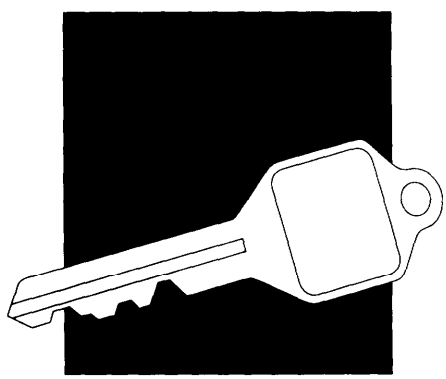
Safeguarding Networked Information

2

Networked information is constantly exposed to *threats*—events or agents that have the potential to cause harm to a system or information assets. These threats have the potential to exploit a network's many *vulnerabilities*--weaknesses, or points susceptible to attack. New vulnerabilities emerge as systems are built or changed. If these are exploited, substantial financial losses and an overall failure to achieve the original objectives of the network can result. The true incidence rates and losses arising from these threats are unknown, however, since the y are often not detected, not reported, or require placing a monetary value on a relatively intangible loss. Financial institutions, in particular, are reluctant to report losses to avoid negative publicity that might cause more losses or loss of business. Also, the probability that particular threats will exploit particular vulnerabilities in a network—the amount of risk—varies from network to network.

Although multiple threats often combine to expose a vulnerability, threats to networked information can be loosely grouped into the following categories:

- **Human errors and design faults. The** largest source of losses is due to unintentional human actions during operations. Some experts estimate that over one-half of the total financial and productivity losses in information systems is the result of



human errors, as opposed to intentional and malicious acts.[1] These acts include improperly installing and managing equipment or software, accidentally erasing files, updating the wrong file, transposing numbers, entering incorrect information in files, neglecting to change a password or back up a hard disk, and other acts that cause loss of information, interruptions, and so forth.

Many of these and other circumstances are arguably due to faults in design that do not prevent many common human errors (or other threats) from resulting in losses. An unusual but legitimate sequence of events also can reveal a vulnerability in system design. Such design errors may come with off-the-shelf software or hardware, or may be built into the system by the network managers.

- **Insiders.** Many violations of information safeguards are performed by trusted personnel who engage in unauthorized activities or activities that exceed their authority. These insiders may copy, steal, or sabotage information, yet their actions may remain undetected.[2] These individuals can hold clearances or other authorizations, or may be able to disable network operations or otherwise violate safeguards through actions that require no special authorization.
- **Natural disasters and environmental damage.** Wide-area disasters such as floods, earthquakes, fires, and power failures can destroy both the main information facilities as well as their backup systems. Broken water lines. uneven environmental conditions, and other localized threats also produce significant but less sensational damage.
- **"Crackers" and other intruders.** A small but growing number of violations come from unauthorized "crackers"[3] who may intrude for monetary gain, for industrial secrets, or for the challenge of breaking into or sabotaging the system. This group receives the most sensational treatment in the press and includes teenagers breaking into remote systems as well as professional criminals, industrial spies, or foreign intelligence.
- **Viruses and other malicious software.** Viruses, worms, and other malicious software can enter a network through borrowed diskettes, prepackaged software, and connections to other networks.[4] These hazards could also be *a result of* human error (negligence), insiders, or intruders.

SAFEGUARDS FOR NETWORKED INFORMATION

Federal agencies and other organizations use *safeguards-countermeasures-that* eliminate specific vulnerabilities or otherwise render a threat impotent, thereby protecting the organizations' information assets. In this report, *security is* used generally to describe the protection against disclo-

---

[1] This is consistent with other areas of engineering as well; notable examples include the Chernobyl nuclear disaster, the Bhopal chemical plant disaster, and the Exxon Valdez oil spill. Charles Cresson Wood and William W. Banks, "Human Error: An Overlooked but Significant Information Security Problem," *Computers and Security*, vol. 12, No. 1, pp.51 -60. Another analysis of information systems conducted over 12 years in 2,000 organizations found human error the cause of 65 percent of total security losses. See United Nations, Advisory Committee for the Coordination of Information Systems (ACCIS), *Information Systems Security Guidelines for the United Nations Organizations (New* York, NY: United Nations, 1992), p. 9.

[2] The United Nations report estimated that 19 percent of total security losses were from dishonest ordisgruntled employees, 13 percent were from infrastructure loss or water damage, and 3 percent were from outsiders. Viruses were not listed. (Ibid.)

[3] "Crackers"' are often called "hackers," but "hacker" also refers to a broader set of individuals who innovate legitimate solutions to computer challenges.

[4] Experts differ over the actual losses and relative importance of viruses compared with other threats. See testimony by Peter S. Tippett, Symantec Corp., and material submitted for the record by Cynthia Carlson, USA Research, in hearings before the House Subcommittee on Telecommunications and Finance, June 9, 1993. One study estimated that viruses account for roughly 2 percent of all losses. See James Lipshultz, "Scare Tactics Exaggerate Actual Threat from Computer Viruses," *Federal Computer Week, Dec. 6, 1993,* p. 15.

sure, modification, or destruction of networked information through the use of safeguards. These safeguards include hardware, software, physical controls, user procedures, administrative procedures, and management and personnel controls. The degree of security, along with the safety and reliability of a system, is reflected in the level of confidence that the system will do what it is expected to do-that is, its trustworthiness.

This report loosely defines an *information network* as any set of interconnected electronic information systems (computers, magnetic drives, telecommunications switches, etc.); therefore, a "network" is not restricted to the Internet,[5] corporate networks, the telephone network, and so forth. In any case, today's networks are increasingly interconnected or overlapping, and distinctions are difficult to make. In this report, a network *user* may refer to a nonexpert individual, an expert system administrator, or an entire organization, depending on the context.

Expressing Organizational Objectives

To be successful, safeguards must be applied in a coordinated fashion to contain the risks from the above threats, while maintaining the functional objectives of the network.[6] To implement such safeguards, professionals can use a top-down and ongoing process that is based on the objectives and design of each particular network. Alternatively, many managers and users attempt to protect information through more *ad hoc* applications of products and services that sometimes lack even an informal consideration of an overall process. While such an informal approach maybe adequate for some small networks, it can put the information in other networks at great risk.

The single most important step toward implementing proper safeguards for networked information in a federal agency or other organization is for its top management to define the organization overall objectives, define an organizational security policy to reflect those objectives, and implement that policy. Only top management can consolidate the consensus and apply the resources necessary to effectively protect networked information. For the federal government, this requires guidance from the Office of Management and Budget (OMB), commitment from top agency management, and oversight by Congress. Without understanding and support from top management, an organization's deployment of safeguards may be completely ineffective.

Reflecting their organizational objectives, different types of network providers and users em–

[5] The Internet is defined here as many thousands of interconnected smaller networks that use the Internet Protocol (1P) format to exchange data. In practice, the degree to which a network is part of the Internet varies, and formats other than IP are also sent over the Internet or used within subnetworks. The Internet is prominent because of its size and rate of expansion, and its decentralized management and financing.

[6] For information on the many aspects of information security discussed in this chapter, see William Caelli, Dennis Longley, and Michael Shain (eds.), *Information Security Handbook (New* York, NY: Stockton Press, 199 I); Knsh Bhaskar, *Computer Security: Threats and Countermeasures* (Oxford, England NCC Blackwell, Ltd., 1993), Deborah Russell and G.T. Gangemi, Sr., *Computer Security Basics* (Sebastopol, CA ()' Reilley & Associates, Inc., 1991): Morrie Gasser, *Building a Secure Computer System* (New York, NY. Van Nostrand Reinhold Co., 1988); National Research Council, *Computers at Risk: Safe Computing In the Information Age* (Washington, DC: National Academy Press, 1991); U.S. Department of Commerce, National Institute of Standards and Technology, "Workshop in Security Procedures for the Interchange of Electronic Documents: Selected Papers and Results," Roy G. Saltman (ed.), August 1993; and U. S. Congress, Office of Technology Assessment, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*, OTA-CIT-3 10 (Wash ington, DC: U.S. Government Printing Office, October 1987). See also U.S. Department of Commerce, National Institute of Standards and Technology, *An Introduction to Computer Security: The NIST Handbook*, in press.

phasize different security aspects or services.[7] Long-distance (interexchange) earners, local telephone companies, cable companies, satellite providers, wireless carriers, and other providers of the telecommunications links generally place the most emphasis on the *availability* of their services. Availability means that core services will be operational despite threats of fire, flood, software errors, undercapacity, virus attacks, and so forth.

Building on the links are value-added providers, some resellers, computer network services, and others who use the links to transport information, but also add features of their own. Commercial Internet providers primarily emphasize availability, while electronic data interchange (EDI) value-added services emphasize *integrity* and *nonrepudiation.* Integrity means that the information is only altered from its original form and content for authorized reasons.[8] (Banks, for example, are particularly concerned about the integrity of electronic funds transfers.) Non-repudiation refers to the ability to prove that a party sent a particular message (see discussion in chapter 3). Subscription services, such as CompuServe, America Online, Genie, Delphi, and Prodigy, also emphasize *access control.* Access control refers to mechanisms based on user-identification and user-authentication procedures that restrict each user to reading, writing, or executing only the information or functions for which he or she is authorized.

At the periphery-but no less important-are the users: individuals, government agencies, banks, schools, libraries, database services, corporations, citizen groups, managers of electronic bulletin boards, and others. Users are both providers and consumers of information; they may have little control over the overall availability of the links, but they can control other aspects. Users can assure the *confidentiality* of classified, proprietary, or private information through the use of cryptography (see box 4-1) and access controls. Confidentiality refers to the assurance that only properly authorized persons can view particular information. Online publishers and corporations may use cryptography and access controls to emphasize the protection of copyrighted or proprietary information--i.e., assuring that two parties have properly exchanged payments or permissions for services or products delivered electronically.

