, "The basic scientific theory involved is that every human voice is unique and that the qualities of uniqueness can be electronically reduced . . .' (*State* v. *Wheeler,* 84-86-C, A., July 29, 1985). Source: *Privacy Journal*, August 1985. p. 2.

tic signal with a phonetic and linguistic pattern that varies not only with the speaker's language and dialect, but also with personal features that can be used to identify a particular speaker.

Voice recognition technology has been around for some time,[s2] but personal identification systems using it are just beginning to reach the market, mainly because of the formerly high cost and relatively high error rates.[53] Some large electronics and communications firms have experimented with voice recognition systems for many years, but are just now developing systems to market."

An important distinction should be made here between technologies to understand words as spoken by different individuals (speech recognition) and technologies to understand words only as they are spoken by a single individual (speech verification). Voice identification systems are based on speech verification. They operate by comparing a user's live speech pattern for a preselected word or words with a pre-enrolled template. If the live pattern and template match within a set limit, the identity of the speaker is verified. Personal identification numbers are used to limit searching in the matching process. According to manufacturers and industry analysts, potential applications include access control for computer terminals, computer and data-processing facilities, bank vaults, security systems for buildings, credit card authorization, and automatic teller machines.

### Signature Dynamics

A person's signature is a familiar, almost universally accepted personal verifier with well-established legal standing. However, the problem of forgery—duplicating the appearance of another person's signature-raises substantial barriers to the use of static signatures (i.e., recognizing the appearance of the signed name) as a secure means of personal identification.

Newer signature-based techniques use dynamic signature data that capture the way the signature is written, rather than (or, in addition to) its static appearance, as the basis for verification. The dynamics include the timing, pressure, and speed with which various segments of the signature are written, the points at which the pen is raised and lowered from the writing surface, and the sequence in which actions like dotting an "i" or crossing a "t' are performed. These actions are very idiosyncratic and relatively constant for each individual, and are very difficult to forge.[bs]

A number of companies have researched signature dynamics over the past 10 years and several have produced systems for the market. The systems consist of a specially instrumented pen and/or a sensitive writing surface. Data are captured electronically and processed using proprietary mathematical algorithms to produce a profile that is compared with the user's enrolled reference profile or template. The systems work with an identification number or smart card identifying the profile and template to be matched.

Prices for these systems are relatively low compared with some other identification technologies. Combined with the general user acceptability of signatures (as opposed, say, to fingerprinting or retinal scans), this is expected to make signature dynamics suitable for a wide range of applications.[s6] Potential financial applications include credit card transactions at the point of sale, banking, automatic teller machines, and electronic fund transfers. Systems are currently being tested in bank-

[52] The basics of most voice systems can be traced to work over the past 20 years at AT&T Bell Laboratories. *Personal Identification News*, October 1985.

[53] See Tosi, "Fingerprint Identification, " U.S. Department of Justice, Federal Bureau of Investigation (rid); and *The Science of Fingerprints,* U.S. Department of Justice, Federal Bureau of Investigation (Washington, DC: U.S. Government Printing Office, Rev. 12/84), ch. 2.

"Personal Identification News, January 1986.

"Several signature dynamics systems have adaptive features that can allow a person's signature to vary slowly over time; enrollment procedures require several signatures to set the reference signature profile and users are permitted more than one (usually two) signature attempts for identification.

[56] George Warfel, "Signature Dynamics: The Coming ID Method, *Data Processing and Communications Security*, vol. 8, No. 1. (n.d. )

ing (check cashing) and credit card applications, where they might eventually replace dial-up customer verification systems.[57] Systems connected to a host computer could also provide access control as well as accountability and/or authorization for financial transactions and controlled materials, among other uses.

### Keyboard Rhythm

Early work, beginning in the 1970s, on user verification through typing dynamics was done by SRI International and, with National Science Foundation (NSF) funding, the Rand Corp.[58] In 1986, two firms were developing commercial personal identification systems based on keyboard rhythms for use in controlling access to computer terminals or microcomputers, including large mainframe computers and computer networks. One of the firms acquired the keystroke dynamics technology from SRI International in 1984 and contracted with SRI to develop a product line. In 1986, the firm reported that it was developing 11 products configured on plug-in printed circuit boards and that it planned to test these products in several large corporations and Government agencies in 1987. By mid-1987, the firm had contracts with over a dozen Fortune 500 corporations and five Government agencies to test its products.[59] A researcher in the second firm, who had received an NSF grant in 1982 to investigate typists' "electronic signatures, " formed a venture corporation in 1983 to commercialize an access control device based on the technique. He was awarded a patent in late 1986.