Confidentiality is distinguished here from *privacy, which* is less commonly used in the computer security profession. Briefly, confidentiality refers to the treatment of data; confidentiality is achieved "when designated information is not disseminated beyond a community of authorized knowers." Privacy refers here to a social contract: "the balance struck by society between an individual's right to keep information confidential and the societal benefit derived from sharing that information. . . ."[9] (See chapter 3 for discussion of privacy.)

---

[7] Computer security is often said t. have three primary aspects (defined in the text): confidentiality, integrity, and availability (the "CIA" of security). Historically there has been greater emphasis on confidentiality and integrity, and less on availability. The international Standards Organization (1S0) 7498-2 international standard also distinguishes nonrepudiation and access controls, but most references subsume these and all other attributes into the first three. Dorm Parker has suggested including other aspects; see Dorm B. Parker, SRI International, Menlo Park, CA, "Using Threats To Demonstrate the Elements of Information Security," January 1994 (obtained from the author).

[8] Another definition is that "Integrity is the knowledge that a given body of data, a system, an individual, a network, a message in transit through a network, or the like has the properties that were a *priori* expected of it. " (Willis H. Ware, Rand Corporation, Santa Monica, CA, "Policy Considerations for Data Networks," December 1993.)

[9] Anita Allen, *Uneasy Access: Privacy for Women in a Free Society* (Totowa, NJ: Rowman & Littlefield, 1988), p. 24. See discussion in U.S. Congress, Office of Technology Assessment, *Protecting Privacy in Computerized Medical Information, OTA-TCT-576* (Washington, DC: U.S. Government Printing Office, 1993), pp. 7-9

Writing an Organizational Security Policy

The *security policy* of an agency or other organization is intended to implement the overall objectives, express the organization's view on risk, and assign responsibilities, among other things .'" Whether implicit or explicit, the policy is essential to define the requisite safeguards: "Without a security policy, it could be argued that it isn't possible to have a security violation. The business has nothing defined as confidential [for example] and no standards to meet."[11] In an organization, a successful security policy is made by the top management—a chief executive officer or agency head, for example. In cooperative networks, the policy may be made by representatives of its members, standards committees, regulatory bodies, or by law.

Organizational security policies range from one page to several volumes in length, but should not be overly specific. As one observer noted, "security policies are not unlike the Ten Commandments or the Bill of Rights. They must not include the specifics of the implementations. They are far more effective if they are brief, generic, and forceful."[12]

As any user, the federal government must examine its own objectives, set its own security and privacy policies, and continually review its own information safeguards.[13] Just as different users and providers have conflicting interests, however, so do different federal agencies have conflicting missions and policies. The pressure to make government more efficient, in particular, often complicates the need to protect copyrighted, private, and proprietary information. For example, improving federal services to citizens, including electronic delivery of those services, will require more sharing of information and resources among agencies and between federal agencies and state or local agencies.[14]

Agencies historically have delivered their services in a "stovepipe" fashion—managing services vertically within an agency but not horizontally across agency boundaries. This isolation between agencies provided a degree of privacy simply due to the difficulty of consolidating such information using existing methods. Information networks make horizontal exchanges of information between low-level agency employees much easier, but sharing such information also brings new risks since different agencies (and nonfederal government users) have different objectives and policies about handling such information. Agencies and other organizations will have to work together to assure that sensitive information is handled uniformly according to privacy and computer matching laws (see chapter 3).

There is a great need for agencies and other organizations to develop sound security policies that match the reality of modem information networks. These policies should be mandated from the highest level. They should support the specific organizational objectives and interests, including

---

10 *Security policy* refers here 1, the statements made by organizations, corporations, and agencies to establish overall policy on information access and safeguards. Another meaning comes from the Defense community and refers to the rules relating clearances of users to classification of information. In another usage, *security policies* are used to refine and implement the broader, organizational security policy described here.

11 Paul Dorey, "Security Management and Policy," in *Information Security Handbook*, William Caelli, Dennis Longley, and Michael Shain (eds.) (New York, NY Stockton Press, 1991), p. 32.

12 Robert H. Courtney, 'r' President, RCI, Inc., Lynn Haven, FL, personal communication, June 2, 1994.

13 For discussion, see Dennis M. Gilbert, A *Study of Federal Agency Needs for Information Technology Security*, NISTIR-5424 (GaiLhersburg, MD National Institute of Standards and Technology, May 1994).

14 U.S. Congress, Office of Technology **Assessment,** *Making Government Work: Electronic Delivery of Federal Services*, OTA-TCT-578 (Wash ington, DC: U.S. Government Printing Office, Sept. *1993).* Vice president Al Gore, *Creating a Government That Works Better and Costs /e\\: Report o/ the National Performance Review* (Washington DC: U.S. Government Printing Office, Sept. 7, 1993); U.S. General Services Administration, Information Resources Management Service, "Service to the Citizens: Project Report," KAP-93- 1, February 1993.

but not limited to policies regarding private information. These policies must also anticipate a future where more information may be shared among agencies and organizations.

Cost-Justifying Safeguards

Ideally, the actual safeguards implemented to protect networked information should represent the overall objectives of the organization, but in practice they often do not. Network designers must continually balance utility (including speed, capacity, flexibility, user-friendliness, and interoperability), cost, and security. In any case, information can never be *absolutely* secured, and safeguarding information is therefore not an issue of *how* to secure information, but *how much* security an agency or business can justify. Many approaches are effective and inexpensive, but others can be very costly, for both small and large organizations. The organization's management, therefore, must have a method to balance the cost of a safeguard with the potential loss that may occur if it doesn't use that safeguard.

Security professionals can use *risk analyses* to estimate risks [15] and probable losses for information assets. These analyses can then be used to determine the appropriate safeguard expenditures. A crude qualitative risk analysis may simply identify the obvious holes in a system but can, nevertheless, be valuable. A rigorous quantitative analysis requires some experience with security systems and understanding of how to determine the value of information assets.

Management benefits from risk analyses only insofar as an analysis provides timely, quantifiable, and credible measurements. In practice, however, risk often can be difficult to quantify and the analysis expensive. Quantification requires statistics about the frequency and size of losses in similar organizations. Such statistics may be difficult to obtain, and the frequencies of losses may be too low to be useful or may not be applicable to a particular organization. Incidents of loss are widely underreported or undetected. The discipline of risk analysis also is still relatively young and needs further development.

Therefore, a risk analysis does not necessarily assure that a system is effectively safeguarded, only that the organization is following a systematic approach. New developments in risk analysis have made the process easier, however, relying on past experience and on automated tools with extensive threat, vulnerability, and safeguard knowledge bases, and user-friendly interfaces. Risk analysis performs best where the nature of losses are best understood or frequent—such as in cases of natural disasters or credit card fraud. Its shortcomings lie in cases where the losses are less understood.

Alternatively, management can use a *due care* (also called *reasonable care)* approach to determine how much security an organization can afford. A due care approach seeks an acceptable level of safeguards *relative to other businesses and agencies,* as opposed to an acceptable level *relative to an absolute measure of risk.* This approach uses "baseline" controls and practices, as well as risk analyses for vulnerabilities not addressed by the baseline. The baseline varies depending on the application or industry; for example, the baseline for the banking industry would be different from that of an information publisher. The baseline is also intended to be flexible and incorporate changes in technology. The due care approach is intended to build on the experience of others in the field and, therefore, to lower the cost of managing networked information.

The due care approach to safeguarding information assets is not well established, however, and has relatively little precedent or experience to

---

[15] *Risk* is the likelihood that a particular threat will exploit a particular vulnerability to cause an undesirable event to occur—a measure of uncertainty. It is sometimes defined as the asset value multiplied by the exposure factor (fraction of the asset destroyed in an event) and the annualized rate of occurrence. Using this definition, risk can be expressed in units of dollars per year. (Will Ozier, Ozier, Peterse, and Associates, San Francisco, CA, personal communication, Dec. 14, 1993.)

build on. The establishment of *generally accepted principles* (explained in a later section) is integral to providing standards for due care, but detailed principles will take some time to develop. Critics claim that following only the due care principles can provide inadequate safeguards and may therefore fail as a liability defense. Even within one industry such as banking, for example, safeguard needs vary greatly from one location to another, and appropriate safeguards change as technology changes. Taking a follow-the-leader approach may cause the organization to overlook reasonably available safeguards, suffer a significant loss, and be found negligent, even though it was following otherwise-accepted procedures.

Both risk analysis and principles of due care need further development. Neither approach is necessarily always appropriate and, therefore, neither is always sufficient to provide a strong defense against liability in the case of a monetary loss related to loss, theft, or exposure of networked information. A combination of the two approaches will likely provide improved protection. Proponents of risk analysis suggest that risk analysis done correctly provides better safeguards, while proponents of due care suggest that performing only risk analyses is impractical.

Formal Security Models

Given a particular set of objectives and a stated organizational policy, a formal model is sometimes developed to express or formalize a more specific policy in a way that can be tested in a system. The model should be written in precise, simple, and generic terminology and, therefore, is often written in mathematical notation, particularly for systems requiring relatively strong safeguards.[16] A specification process is derived from the model and provides a step-by-step method to assure that the model is actually implemented. The formal process thus provides a series of steps that can be isolated and tested.

An example of a well-known security model is the Bell-LaPadula model used for protecting the confidentiality of classified information, based on multilevel security classifications. [17] The Clark-Wilson model is a less formal model aimed at financial and other unclassified transactions. The Clark-Wilson model implements traditional accounting controls including segregation of duties, auditing, and well-formed transactions such as double-entry bookkeeping.[18]

Most of the existing work in formal security models is oriented toward confidentiality in classified applications. This emphasis may be because only the Department of Defense (DOD) classification hierarchy and requirements for high assurance of security seem to be amenable to formal models. Comparable security models for unclassified information, with emphasis on integrity and availability have not, and may never, emerge. Some claim that the private sector can simply provide better safeguards without the need for forma] models characteristic of the DOD approach.

Within the government sector, research in security models may be appropriate for applications involving the exchange of sensitive or private information among federal agencies, or between federal agencies and state or local governments. These models then could be applied to assure conformance to security and privacy policies that have been coordinated among those agencies that share information. Especially needed are models that address heterogeneous network environments and that are integrated with other systems approaches that account for network reliability and fault-tolerant computing.

16 This mathematical notation is analogous to the role of Boolean algebra in expressing electronic circuits that perform logical functions.

17 The *Biba model* is similar to the Bell-LaPadula model but protects the *integrity* of information instead of its *confidentiality*. The rigor of the Biba model, however, is not generally a good match for real world integrity requirements and is rarely implemented.

18 For a discussion of formal models, see Morrie Gasser, op. cit., footnote 6, ch. 9. See also Dennis Longley, "Formal Models of Secure Systems," in *Information Security Handbook*, op. cit., footnote 6.

Before formal models can be successful for safeguarding the exchange and sharing of information among agencies, the agencies must first review and coordinate their individual policies regarding the protection of sensitive or private information (see discussion of data sharing in chapter 3). These policies could then be implemented according to new or existing formal models, as needed. The Office of Technology Assessment (OTA) found in its interviews, however, that while exploration into new types of formal models may be warranted, there is considerable doubt about the utility of formal models for safeguarding networked information, particularly to protect information integrity and availability.

Specific Safeguard Techniques and Tools

The marketplace provides products and services that range from simple devices such as a metal key used to shut off a personal computer at night, to elaborate methods for encryption and digital signatures. The tools and techniques alone will not safeguard an organization's information; they require expert personnel to apply and maintain them. They also must be combined in a coordinated fashion to meet the organization's objectives, whether they emphasize confidentiality, integrity, availability, or any other attributes of security. A few classes of techniques and tools are listed here as examples of features that are currently available.[19]

Challenge-Response Systems

Even small networks require users to identify themselves through a user name and a confidential password. These passwords are usually stored in an encrypted file in a central computer, and few people or perhaps no one has the key to the file that contains the passwords. An intruder might guess a password by trial and error, however, using typical passwords such as names, nicknames, names of spouses or children, and so forth (see box 2-1). An intruder might also monitor and copy passwords that are sent to the central computer as the user logs on, or that are written on scraps of paper left near the user's computer.

This latter type of attack can be deterred by "challenge-response" systems that never actually send the password over the network. When the user enters his or her account name at a terminal, the central computer issues the user a random challenge. The user sees the challenge, and transcribes it and a password into the keypad of a handheld authenticator (the size of a credit card or small calculator). The authenticator calculates a unique response; the user enters that response into the terminal and sends it to the central computer. The central computer repeats the calculation and compares its result with the user's result. An intruder cannot imitate the user without access to the identical authenticator and its associated password.

Secure tokens (see below) or a laptop computer can also substitute for the authenticator. Also, the user's token can generate a response based on a card-unique secret key and the local time (synchronized with the central computer), instead of the challenge sent by the central computer.

---

19 For an overview of information security and related products and techniques, see Deborah Russell and G.T. Gangemi, Sr., op. cit., footnote 6. For techniques relating to only UNIX, see Simson Garfinkel and Gene Spafford, *Practical UNIX Security* (Sebastopol, CA: O'Reilly & Associates, Inc., August 1993). For an introduction to network security, see Mario Devargas, *Network Security* (Manchester, England: NCC Blackwell Ltd., 1993). See also Teresa F. Lunt (cd.), *Research Directions in Database Security (New* York, NY: Springer-Verlag, 1992); and D.W. Davies and W.L. Price, *Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer,* 2nd Ed. (New York, NY: John Wiley & Sons, 1992).

BOX 2-1: Weak Passwords

Perhaps the most widespread and serious vulnerability in information networks is the use of weak password systems Systems administrators can no longer safely send unencrypted passwords over the Internet and other networks Instead, experts recommend that network managers use challenge-response systems, electronic tokens, and sophisticated, one-time password techniques to protect their networks Users will continue to employ traditional passwords, however, to protect "local" workstations and files Unfortunately, passwords assigned by administrators to protect these local assets are often "strong" but easily forgotten, while passwords chosen by users are more easily remembered but often "weak "

For example, an eight character password has 2^{56} (over 72,000,000,000,000,000) possible combinations (counting both uppercase and lowercase characters and symbols, and eight bits per ASCII character, less one bit for parity) An intruder who has copied an encrypted file might need hundreds of years to try all these possible combinations in sequence in order to decrypt the file Users who choose words, proper names, or acronyms for passwords reduce considerably the number of possible combinations that an intruder needs to try there are less than 500,000 English words and names with eight or fewer letters, spelled backwards or forwards Of these words, some are more frequently chosen for users' passwords than others An intruder who guesses a few dozen or a few hundred of the most common names, acronyms, and default passwords is often successful

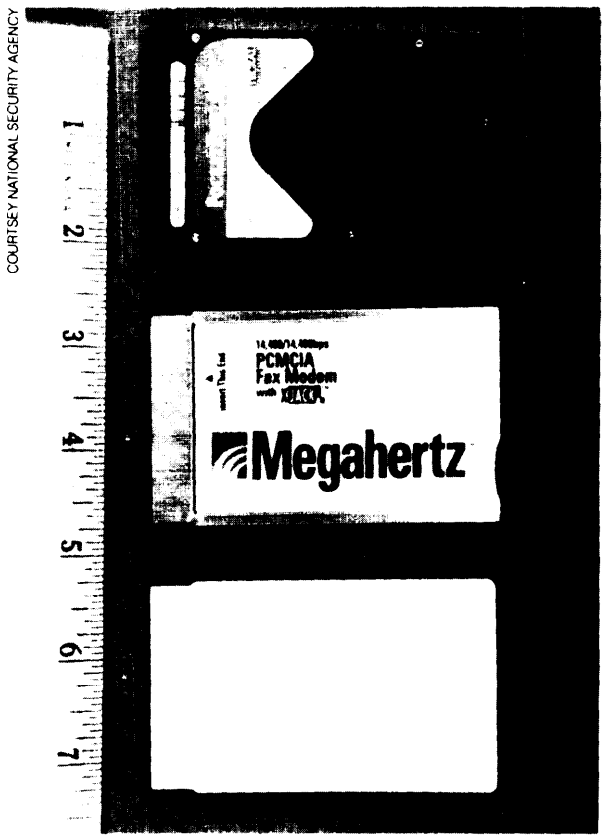
Educating users to choose strong passwords to protect local workstations is perhaps the most difficult task for a network manager Programs exist that screen out weak passwords, but such programs do not substitute for the following simple guidance to users

- Treat your password like your toothbrush use it every day, change it often, and never share it [1]
- Never write your password on anything near your computer If you do write it down, do not Identify it as a password, and hide it well Never place an unencrypted password in the text of an electronic message or store it unencrypted in a file on the network
- Never use the default password (the password assigned from the factory)
- Avoid proper names, nicknames, or full words for passwords---even spelled backwards Do not repeat a password that you have used before
- Do use long, unpronounceable acronyms, such as the first letters of an unfamiliar song or phrase, or an obscure word with vowels omitted For example, an eight-letter password could be *TNPLHTOT* derived from "There's no place like home, Toto, " although a more personal phrase is better
- Do use passwords with numbers or special characters inserted Using the last example, an eight letter password could be TNPL9H&T
- Do use nonsensical but pronounceable words, for example, *SKRODRA8* (NIST has specified an algorithm that uses a random number to generate pronounceable passwords 2,
- Do consider using an electronic token, a challenge-response system, a biometric device, or other technique that better identifies the user Consider using a "three strikes and you're out" system for communications links, such as is used in automated teller machines Remove unused accounts whenever possible.

[1] Attributed to Clifford Stoll, author of *The* Cuckoos Egg, *Tracing a Spy Through the Maze of Computer Espionage (New* York, NY Doubleday 1989)

[2] U S Department of Commerce, National Institute of Standards and Technology, 'Automated Password Generator, " FIPS PUB 181 (Springfield VA National Technical Information Services, October 1993)

SOURCE Office of Technology Assessment, 1994



COURTESY NATIONAL SECURITY AGENCY

From bottom to top PCMCIA card, PCMCIA card with fax modem,PCMCIA card with hard *disk.*

Secure Tokens

Smart cards,[20] PCMCIA cards,[21] SmartDisks,[22] and other secure tokens are devices used to authenticate a user to a computer. In an access control system, the user must insert the token into a reader connected to a computer, which may be connected to a network. The token then obtains access on behalf of the user (to a remote computer, for example) by providing the necessary authorizations and confirming the user's identity.

The token can read and verify digital signatures from the computer so that the card will not be fooled into giving away sensitive information to a computer acting as an impostor. The token also can send its own encrypted digital signature so that the computer knows that the token is not an imitation. No intruder can obtain access to the computer without the token *and* knowledge of secret information needed to activate the token (for example, a password).