Keyboard-rhythm devices for user verification and access control are based on the premise that the speed and timing with which a person types on a keyboard contains elements of a neurophysiological pattern or signature that can be used for personal identification.[60] The stored "user signature" could be developed explicitly or so that it would be transparent to the user—perhaps based on between 50 and 100 recorded log-on accesses or 15 to 45 minutes of typing samples if done openly and explicitly, or based on several days of normal keyboard work if done transparently (or surreptitiously). The stored signature could be updated periodically to account for normal drifts in keyboard rhythms. These types of devices might be used only at log-on, to control access to selected critical functions, or to prevent shared sessions from occurring under one user log-on. The prices of these systems depend on their configuration: current estimates range from $1,000 for a card insert for a host computer capable of supporting several work stations to $10,000 for a base system that could store 2,000 user signature patterns and support four channels that communicate simultaneously.

[57] Ibid.

[58] R. Stockton Gaines, William Lisowski, S. James Press, and Norman Shapiro, "Authentication by Keystroke Timing: Some Preliminary Results, " R-2526 -N' SF. The RAND Corp., Santa Monica, CA, May 1980.

[59] Rob Hammon, International Bioaccess System Corp., personal communications with OTA staff, Aug. 4, 1987.

[60] Some speculate that this method would only be effective for experienced typists, rather than erratic "hunt and peck" novices, but at least one of the firms claims that the method can be implemented for use by slow or erratic typists as well.

## ACCESS CONTROL SOFTWARE AND AUDIT TRAILS

Once the identity of a user has been verified, it is still necessary to ensure that he or she has access only to the resources and data that he or she is authorized to access. For host computers, these functions are performed by access control software. Records of users' accesses and online activities are maintained as audit trails by audit software.

### Host Access Control Software

To provide security for computer systems, networks, and databases, user identifications and passwords are commonly employed with any of a number of commercially available add-on software packages for host access control, Some have been available since the mid-to-late

### Box D.—Host Access Control Software

A number of host access control software packages are commercially available that work with a computer's operating system to secure data and the computing resources themselves. Access control software is designed to offer an orderly method of verifying the access authority of users. As such, it can protect the system, its data, and terminals from unauthorized users and can also protect the system and its resources from unauthorized access to sensitive data and from errors or abuses that could harm data integrity.

Access control software intercepts and checks requests for system or database access; the various commercial packages vary in the ways they check requirements for authorized access. Most require both user identification and a password to allow access; the user's identification determines his or her level of access to the system hardware and files. Passwords may be changed from time to time, or even (in some systems) encrypted. To prevent unauthorized users from guessing passwords, most of these systems limit the number of incorrect access attempts before logging the user off and sending a security alert message (including the user's identification number). Some packages generate their own passwords; these tend to be more difficult for intruders to guess, but also are more difficult for authorized users to remember. The data files containing user identification numbers and passwords are critical to system security because knowledge of correct identification number and password combinations would allow anyone access to the system and its most sensitive files. Therefore, some access control packages do not allow even security administrators to know user passwords—users set up their own, or the system generates the passwords, which may change frequently. The structure of system-generated passwords is being studied to make them easier to remember.

Access control software packages allow for audit features that record unauthorized access attempts, send violation warning messages to security, and/or log the violator off the system. Other audit features include keeping a log of users' work activities on a daily basis, printing reports of use and violation attempts, and allowing security officers to monitor users' screens. These packages can also be used in conjunction with special facility-specific security access controls implementing other restrictions (time-of-day, database, file, read-only, and location/terminal) written in custom code to fit the application environment. Versions of access control software packages are currently available to protect a variety of manufacturers' mainframe operating systems and minicomputers.

Development of software for commercial host access control began in the early 1970s. Currently, there are more than 24 software packages from different vendors. These packages are designed to work with a variety of host configurations (CPU, operating system, storage space, interfaces to other system software).