The PCMCIA card is slightly larger than a credit card but with a connector on one end, and plugs directly into a standard slot in the computer. The card has a microprocessor chip embedded inside that performs the sophisticated authentication features. Other types of PCMCIA cards can be used to provide extra and portable memory capacity and to provide communications capability. As new computer models include slots for PCMCIA cards, their use as secure tokens appears promising.

Other technologies perform similar functions in different forms. Smart cards are plastic cards the size of bank cards that have a microprocessor chip embedded in the plastic, sometimes with a magnetic stripe also on the back. The SmartDisk is a token in the shape of a 3.5-inch diameter magnetic disk with a connectionless interface that communicates with the disk drive head.

Firewalls

Individual workstations usually vary greatly within an organization's network. Because of this variation and difficulties managing each workstation, it is difficult to safeguard individual workstations from intrusions from outside the network. A *firewall* provides a focus for managing network safeguards by restricting communication into and out

---

20 U.S. Department of Commerce, National Institute of Standards and Technology, *Smart Card Technology: New Methods for Computer Access Control*, NIST Spec. Pub. 500-147 (Gaithersburg, MD: N] ST, September 1988). See also Jerome Svigals, "Smart Cards—A Security Assessment," *Computers & Security, vol.* 13 (1994), pp. 107- I 14.

21 PCMCIA stands for Personal Computer Memory Card Industry Association. The National Security Agency's TESSERA Card uses a PCMCIA interface, with a Capstone chip inside the card. Capstone and the Escrowed Encryption Standard are discussed in box 2-6 and in chapter 4.

22 "SmartDisk" is a trademark of SmartDiskette, Ltd.

of the network. The firewall itself is a dedicated computer that examines and restricts mainly incoming, but sometimes outgoing, communications.[23]

The form of the firewall restriction maybe simple; for example, electronic mail may be allowed while other services are not. Or the restriction may be more elaborate, perhaps requiring individual user authentication as a prerequisite for communication through the firewall. Firewalls are particularly important for networks connected to the Internet, to assure that computers on a smaller network are less vulnerable to intruders from the much larger Internet.[24]

Virus Checkers

Virus checkers are software programs that automatically search a computer files for known viruses (for an explanation of viruses and other malicious software, see box 2-2). The checker scans files every time the computer is turned on or when new memory disks are inserted into the computer. The virus checker looks for patterns of code that resemble the code used in known viruses, and alerts the user when it finds a resemblance.[25] Since new viruses are discovered every month, virus checkers must be updated often, although many viruses cause no damage or are not relevant to most users.

Auditing and Intrusion Detection

Auditing is the act of automatically monitoring certain transactions that occur in a network over a period of time. Such transactions include transfers of files, and the local time when a user accesses the network. Auditing features on a network can quickly generate volumes of information about network use, however, that can overwhelm busy security personnel. Auditing, therefore, is often a passive activity where records are only kept for later examination. It is also a passive deterrent to authorized users who might fear getting caught should an investigation arise.

Integrated, dynamic auditing systems not only record information, but also act to restrict use or to alert security personnel when possible safeguard violations occur—not just violations from intruders but also from insiders. One feature might alert security personnel if users are accessing certain files after hours or if a user (or possible intruder) repeatedly but unsuccessfully attempts to access a certain computer. The securit y officer might then closely monitor the user actions to determine what further actions should be taken (simply denying access might alert an intruder to use a more reliable or more covert method, confounding the security staff). Some sophisticated systems use expert systems that "learn" users' behavior.[26]

Encryption, Electronic Mail, and Digital Signatures

Encryption is used for a variety of applications, including the protection of confidentiality and integrity, authentication, and nonrepudiation. Different methods are used to assure these properties,

[23] An information firewall is in this way like an airlock that eliminates a direct connection between two environments. The label *firewall* is misleading since firewalls used in buildings are intended to stop all fires; network firewalls monitor (mostly incoming) traffic while generally allowing most of it through.

[24] Steven M. Bellovin and William R. Cheswick, *Firewalls and Internet Security: Repelling the Wdey Hacker* (Reading, MA. Addison-Wesley, 1994). See also Frederick M. Avolio, "'Building Internetwork Fireballs,'' lousiness *Communications Review*, January 1994, pp. 15-19.

[25] Some viruses mutate every time they replicate, however, making programs that scan for a specific virus code less effective.

[26] See Dorothy E. Denning, "An intrusion-Detection Model, " *IEEE Transactions on Software Engineering*, SE-13, February 1987, pp. 222-232; Susan Kerr, "Using AI [Artificial Intelligence] To [reprove Security, " *Datamation*, Feb. 1, 1990, pp. 57-60; and Teresa F. Lunt et al., "A Real-Time Intrusion-Detection Expert System," final technical report, SRI International, Feb. 28, 1992.

BOX 2-2: Viruses, Worms, and How To Avoid Them

The term virus is popularly used for any malicious software or so-called rogue program that can enter a computer and cause damage. ' A true virus is a fragment of a program that replicates itself and modifies ("infects") other programs A worm, on the other hand, is an independent program that moves through a system and alters its operation, but does not infect other programs, Viruses and worms can use techniques such as "logic bombs" and "Trojan horses" to disguise their function. A logic bomb, for example, is triggered to perform an action when a certain event or condition occurs, such as on Friday the 13th. A Trojan horse tricks a user into using a desirable function so that it can perform some other function, such as recording passwords,

What do viruses do that users should worry about? The possibilities for damage are only limited by the imagination of those who create the viruses Types of virus damage include changing the data in files, changing file attributes so that others can access confidential files, filling up computer memory with meaningless data, changing internal addressing so that the user cannot access files, displaying obscene messages on the screen or in printouts, slowing down the computer, and changing the initialization program for the computer so that it cannot operate, Managers must often rely on users to follow good practices, such as the following, to keep networks clean

- Do check all Incoming software and computer diskettes with an up-to-date virus checker program (even including off-the-shelf software from reputable sources)
- Do backup all files frequently so that in case of a virus attack, the original uninfected files are still accessible Do check all files with the virus checker program before reinstalling them
- Do consider protecting software from Trojan horses by only allowing read-only access by all users except the system administrator.
- Do be wary of publicly available and free software, software borrowed from others, or software without the original packaging Do not use pirated software

[1] See Philip E Fites, Peter Johnson, and Martin Katz, *The Computer Virus Crisis* (New York, NY Van Nostrand Reinhold, 1992) See also Lance J Hoffman (ed), *Rogue Programs Viruses Worms, and Trojan Horses* (New York, NY Van Nostrand Reinhold, 1990), Peter J Denning (ed), *Computers UnderAttack Intruders, Worms, and Viruses* (New York, NY Addison Wesley, 1990), and John B Bowles and Colón E Peláez, "Bad Code, " and other articles in *IEEE Spectrum*, August 1992, pp 36-40, and Jeffery O Kephart et al , "Computers and Epidemiology," *IEEE Spectrum*, May 1993, pp 20-26

SOURCE Off Ice of Technology Assessment, 1994, and sources referenced below

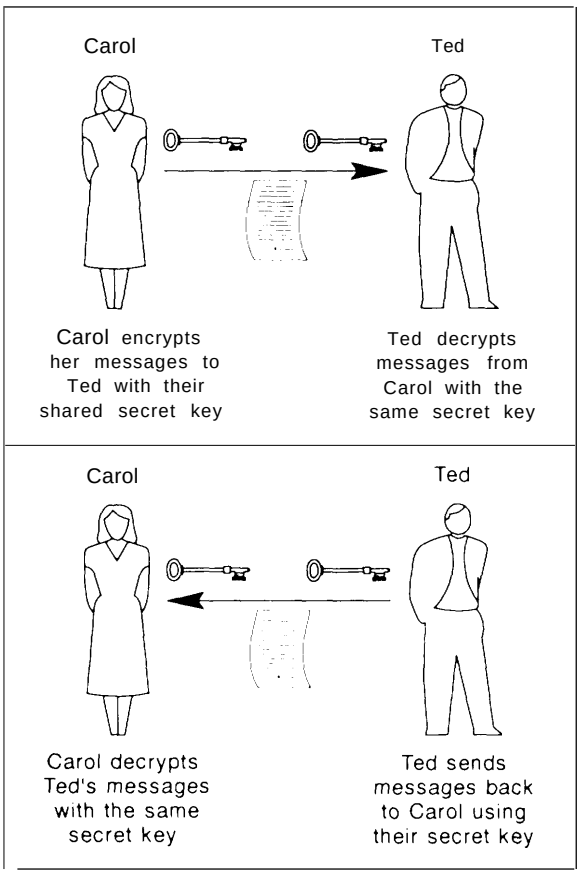
and each method has its strengths and weaknesses. These different methods can be integrated to provide multiple safeguards (see box 2-3).[27]

One widely used network application is electronic mail (email). Large and small networks can transfer electronic mail messages from workstation to workstation, holding the message for the addressee until he or she accesses it on a computer. Historically, electronic mail has not used encryption to protect the confidentiality of the message contents. PEM--or Privacy-Enhanced Mail—is a specific set of proposed standards that specifies how to encrypt the contents of electronic mail messages for the Internet.[28] Unauthorized users cannot read a PEM encrypted message even if

27 For a short description of better known algorithms, see Bruce Schneier, "A Taxonomy of Encryption Algorithms," *Computer Security Journal, vol. IX, No.* 1, p. 39.

28 Stephen T. Kent, "Internet Privacy Enhanced Mail," *Communications of the ACM*, vol. 36, *No. 8, August* 1993, p. @59.

FIGURE 2-1: Secret-Key (Symmetric) Encryption



NOTE Security depends on the secrecy of the shared key

they were to obtain access to it. PEM can also digitally "sign" the message to authenticate the sender. Although PEM can protect the confidentiality of the message, it cannot protect the confidentiality of the address, since that information must be understood by network providers in order to send the message. Privacy-enhanced mail requires that both the sender and the receiver of the electronic mail message have interoperable software programs that can encrypt and decrypt the message, and sign and verify the digital signature. Therefore, widespread adoption is still far off.