SOURCE: DataPro Research Corp., "All About Host Access Control Software, " 1S5'2-001, June 1985,

1970s. (See box D.) As of 1986, three access control software packages were market leaders: RACF, with some 1,500 installations since 1976; ACF2, developed by SKK, Inc., and marketed by the Cambridge Systems Group, with more than 2,000 installations since 1978; and Top Secret, marketed by the CGA Software Products Group, with more than 1,000 packages installed since 1981.[6']

In all, more than two dozen software packages are being marketed, some for classified applications. These packages vary widely in their range of capabilities and applications, and are usually either licensed with a one-time fee or leased on a monthly or yearly basis. Fees and maintenance can range from several hundred dollars up to $50,000 per year.

Instead of the "add-on" software packages mentioned above, the operating systems of many computers include some level of access

"DataPro, reported in *Government Computer News*, Dec. 5, 1986, p. 40.

control built into the basic system software. Most of the built-in systems offer features comparable to the add-on systems designed for commercial use.[62] The number of new computer operating systems incorporating access control and other security features is expected to increase.

Commercial access control software packages commonly rely on users memorizing their identification numbers or passwords keyed into the terminal. Thus, they tend to rely on the "something known" criterion for security. They also tend to permit a single individual-in principle, the security officer–access to the central files containing users' authorization levels and, although less prevalent in newer systems, their users' passwords. A characteristic of the higher security packages is that they are designed for applications in which users with varying levels of authorization are using a system containing information with varying degrees of sensitivity. An example is a system containing classified information, where some is classified "confidential" and some "secret."

NSA's National Computer Security Center (NCSC) has provided Federal agencies with criteria to evaluate the security capabilities of trusted computer systems. According to the NCSC definition, a trusted computer system is one that employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information. The trusted system criteria contained in the so-called "Orange Book, [63]' developed by NSA, define four classes of security protection. These range from Division D (minimal protection) up through Class Al of Division A (verified protection). NCSC also evaluates access control software products submitted by vendors and rates them according to the Orange Book categories. The evaluations are published in the Evaluated Products List, which is made available by NCSC to civilian agencies and the public. As of May 1987, eight products had received NCSC ratings and more than 20 others were being evaluated.

Despite their importance to host computer security, particularly for classified applications, a detailed look at trusted operating systems is beyond the scope of this OTA assessment. A number of computer security experts, including those at NSA, consider trusted operating systems to be crucial to securing unclassified, as well as classified, information. They consider access controls to be of limited value without secure operating systems and the NCSC criteria, at least at the B and C levels, to be of significant value in both classified and commercial applications.[64] However, other computer security experts have questioned whether design criteria appropriate for classified applications can or should be applied to commercial applications or even to many unclassified Government applications. (See ch. 5.)

The recent debate over the applicability of what some term the 'military' model to commercial computer security[65] had progressed to the point where plans were made for an invitational workshop on this topic to be held in the fall, 1987.[66] This specific area of concern illustrates the issue of whether or not it

"S. Lipner, personal communication with OTA staff, Dec. 24, 1986.

[63] Department of Defense Trusted Computer System Evaluation Criteria, Department of Defense Standard DoD 5200.28-STD, December 1985. Two companion DoD documents ("Yellow Books") summarize the technical rationale behind the computer security requirements and offer guidance in applying the standard to specific Federal applications: *Computer Security Requirements–Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, CSC-STD-O03-85*, June 25, 1985; and *Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements*, CSC-STD-004-85, June 25, 1985.

"Harold E. Daniels, Jr., NSA S-0022-87, Jan. 21, 1987. Safeguards currently used by the private and civil sectors have received B- and C-level ratings.

[65] See, for example, David D. Clark and David R. Wilson, "A Comparison of Commercial and Military Computer Security Policies, " *Proceedings*, 1987 *IEEE Symposium on Security and Privacy* (Oakland, CA: Institute for Electrical and Electronic Engineers, Apr. 27-29, 1987).

[66] The Workshop on Integrity Policy fOr Computer Information Systems will be held at Bentley College, Waltham, MA in the fall, 1987. I t is being organized by Ernst & Whinney, and is co-sponsored by the Association for Computing Machinery, the Institute for Electrical and Electronic Engineers, the National Bureau of Standards, and the National Computer Security Center.

is in the Nation's best interests to assign to one agency—namely, NSA—the task of meeting all the needs of the Government civilian agencies and the private sector while continuing to carry out its other missions. These concerns will be raised again and explored in chapters 5 and 7.

### Audit Trails

Another major component of computer security, usually part of a host access control system, is the ability to maintain an ongoing record of who is using the system and what major actions are performed. The system's operators can then review this "audit trail" to determine unusual patterns of activity (e.g., someone consistently using the system after office hours) or to reconstruct the events leading to a major error or system failure.

In the past few years, software has begun to combine auditing with personal identification. An audit log can record each time a user seeks access to a new set of data. Figure 21 shows a sample audit log. Audit trail software is routinely recorded on most mainframe computers that have many users. Such software is available but seldom used on similar minicomputers, in part because it slows down the performance of the system and is only rarely available for microcomputers.

Audit trails are among the most straightforward and potentially most effective forms of computer security for larger computers and multi-user minicomputers. However, the fact that they are easily available for these machines does not mean that they are effectively used. Many system managers either do not use the audit trails or rarely if ever review the logs once generated. For example, OTA found that only 58 percent of 142 Federal agencies surveyed use audit software for computers containing unclassified, but sensitive information. Only 22 percent use audit software for all of their unclassified, but sensitive systems.[67] Similarly, a 1985 General Accounting Office (GAO) study that exam.ined 25 major computer installations found that only 10 of them met GAO's criteria for use of audit trails.[68]

Part of the reason why audit trails are not more widely and effectively used is that they tend to create voluminous information that is tedious to examine and difficult to use. Technical developments can ease this problem by providing tools to analyze the audit trail information and call specified types or patterns of activities to the attention of system security officers. Thus, it would not be necessary, except in case of a disaster, to review the entire system log.

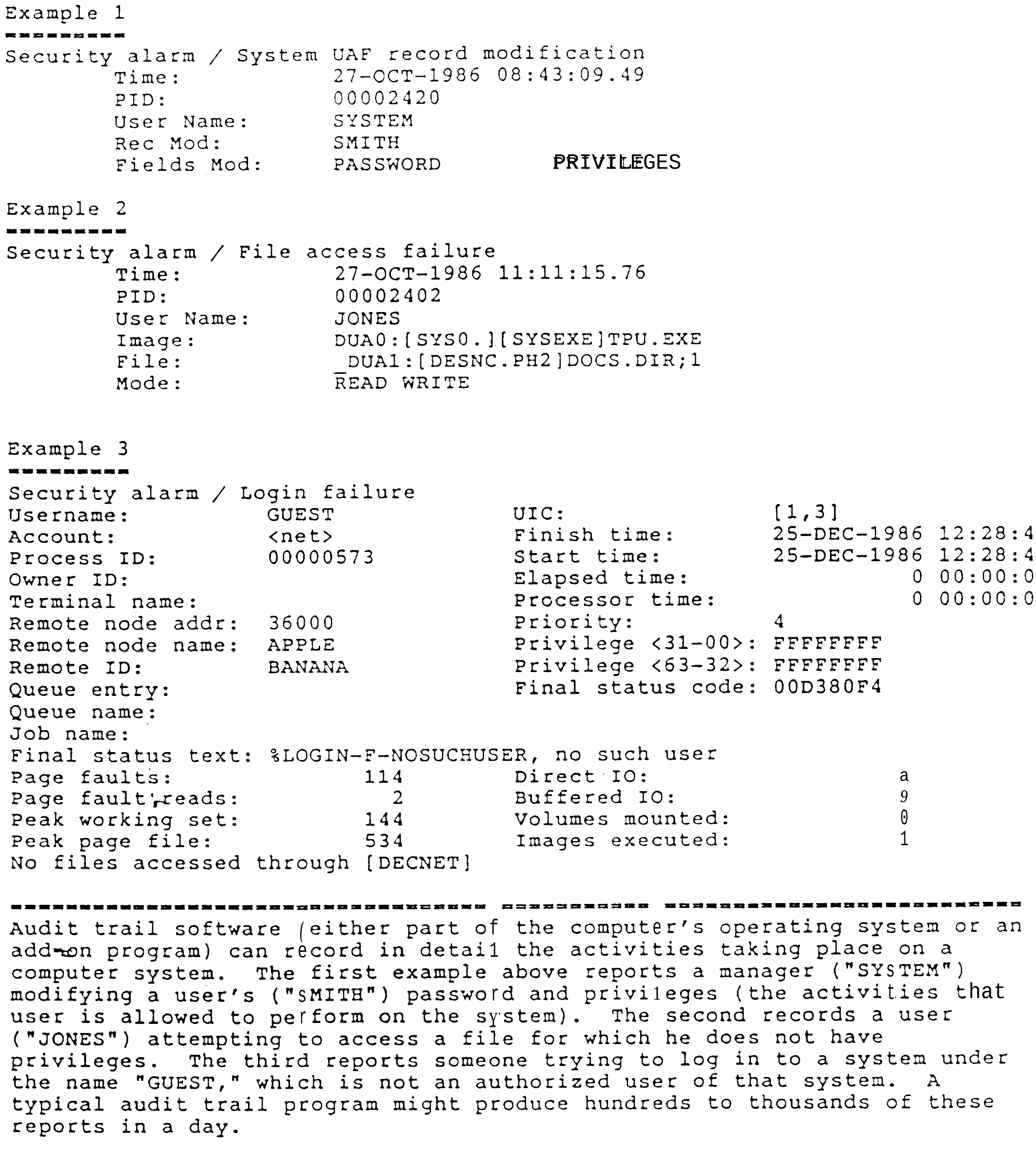
[67] Information Security, Inc., "Vulnerabilities of Public Telecommunications Systems To Unauthorized Access, " OTA contractor report, November 1986.