Biometric Devices

Access-control systems can use three methods to identify a particular user: something the user knows (e.g., a password), something the user has in his or her possession (e.g., a secure token), or something that physically characterizes the user. This last method is known as *biometrics.* Characteristics that might be analyzed by biometric devices include retinal scans of the eye, fingerprints, handprints, voice "prints," signature dynamics, and the typing of keystroke patterns.[29]

Biometric devices can be effective in many cases, but are expected to be less effective for protecting networked information due to their generally higher cost. Biometric signatures also can be intercepted and imitated, just as unchanging passwords can, unless encryption or an unpredictable challenge is used (see the discussions above).

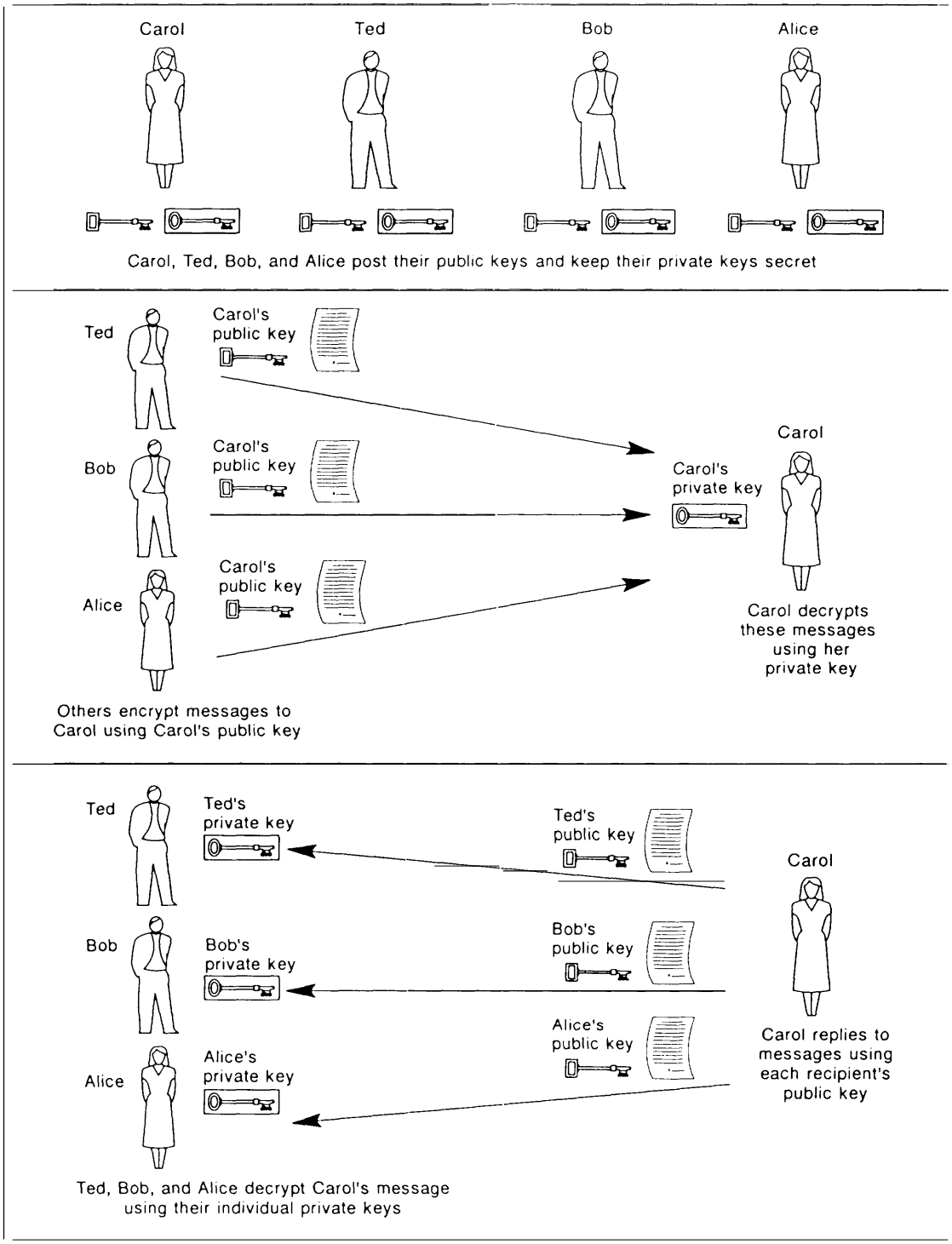
Separation of Duties

Safeguards need not be based in only hardware or software. They can also include administrative and other procedures like those used in accounting practices. As only one example, the authority and capacity to perform certain functions to networked information should be separated and delegated to different individuals. This principle is often applied to split the authority to write and approve monetary transactions between two people. It can also be applied to separate the authority to add users to a system and other system administrator duties from the authority to assign passwords, review audits, and perform other security administrator duties. The separation of duties principle is related to the "least privilege" principle, that is, that users and processes in a system should have least number of privileges and for the minimal period of time necessary to perform their assigned tasks.

Wiretap laws apply the separation of duties principle by requiring the law-enforcement agency that conducts a wiretap (in the executive branch), to obtain permission from a court (in the

[29] Benjamin Miller, "Vital Signs of Identity," *IEEE Spectrum, vol. 31,* No. 2, February 1994, p. 22.

FIGURE 2-2: Public-Key (Asymmetric) Encryption



NOTE Security depends on the secrecy of the private keys and the authenticity of the public keys

BOX 2-3: How Cryptography Is Used To Protect Information

Different cryptographic methods are used to authenticate users, protect confidentiality, and assure Integrity of messages More than one method usually must be used to secure an overall operation, as described here (see also boxes 4-1 and 4-4). Cryptographic algorithms are either *symmetric* or *asymmetric,* depending on whether or not the same cryptographic key is used for encryption and decry p-tion The key is a sequence of symbols that determines the transformation from unencrypted *plaintext* to encrypted *ciphertext,* and vice versa.

Symmetric cryptosystems—also called secret-key or single-key systems—use the same key to encrypt and decrypt messages (see figure 2-1) The federal Data Encryption Standard (DES) uses a secret-key algorithm Both the sending and receiving parties must know the secret key that they will use to communicate Secret-key algorithms can encrypt and decrypt relatively quickly, but systems that use only secret keys can be difficult to manage because they require a courier, registered mail, or other secure means for distributing keys.

Asymmetric cryptosystems--also called public-key systems—use one key to encrypt and a second, different but mathematically related, key to decrypt messages, The Rivest-Shamir-Adleman (RSA) algorithm is a public-key algorithm. Commonly used public-key systems encrypt relatively slowly, but are useful for digital signatures and for exchanging the session keys that are used for encryption with a faster, symmetric cryptosystem.[1] The initiator needs only to protect the confidentiality and Integrity of his or her private key. The other (public) key can be distributed more freely, but its authenticity must be assured (e g , guaranteed by binding the Identity of the owner to that key)

For example, if an associate sends Carol a message encrypted with Carol's public key, in principle only Carol can decrypt it, because she IS the only one with the correct private key (see figure 2-2) This provides confidentiality and can be used to distribute secret keys, which can then be used to encrypt messages using a faster, symmetric cryptosystem (see box 2-5).

For authentication, if a hypothetical user (Carol) uses her private key to sign messages, her associates can verify her signature using her public key This method authenticates the sender, and can be used with hashing functions (see below) for a *digital signature* that can also check the integrity of the message

Most systems use a combination of the above to provide both confidentiality and authentication