[68] William S. Franklin, General Accounting Office, statement on Automated Information System Security in Federal Civilian Agencies, before House Committee on Science and Technology, Subcommittee on Transportation, Aviation, and Materials, 99th Cong., lst. sess., Oct. 29, 1985.

## ADMINISTRATIVE AND PROCEDURAL MEASURES

Important as technical safeguard measures like the ones that have been described above can be, administrative and procedural measures can be even more important to overall security. For example, encryption-based communications safeguards can be rendered useless by improper management of "secret" encryption or decryption keys (see below). In the field of computer security, technical measures of the types mentioned above are almost useless if they are not administered effectively. While they can only be raised briefly here, some

**Figure 21 .—Example Reports From Audit Trail Software**



```
Example 1
=========
Security alarm / System UAF record modification
        Time:           27-OCT-1986 08:43:09.49
        PID:            00002420
        User Name:      SYSTEM
        Rec Mod:        SMITH
        Fields Mod:     PASSWORD         PRIVILEGES

Example 2
=========
Security alarm / File access failure
        Time:           27-OCT-1986 11:11:15.76
        PID:            00002402
        User Name:      JONES
        Image:          DUA0:[SYS0.][SYSEXE]TPU.EXE
        File:           _DUA1:[DESNC.PH2]DOCS.DIR;1
        Mode:           READ WRITE


Example 3
=========
Security alarm / Login failure
Username:           GUEST               UIC:                [1,3]
Account:            <net>               Finish time:        25-DEC-1986 12:28:48.
Process ID:         00000573            Start time:         25-DEC-1986 12:28:47.
Owner ID:                               Elapsed time:                 0 00:00:00.
Terminal name:                          Processor time:               0 00:00:00.
Remote node addr:   36000               Priority:           4
Remote node name:   APPLE               Privilege <31-00>:  FFFFFFFF
Remote ID:          BANANA              Privilege <63-32>:  FFFFFFFF
Queue entry:                            Final status code:  00D380F4
Queue name:
Job name:
Final status text: %LOGIN-F-NOSUCHUSER, no such user
Page faults:               114          Direct IO:                  a
Page fault reads:            2          Buffered IO:                9
Peak working set:          144          Volumes mounted:            0
Peak page file:            534          Images executed:            1
No files accessed through [DECNET]

==================================== =========== ========================
```

Audit trail software (either part of the computer's operating system or an add-on program) can record in detail the activities taking place on a computer system. The first example above reports a manager ("SYSTEM") modifying a user's ("SMITH") password and privileges (the activities that user is allowed to perform on the system). The second records a user ("JONES") attempting to access a file for which he does not have privileges. The third reports someone trying to log in to a system under the name "GUEST," which is not an authorized user of that system. A typical audit trail program might produce hundreds to thousands of these reports in a day.

SOURCE: Digital Equipment Corp., 1986.

of the most important aspects of computer security administration include:[69]

- *Maintaining a Written Security Policy and Assigning Responsibilities for Security.* Many organizations simply do not have a policy regarding computer security, or the policy is unavailable to computer users, or the policy is not followed. Computer security experts report that one of the most important factors in encouraging good computer security is for users to know that management is indeed committed to it. Also, it is important that each individual in the organization be aware that protecting information assets is part of his or her responsibility.
- *Password Management.* Password-based access control systems are much less effective if computer users write their passwords on the wall next to their terminal, if they choose their birthday or spouse's name as their password, or if passwords are never changed. Thus, policies to encourage reasonable practices in password systems are not only essential, but are probably one of the simplest and most neglected ways to enhance security.
- *Reviewing Audit Trails.* Similarly, audit software is of little value unless the logs created by its use are reviewed.
- *Training and Awareness.* Relatively simple programs can help users understand what kind of security problems the organization faces and their role in enhancing security.
- *Periodic Risk Analyses.* Such an analysis involves examining each computer system, the sensitivity of the data it handles, and the measures that are in use or should be considered to protect the system.
- *Personnel Checks.* Organizations may wish to avoid putting employees with certain kinds of criminal records or financial problems in jobs with access to sensitive information. It maybe difficult, however, to perform such checks without raising concerns about employee privacy.
- *Maintaining Backup Plans and Facilities.* Many organizations do not have any policy or plans for what to do in the event of a major disaster involving an essential computer system. For example, in 1985 only 57 percent of Federal agencies had (or were in the process of developing) backup plans for their mainframe computer systems.[70]

[69] For a more complete discussion of administrative procedures for computer security, see U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Management, Security, and Congressional Oversight, OTA-C IT-297* (Washington, DC: U.S. Government Printing Office, February 1986). Additionally, the General Accounting Office (GAO) has issued many reports over the last decade identifying major information security problems and surveying information security practices in Federal agencies (see tables 4-5 in the February 1986 OTA report for a selected list of some of these GAO reports).

[70] Data from OTA's Federal Agency Request given in ch. 4 of *Federal Government Information Technology: Management, Security, and Congressional Oversight, OTA-C IT-297* (Washington, DC: U.S. Government Printing Office, February 1986).

# COMPUTER ARCHITECTURES

The computer itself has to be designed to facilitate good security, particularly for advanced security needs. For example, it should monitor its own activities in a reliable way, prevent users from gaining access to data they are not authorized to see, and be secure from sophisticated tampering or sabotage. The national security community, especially NSA, has actively encouraged computer manufacturers to design more secure systems. In particular, NCSC has provided guidelines for secure systems and has begun to test and evaluate products submitted by manufacturers, rating them according to the four security divisions discussed above. A more thorough discussion of secure computing bases is beyond the scope of this assessment.

While changes in computer architecture will gradually improve security, particularly for larger computer users, more sophisticated architecture is not the primary need of the vast majority of current users outside of the national security community. Good user verification coupled with effective access controls, including controls on database management systems, are the more urgent needs for most users.

## COMMUNICATIONS LINKAGE SAFEGUARDS

In the past few years it has become increasingly clear that computers are vulnerable to misuse through the ports that link them to telecommunications lines, as well as through taps on the lines themselves. Although taps and dial-up misuses by hackers may not be as big a problem as commonly perceived, such problems may grow in severity as computers are increasingly linked through telecommunications systems. Similarly, computer and other communications using satellite transmissions motivate users to protect these links.