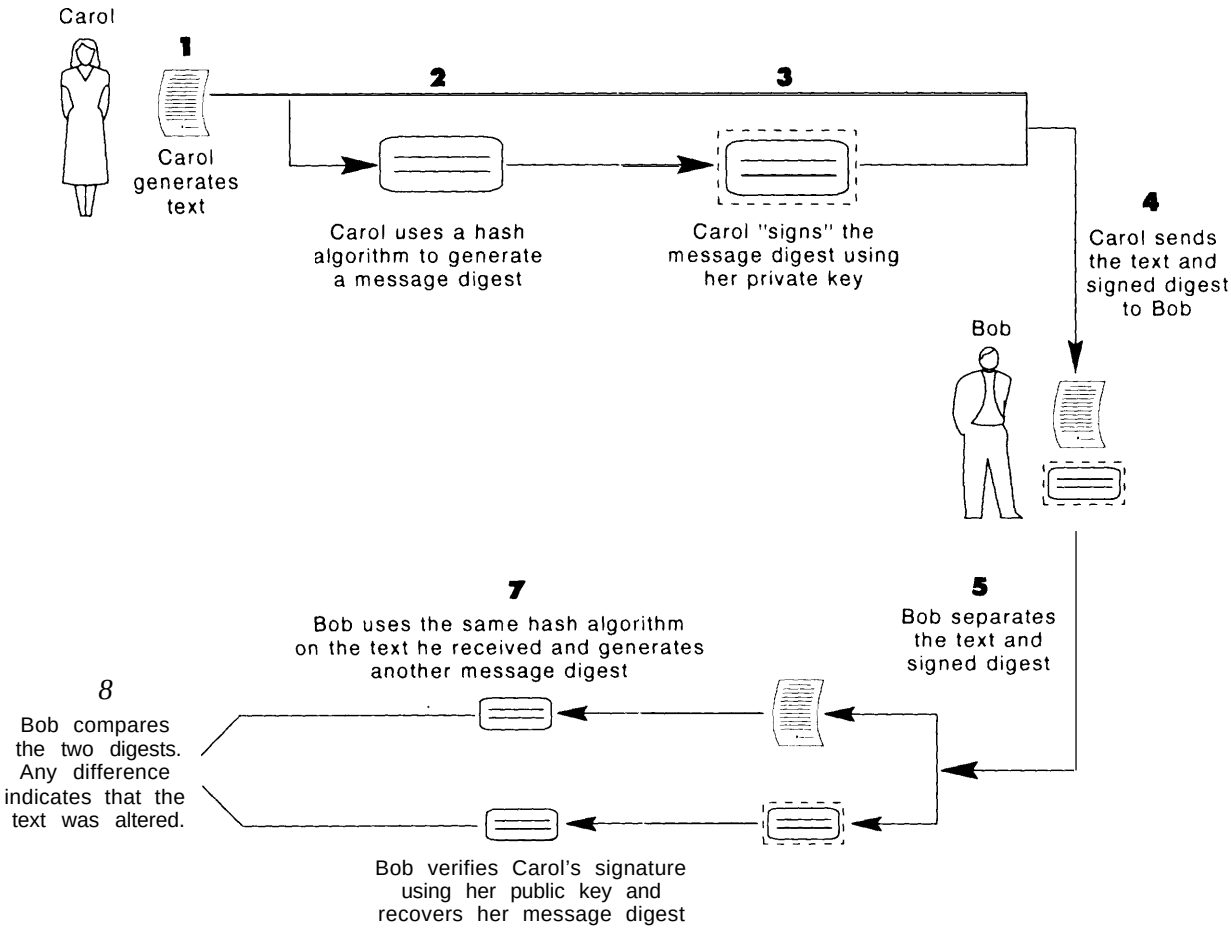
One-way hash functions are used to ensure the integrity of the message-that Is, that it has not been altered For example, Carol processes her message with a "hashing algorithm" that produces a shorter message digest—the equivalent of a very long checksum Because the hashing method is a "one-way" function, the message digest cannot be reversed to obtain the message Bob also processes the received text with the hashing algorithm and compares the resulting message digest with the one Carol signed and sent along with the message If the message was altered in any way during transit, the digests will be different, revealing the alteration (see figure 2-3)

[1] For example, in hardware, the DES is between 1,000 and 10,000 times as fast as the RSA public key algorithm, depending on the implementation In software, the DES is generally at least 100 times as fast as the RSA RSA Laboratories, "Answers to Frequently Asked Questions About Today's Cryptography, " 1993, p 9

SOURCE Off Ice of Technology Assessment, 1994

judicial branch). The Clinton Administration's key-escrowed encryption initiative applies the separation of duties principle in storing escrowed key components with two escrow agents. (The original escrow agents are both in the executive branch—see discussion in chapter 4).

FIGURE 2-3: Example of a Hashing and Digital Signature Scheme



NOTE Different methods for generating and verifying signatures (as in the federal Digital Signature Standard) are possible Measures to protect the signature and text may also be used

In summary, many individual safeguard products and techniques are currently available to adequately address specific vulnerabilities of information networks—provided the user knows what to purchase and can afford and correctly use the product or technique. Easier-to-use, more affordable safeguards are needed. In particular, there is a need for general-purpose products that integrate multiple security features with other functions, for example, electronic commerce or electronic mail.

INSTITUTIONS THAT FACILITATE SAFEGUARDS FOR NETWORKED INFORMATION

The discussion above describes processes and tools that a network manager might use to safeguard a particular network using formal or informal methods. It does not explain how networks are collectively safeguarded through the established marketplace and institutions. Safeguarding

networks collective y amounts essentially to safeguarding the so-called information infrastructure.

An *information infrastructure--for* the purposes of this discussion—is the collective set of computer hardware and soft ware, data storage and generating equipment, abstract information and its applications, trained personnel, and interconnections between all of these components.[30]31 An international information infrastructure already exists; a user in one country can move data that is stored in another country to be used in a computer program in a third country.[32] The infrastructure includes the public-switched telephone network, satellite and wireless networks, private networks, and the Internet and other computer and data networks. The infrastructure is continually and rapidly evolving as technology advances and as users find new applications.

Individuals, corporations, governments, schools and universities, and others own components of the infrastructure, but no one owns or controls it as a whole. Moreover, the numerous stakeholders have diverse and often conflicting goals. The transportation infrastructure is similar: better freeways favor the interests of suburban living and private transportation, for example, but conflict with the interests of inner cities and public transportation.

In particular, very large cooperative networks are too large and diverse to have one explicit policy regarding safeguards; each stakeholder has particular objectives that determine its own explicit or implicit policy. This is true for the Internet, for example; according to Vinton Cerf, President of the Internet Society:

> Among the lessons learned in the two decades of research and development on the Internet is the realization that security is not a uniform requirement in all parts of the system. . . . These needs vary by application and one conclusion is that no single security procedure, policy, or technology can be uniformly applied throughout the Internet environment to meet all its needs.[33 34]

The information infrastructure and its associated safeguards also cannot be built "from the ground up." Instead, the infrastructure must be steered by its stakeholders—including users and the federal government-by strengthening its institutions and assuring that there are adequate

---

30 There is no single accepted definition of an information infrastructure. See also U.S. Congress, Office of Technology Assessment, *Critical Connections: Communication for the Future*, OTA-CIT-407 (Washington, DC: U.S. Government Printing Office, January 1990), and Institute for Information Studies, A *National Information Network: Changing Our Lives in the 21st Century* (Queenstown, MD: The Aspen Institute, 1992).

31 The general infrastructure discussed in [his chapter is distinguished from the Clinton Administration's "National Information Infrastructure" (N]]) *initiative*, which seeks to "promote and support full development of each component [of the infrastructure]." See Information Infrastructure Task Force, *The National Information Infrastructure: Agenda for Action* (Washington, DC: National Telecommunications and Information Administration, Sept. 15, 1993).

32 The European Union faces similar issues and has, therefore, called for the "development of Strategies to enable the free movement of information within the single market while ensuring the security of the use of information systems throughout the Community." See Commission of the European Communities, Directorate General X111: Telecommunications, Information Market and Exploitation of Research, "Green Book on the Security of Information Systems: Draft 4.0," Oct. 18, 1993.

33 Vinton G, Cerf President Internet Society, testimony, *Hearing on Internet Security*, Subcommittee on Science, Committee on Science, Space, and Technology, U.S. House of Representatives, Mar. 22, 1994.

34 The National Institute ~) f Standards and Technology (NIST) proposed a security policy for the National Research and Education Network (NREN), however, where the NREN program was viewed as a steppingstone to development of the broader information infrastructure. The proposed policy was approved by the Federal Networking Council. See Dennis K. Branstad, "NREN Security Issues: Policies and Technologies," *Computer Security Journal*, vol. IX, No. 1, pp. 61-71. See also Arthur E. Oldehoeft, Iowa State University, 'foundations of a Security Policy for Use of the National Research and Educational Network," repro prepared for the National Institute of Standards and Technology (Springfield, VA National Technical Information Service, February 1992).

The NREN is part of the High Performance Computing and Communications program. See U.S. Congress, Office of Technology Assessment, *Advanced Network Technology*, OTA- BP-TCT- 10 1 (Washington, DC: U.S. Government Printing Office, June 1993).

products and services available to users. By strengthening the roles of each of these interdependent institutions, the overall marketplace gains by more than the sum of the parts.

Finally, the overall information infrastructure is not a well-defined or closed system and cannot be strengthened through technical solutions alone. Rather, the infrastructure is changing and growing, and its vulnerabilities are not well understood. The federal government must work together with the many stakeholders to assure robust solutions that will automatically accommodate changes in technology and that can provide feedback for steadily strengthening safeguards overall.

The information infrastructure is already international. Networks like the Internet seamlessly cross national borders. Networked information is also borderless and affects many different stakeholders worldwide. Achieving consensus regarding safeguards among these diverse, international stakeholders is more difficult than achieving technical breakthroughs. Nevertheless, the federal government has the capacity for resolving many of the issues that inhibit or facilitate the use of quality safeguards by diverse communities. These issues are interrelated, however, so solving them piecemeal may not provide an overall solution.

OTA found the following inhibitors and facilitators of safeguards for networked information: management issues (including assigning responsibility, managing risk, and making cost decisions); availability of insurance; vendor and developer issues (including liability and export restrictions); product standards, evaluations, and system certifications and accreditations; professionalism and generally-accepted principles; establishment of public key infrastructure(s); emergency response teams; user education and ethical studies; sanctions and enforcement against violators; regulatory bodies; and research and development. These are discussed below.

Management

Information has become as much of an asset to a business or government agency as buildings, equipment, and people. The information in a corporate database is as crucial to one business, for example, as manufacturing equipment is crucial to another. Once the value of information is recognized, it follows that an organization's management should protect it in the same manner as other corporate or government assets; for example, using risk analyses, contingency plans, and insurance to cover possible losses.

Managers and accountants often do not recognize electronic information as an asset, however, because of its less tangible nature, its relatively recent prominence, and the lack of documentation of monetary losses arising from loss or theft of information. Paper-based information and money can be protected in a safe inside a secured building. Destruction of the building in a fire is a very tangible and easily documented event. In contrast, loss or duplication of electronic information may not even be noticed, much less reported publicly.

The losses that are reported or that reach the public consciousness also do not necessarily represent the overall losses. Until now, most losses in corporate networks arise from human errors and authorized users. Media attention, however, most often highlights virus attacks or teenage and adult "crackers"-- important, but often unrepresentative, sources of lost information, time, and money. Management may perceive that the corporate or agency network is safe from these sensational threats, while ignoring other important threats. Management may also be reluctant to make changes to the network that can cause disruptions in productivity.