### Port-Protection Devices

For some computer applications, misuse via dial-up lines can be dramatically reduced by the use of dial-back port protection devices used as a buffer between telecommunications lines and the computer. The market for these is fairly new, but maturing. Some products are stand-alone, dial-back units, used for single-line protection; others are rackmounted, multi-line protection units that can be hooked up to modems, telephones, or computer terminals. Some 40 different models of commercial dial-back systems were being sold in 1986, with prices ranging from several hundred to several thousand dollars (on the order of $500 per incoming line), depending on the configuration, features, and number of lines protected. Some, but not all, models offer data encryption as a feature, using DES and/or proprietary algorithms.

In addition to these dial-back systems, security modems can be used to protect data communications ports. These security modems are microprocessor-based devices that combine features of a modem with network security features, such as passwords, dial-back, and/or encryption. Security modems featuring encryption must be used in pairs, one at each end with the correct encryption key and algorithm to encrypt and decrypt communicated data and instructions. About 20 different models of commercial security modems were available in 1986, with various combinations of features, such as password protection, auditing, dial back, and/or encryption. Security modems featuring encryption offer the DES and/or proprietary encryption algorithms.

According to DataPro Research Corp., the market for security modems has been in a period of rapid change since the early 1980s—new and advanced products have been introduced, more users have adopted remotely accessible data operations, and prices have continued to fall. Prices for security modems range from less than $500 to almost $2,000, depending on the features included.

An example of the use of this type of port protection follows: When a remote user wants to logon to the machine, the security modem is programmed to answer the call, ask for his or her log-on identification and password, and then (if the identification and password are proper) call back the computer user at the location at which he or she is authorized to have a terminal. There may be some inconvenience in using the device, however, if authorized computer users frequently call from different phone numbers. In addition, there are ways to thwart dial-back modems, such as using "call-forwarding" at the authorized user's phone to route the computer transmission elsewhere to an unauthorized phone or user.

Dial-back devices are generally considered too inconvenient to use for one very important application: large-scale database applications, such as commercial credit reporting services. These services can receive thousands of calls a day from terminals in banks and credit bureaus seeking to verify a person's credit worthiness, often prior to a loan or establishment of a line of credit. The use of dial-back devices for such an application are time-consuming and costly, and are difficult to administer given the number of terminals that would have to be connected to the devices. Thus, those who illegally obtain passwords to access these systems can now use them relatively easily.

Other technical measures may be useful for large public database systems, however. For example, remote terminals in retail stores could be equipped to perform a coded "handshake" with the host computer before they can gain access to the database. Or, as the telecommunications network evolves toward wider use of digital signaling equipment, it will increasingly be possible for host computers to know the phone number of the person trying to gain access and thus to check that phone number against its list of authorized customers.

### Satellite Safeguards

In the military, highly directional antennas, spread-spectrum modulation, and laser communication are among the measures used or contemplated to protect satellite signals from unauthorized reception. Other methods range from analog scrambling to full digital encryption. For encryption, equipment costs and operational complexity tend to inhibit the widespread deployment of elaborate encryption techniques. This is particularly true for point-to-multipoint networks, where the expense of providing a large number of end users with decryption equipment may not be worth the cost.

The current trend is toward the implementation of security by some service providers. For example, the video industry, one of the largest users of satellite capacity, has begun to use analog scrambling techniques to discourage casual theft of service. Methods for encrypting video signals range in complexity from line-by-line intensity reversal to individual pixel scrambling. Decryption keys may be broadcast in the vertical blanking interval. In some systems, individual subscribers can be addressed, providing selective access to the programming. Scrambling techniques are also being used by some providers of point-to-multipoint satellite data networks. Since these transmissions are typically digital, more effective encryption systems can be used. In some cases, a device using the Data Encryption Standard is provided in the subscribers' receiver equipment and key distribution is accomplished in real time to selected end users (i.e., to those who have paid to receive the broadcast) .7'

The Department of Defense has had continuing concerns for the vulnerability of satellites to interception and other misuse. The Senate Committee on Appropriations approved funds in 1986 for the first year of a 5-year plan developed by NSA that would enable DoD to reimburse satellite carriers for installing encryption equipment to protect their transmissions. [72]

### Fiber Optic Communications

Fiber optic communications links provide an important barrier to misuse, because more sophisticated means are required to eavesdrop. Further, means are available to detect some forms of misuse.

### Common Carrier Protected Services

Several common carriers encrypt their microwave links in selected geographic areas as well as their satellite links that carry sensitive Government communications. These protected services are largely the result of NSA and GSA procurements beginning in the 1970s. Much of the following discussion is excerpted from the OTA contractor report, "Vulnerabilities of Public Telecommunications Systems to Unauthorized Access, prepared by Information Security Incorporated, November 10, 1986.

[71] Note that the Electronic Communications Privacy Act of 1986 (Public Law 99-508) made the private use of "backyard" earth stations legal for the purpose of receiving certain satellite transmissions, unless it is for the purpose of direct or indirect commercial advantage or for private gain.

[72] See U.S. Senate, Committee on Armed Services, National Defense Authorization Act for Fiscal Year 1987. Report 99-331 to accompany S. 2638, 99th Cong., 2d sess., July 8, 1986, p. 295.

The latest transmission technology using fiber optics is difficult to intercept because the information signal is a modulated light beam confined within a glass cable. NSA judges both cable and fiber media to provide adequate protection for unclassified national security-related information.

American Telephone & Telegraph Co. (AT&T) protects its microwave links in Washington, D. C., New York, and San Francisco. Major routes are being expanded with fiber optics. Protected service is available in areas designated by NSA and private line service can be offered over selected fiber and cable routes. In addition, customized encryption can be installed on selected microwave and satellite circuits for particular customers.[73]

MCI offers protected terrestrial microwave services in those areas specified by NSA. In addition, MCI offers customers the option of protected service in many other major metropolitan areas. These customers can order protected communications throughout the MCI portion of the circuit, using MCI fiber optic system, encrypted terrestrial microwave, and the MCI-encrypted satellite network.[74]

U.S. Sprint, which reached 2.5 million customers or about 4 percent of all long-distance customers in 1986, intends to create an all-fiber network by the end of 1987 that the company expects will carry more than 95 percent of its voice and data traffic.[75] This means any call or circuit carried via the Sprint network would be harder to intercept than unprotected microwave transmissions. Currently, Sprint has protected microwave radio in the NSA-designated areas. [76]

International Telephone & Telegraph Co. (ITT) offers protected service in the NSA-designated zones, consisting of protected microwave circuits. The service is available now on a private-line basis to commercial or business customers. [77]

The American Satellite Co. offers two types of protected carrier services. One uses an encrypted satellite service that has been approved by NSA for protecting unclassified, but sensitive information. The second service uses protected terrestrial microwave in the NSA-designated areas. This also is available on a private line basis in the service areas.[78]

Pacific Bell plans to have a complete fiber and cable network between all its central offices within 10 years. These plans include most of San Francisco, Los Angeles, and San Diego; at present, two fiber rings in San Francisco are routed past all major office buildings. Pacific Bell can offer customers in the San Francisco area fiber optic routes throughout most of their operating region. In Los Angeles, the company has 27 locations used in the 1984 Olympics linked by fiber optic facilities and is extending its network. These offerings can be augmented with new fiber spurs to a customer's location. All of these services are filed with the California Public Utility Commission as special service engineering and are not tariffed by the FCC.[79]

Bell Communications Research (Bellcore) is developing a service that would be implemented by the Bell Operating Companies. The service would provide special handling and routing over protected or less-interceptable (i.e., fiber or cable) lines. The initial goal is to use as much as possible the inherent security features of the existing network. This service is being designed to meet NSA requirements for protecting unclassified government information so that costs (for Government contractors) will be reimbursable under National COMSEC Instruction 6002 and Department of Defense Instruction 5210.74. Bellcore anticipates that this service will also be available to other commercial customers,”)

[73] ‘AT&T Communications Security, marketing literature, 1986.

[74] MCI Communication Protection Capabilities, marketing literature, 1986.

[75] U.S. Sprint, "Clearline," vol. 2, Issue 5, Kansas City, MO, spring 1987.

[76] “M'hy U.S. Sprint Is Building the First Coast-to-Coast Fiber Optic Network and What's in It for You, ” U.S. Sprint marketing literature, 1986.

[77] ITT Private Line Service—Security, marketing literature, 1986,

[78] Protected Communications Services, marketing literature, 1986.

[79] OTA Federal Agency Data Request, op. cit.

[80] Ibid., ref. 2'7.