BOX 2-4: How Accounting Protects Financial Assets

Accounting practices and Institutions exist to protect traditional assets as information safeguards and institutions protect information assets Modern accounting practices grew out of the catastrophic stock market crash of 1929 and subsequent efforts to avoid government intervention by the Securities and Exchange Commission In the late 1930s, the American Institute of Certified Public Accountants moved to set accounting standards Changes in the financial markets in the 1960s led to the establishment of the Generally Accepted Accounting Principles and other standards

Several parallels exist with the safeguarding of information assets, and also many differences The parallels are summarized below

Comparison of Information Assets With Traditional Assets

	Information assets	Traditional assets
Typical threats	Human error, insiders, natural disasters	Human error, insiders, natural disasters
Management responsibility	Chief Information Officer and Chief *Executive* Officer	Chief Financial Officer and Chief Executive Officer
Education	Computer Science departments	Business schools
Principles	Generally Accepted System Security Principles	Generally Accepted Accounting Principles
Certification	International Information Systems Security Certification Consortium and Institute for Certification of Computer Professionals certifications (in development)	*Certified* Public Accountants

SOURCE Office of Technology Assessment, 1994, and National Research Council, *Computers at Risk Safe Computing in the Information* Age (Washington, DC National Academy Press, 1991), p 280

Experts note that information is never adequately safeguarded unless the responsibility for information assets is placed directly on top management, which can then assign the necessary resources and achieve consensus among diverse participants within the organization. Information security then becomes a financial control feature subject to audit in the same manner as other control functions (see box 2-4).[35] Responsibility often may never be assigned in a particular corporation or agency, however, unless a catastrophe occurs that gains the attention of, for example, stockholders (in a corporation or in the stock market) or Congress (in the federal government). Unfortunately, by that time it is too late to apply safeguards to protect any information that was lost, copied, or damaged.

Insurers and Disaster Recovery Services

Insurance helps spread and manage risk and therefore, in principle, protect an organization's information assets from losses. Insurance policies exist to protect against the loss of availability of networks in a disaster, threats from computer vi-

35 For a description of how information systems are audited and "to assist management in evaluating cost/benefit consideration s," see Institute of Internal Auditors Research Foundation, *Systems Auditability and Control Report* (Orlando, FL: Institute of Internal Auditors, 1991).

ruses, toll fraud, or claims made by a third party as a result of an error made by the organization. Users can also purchase computer disaster recovery services that can restore services in the event that the main computer center is incapacitated. Insurance for information losses does not cover the great majority of security threats, however, including losses arising from human or software errors from within the organization.[36] Organizations must continue to self-insure against monetary losses due to loss, theft, or exposure of networked information, using appropriate safeguards.[37]

To justify a market for broader insurance coverage, risks must be assessable, the losses must be detectable and quantifiable, and the insurer must have confidence that the insured is acting in good faith to report all relevant information and is exercising reasonable care to avoid and mitigate losses. Network security is a dynamic field, however; losses are not necessarily detectable or quantifiable. The standards for due care and concepts of risk analysis for protecting networked information also are not necessarily adequately developed or dependable to allow insurance companies to make underwriting decisions (see earlier discussion).[38] Moreover, insurance companies may seek to protect themselves and price their policies too high, reflecting their uncertainty about the magnitude of losses, as well as their inability to verify the safeguards undertaken.

Insurance companies are most likely to accommodate risks to networked information into policies by modifying traditional coverage, but these risks are not always comparable with traditional risks such as the loss of availability from a natural disaster. Information can be "stolen" without removing it from the premises, for example.

Ideally, broader insurance coverage for information assets may help stabilize the marketplace by forcing policyowners to meet minimum standards of due care or generally accepted principles and to perform risk analyses. The underwriters could audit the policy owners to ensure that they are following such methods. As more companies buy insurance, the standards could become better developed, helping to improve the level of safeguards overall. On the other hand, insurance can also lead policyholders to become less vigilant and accept a level of risk that they would not accept without insurance (the problem of moral hazard). Insurance can also be expensive; investing in personnel and technology may be a better investment for many organizations.

Vendors and Developers

Critics argue that vendors and others who develop information products are primarily responsible for many faults that appear in software or hardware executing in the user's network. With great market pressure to continuously produce new and higher performance software, designing in safeguards and extensive quality testing take a lower priority and may negatively impact functionality, development cost, or compatibility with other products. Software developers sell new software packages with few or no guarantees that the programs are secure or free of undesirable characteristics—some of which are intentionally built-in for various reasons, and some of which are unintentional ("bugs"). Moreover, the customer or client generally must pay for upgraded versions that repair the "bugs" in original versions or add new features such as security. Products are also not necessarily shipped with security features al-

---

36 See National Research Council, op. cit., footnote 6, pp. 174-176.

37 In other areas, self-insurance schemes run the gamut, from the elaborate mechanism of a multinational corporation taking on the role of a health insurer for its employees (thereby avoiding a conventional insurer's profit margin and administrative costs), to a destitute driver "self-insuring" by simply not buying auto insurance and throwing risks onto the general public and him- or herself.

38 peter Sommer, "Insurance and Contingency Planning: Making the Mix," *Computer Fraud and Security Bulletin,* July 1993, p. 5.

ready switched "on." If products are not user-friendly or fully secure, users have no other choice except to write their own software, go without the safeguards, or make do with what is available. The buyers cannot necessarily articulate what features they want, and the developers are ultimately responsible for designing new and useful products. Given society's growing dependence on networked information, the question of the developers' responsibilities for secure and safe products will be increasingly important in coming years. This complex issue needs further attention, but is outside the scope of this report.[39]

Vendors and product developers often claim that buyers do not strongly demand safeguards. In a very competitive market for software, safeguards often add development cost and may require tradeoffs in functionality, compatibility, or capacity for which users are not willing to sacrifice. Indeed, buyers are often accustomed to thinking of computers as isolated machines, and that security violations "won't happen to me. " Users, therefore, often make computer operation simpler by disabling the safeguards that are provided with the product. Users may not perceive that threats are real, may lack the expertise to use the products, or may simply be willing to assume the associated risk. For whatever reason, the majority of safeguard failures in information networks is attributable to human errors in implementation and management of existing systems.[40]

Vendors are currently restricted from exporting certain encryption products without a license granted by the State Department. The controlled products are those that that the National Security Agency (NSA) deems "strong' '-impractically difficult to decrypt should they be widely distributed internationally. At one time, NSA was the source of almost all encryption technology in the United States, because of its role in signals intelligence and securing classified information. However, encryption technology has moved beyond the national-security market into the commercial market. Today, therefore, U.S. intelligence and law-enforcement agencies are concerned about strong encryption incorporated into integrated hardware and software products (including commercial, public-domain, and shareware products). Much of the controlled encryption is already available outside of the United States as stand-alone products developed legally overseas (sometimes based on articles or books[41] legally exported overseas), or pirated, transported, or developed overseas illegally (e.g., infringing patents; see discussion of export controls in chapter 4).

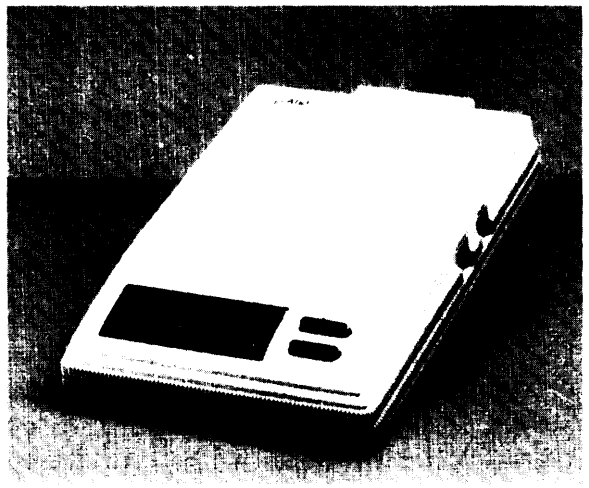
Vendors argue that foreign companies can now produce and export many such products and will capture more of the market for safeguards.[42] Moreover, since security features are usually embedded inside of other hardware and software

39 National Research Council, op. cit., footnote 6, pp. 165-173.

40 Ross Anderson, "Why Cryptosystems Fail," Proceedings from the First ACM Conference on Computer and Communications Security, Nov. 5, 1993, Fairfax, VA, pp. 215-227.

41 In one instance, the author of a book on cryptography received permission to export the book—including a printed appendix of source code 1 istings to implement the algorithms and techniques described in the book-but was denied a license to export the same source code in machine-readable fore]. Bruce Schneier's book, *Applied Cryptography (New* York, NY: John Wiley & Sons, 1994) explains what cryptography can do, innonmathematical language; describes how to build cryptography into products; illustrates cryptographic techniques; evaluates algorithms; and makes recommendations on their quality. According to Schneier, the State Department granted export approval for the book (as a publication, protected as free speech by the Constitution), but denied export approval for the source code disk. According to Schneier, this disk contained, "line for line, the exact same source code listed in the book." (Bruce Schneier, Counterpane S ysterns, Oak Park, IL, personal communication, July 1, 1994.)

42 US House of Representatives, Subcommittee on Economic Policy, Trade, and Environment, hearing on encryption export controls, Oct. 12, 1993.



"Clipper" Telephone Security Device (AT&T Surity 3600),

products, foreign companies could capture more of the overall information technology market. On the other hand, buyers may not be demanding as much encryption protection for confidentiality as vendors claim. Further study into this issue is needed to determine more fully the effects of export controls on the ability of vendors and developers to supply affordable and user-friendly safeguards (see chapter 4).

A number of important intellectual-property issues also have marked the industry, particularly pertaining to cryptography and software (see the 1992 OTA report *Finding a Balance: Computer Software, Intellectual Property, and the Challenge of Technological Change* for discussion of copyright and patent issues pertaining to software and computer algorithms). Selected intellectual property issues are discussed further in chapter 3.

In summary, the dynamic technologies and markets that produced the Internet and a strong networking and software industry in the United States have not consistently yielded products free from defects or equipped with affordable, user--friendly safeguards. More study of software and product quality and liability is needed to fully understand vendors' responsibilities. More study is also needed to understand the effect of export controls on the ability of vendors and developers to provide affordable safeguards.

Standards-Setting Bodies

Standards used in this context are specifications written or understood by formal or informal agreements or consequences. Standards allow different products to work together, making products and services easier to use and less expensive and the market more predictable for buyers. Standards are particularly important in networks, since many parties on the network must store and communicate information using compatible formats and procedures---called *protocols*. In small or closed networks, all the users can employ the same proprietary equipment and protocols, but in large and open networks this is impractical.

An important area of standards-setting is in the protocols used to send messages between computers. The Internet largely uses formats built upon the Transmission Control Protocol/Internet Protocol (TCP/IP). Other protocols include the Open Systems Interconnection (OSI) set.[43] The protocol of one system does not necessarily work with another system, and there is an effort to standardize or translate the various protocols so that computers can all talk easily with one another. To make this possible, some protocols may have to be abandoned, while others may be modified or translated when necessary. Without appropriate "placeholders" in currently developing protocol standards, it may be impossible in the future to set up and maintain desired network safeguards.

Safeguards can be weakened as well as strengthened through the standards-setting process. Designers must often make compromises so that different protocols can work together. Maintaining the safeguarding features is only one aspect of these modifications; other important

[43] See ISO/IEC "Information Processing Systems—Open Systems Interconnection Reference Model—Part 2: Security Architecture," ISO *7498-2, 1988,* and related standards. See also the report of the Federal Internetworking Requirements Panel (FIRP) established by NIST to address short- and long-term issues of internetworking and convergence of networking protocols. including the TCP/IP and OSI protocol suites.

features include user-friendliness, flexibility, speed or capacity, and cost.

The lack of any standards or too many standards, however, significantly limits the effectiveness of many safeguards. In particular, safeguards that require each user of either end of a communication to have compatible schemes—for sending messages, for example, or encrypting and decrypting telephone calls—benefit from the widest possible distribution of that product so that the users can communicate with more people. Even market-driven de facto standards, in such a case, are better than well-protected users who cannot communicate with but a few other users because of a wide variety of incompatible standards.

Standards are set through bodies such as the Internet Engineering Task Force and the Internet Architecture Board, the International Organization for Standardization (ISO)[44] and the American National Standards Institute (ANSI), the former Comité Consultatif Internationale de Télégraphique et Téléphonique (CCITT),[45] the European Computer Manufacturers Association (ECMA), the European Telecommunications Standards Institute (ETSI), the American Bankers Association (ABA), and the Institute of Electrical and Electronics Engineers (IEEE).[46]

In general, vendors in countries with markets and bodies that develop standards quickly can gain an advantage over vendors in other countries lacking quality standards.[47] Achieving the necessary consensus for quality standards is particularly difficult in the rapidly changing information industry, however, including the area of information safeguards. Standards are most effective when applied to relatively narrow, well-defined areas where there is a clear need for them. Policymakers and others must therefore consider carefully the balance between setting de jure standards versus allowing the market to diversify or drift to its own de facto standards.

The National Institute of Standards and Technology (NIST) in the Department of Commerce has a prominent role to work with these standards-setting bodies and also to develop Federal Information Processing Standards (FIPS) for use by the federal government and its contractors. In particular, the Department of Commerce has recently issued two controversial FIPS that involve much larger debates over fundamental issues involving export controls, national-security and law-enforcement interests, and privacy—the Digital Signature Standard (DSS) and the Escrowed Encryption Standard (EES). Broader efforts to protect networked information will be frustrated by cryptography-standards issues unless the process for establishing cryptography policy is clarified and improved (see chapter 4).

Product Evaluations

Product evaluations in general are intended to help assure buyers that off-the-shelf computer and network equipment and soft ware meet contract requirements and include certain acceptable safeguards free of defects. Even relatively simple systems require that all but experts place a significant amount of trust in products and their vendors.

---

44 Also known as the Organisation Internationale de Normalisation, and the International Standards Organization.

45 The CCITT (also called th. International Telegraph and Telephone Consultative Committee) has been reorganized in the International Telecommunications Union (ITU) in its new Telecommunication Standardization Sector.

46 For further information, see Deborah Russell and G.T. Gangemi, op. cit., footnote 6, chapter 2 and appendix D. For further information on encryption standards, see Burt Kaliski, "A Survey of Encryption Standards," *IEEE Micro*, December 1993, pp. 74-81.

47 For an overview of general standards. setting processes and options for improvement, see U.S. Congress, Office of Technology Assessment, *Global Standards; Building Blocks for theFuwre,OTA-TCT-512* (Washington, DC: U.S. Government Printing Office, March 1992). See also David Landsbergen, "Establishing Telecommunications Standards: A Problem of Procedures and Values," *Informatization and the Private Sector*, vol. 2, No. 4, pp. 329-346. See also Carl F. Cargill, *information Technology Standardization: Theory. Process, and Organizations* (Bedford. MA: Digital Press, 1989).

Independent experts can evaluate these products against minimum qualifications and screen for defects, saving buyers the cost of errors that might result from making their own evaluations or from relying on the vendors.

Large user organizations are often capable of running benchmarks and other tests of functional specifications for their constituents. Within the federal government, the Department of the Treasury evaluates products used for message authentication for federal government financial transactions, with input and testing services provided by NSA and NIST. NIST validates products that incorporate the Data Encryption Standard (DES) and other FIPS. NSA provides several services: endorsements of cryptographic products for use by government agencies only; approvals of "protected network services" from telecommunications providers; a list of preferred and endorsed products and test services for TEMPEST equipment;[48] a list of degaussers (tools that demagnetize magnetic media) that meet government specifications; and the assignment of trust levels to "computer systems, software, and components" 49 (through the National Computer Security Center or NCSC[50]).

In the last case, the NCSC evaluates products against the Trusted Computer Security Evaluation Criteria (TCSEC—the "Orange Book") and its related "Rainbow Series" books.[51] An *evacuation* refers here to the "assessment for conformance with a pre-established metric, criteria, or standard," whereas an *endorsement* is an approval for use.[52] The NCSC makes these evaluations at no direct cost to vendors, but vendors must pay for considerable preparation and the process is often slow. This process in turn adds delays for buyers, who must pay for the overall development cost. Critics claim that the process produces obsolete products by the time the products are evaluated.

The Orange Book also emphasizes access control and confidentiality, and not other features such as integrity or availability more relevant to industry, civilian agencies, or individuals. This emphasis is a direct result of the Orange Book's Department of Defense history; applications involving classified information and national security require trusted systems that emphasize confidentiality. Critics claim that this emphasis is too slow to change and perpetuates an obsolete approach. Some also claim that the rating of the evaluated product should pertain to its condition "out of the box," not after the security features have been switched on by a security professional.

To attempt to meet the needs of other buyers, NIST is developing a complementary process that would delegate evaluations of lower level security

---

48 The U.S. government established the TEMPEST program in the *1950s* to eliminate compromising electromagnetic emanations from electronic equipment, including computers. Without such protection, an adversary may detect faint emanations (including noise) from outside the room or building in which the user is operating the computer, and use the emanations to reconstruct information. TEMPEST products are used almost exclusively to protect classified information.

49 National Security Agency, Information Systems Security organization, *Information Systems Security Products and Services Catalog* (Washington, DC: U.S. Government Printing Office, 1994), p. vii. The word *systems* often appears in this context but is misleading; the trust levels are actually assigned to products. See the discussion below on certification and accreditation.

50 The National Computer Security Center was established from the Department of Defense Computer Security Initiative, which in turn was a response to identified security weaknesses in computers sold to the Department of Defense.

51 So called because each book is named after the color of its cover. The first in the series is the Orange Book. See U.S. Department of Defense, *DOD Trusted Computer System Evaluation Criteria (TCSEC)*, DOD 5200.28-STD (Washington, DC: U.S. Government Printing Office, December *1985). The Orange* Book is interpreted for networked applications in the "Red Book." See National Computer Security Center, *NCSC Trusted Network Interpretation*, NCSC-TG-005 (Washington, DC: U.S. Government Printing Office, July 1987). See also the "Yellow Book": National Computer Security Center, Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements-Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, CSC-STD-004-8 (Washington, DC: U.S. Government Printing Office, June 25, 1985).

52 National Security Agency, op. cit., footnote 49, pp. 4-28,4-29.

products to third parties certified by the U.S. government. This program, the Trusted Technology Assessment Program (TTAP), is under development and would be managed by NIST. The evaluators could charge for the evaluations, but would compete to provide timely and inexpensive service. The overall cost might be lower, and products may be brought to market more quickly. This process resembles the Commercially-Licensed Evaluation Facilities (CLEF) program currently in use in the United Kingdom.

Another alternative suggested by NIST is to allow the vendors to validate claims on their own products for low-level security applications. This strategy could exist on its own or coexist with the TTAP described above. The vendors would be guided by using criteria and quality control tests built into the development process. While this alternative may be acceptable in many cases, an independent evaluation using personnel not employed by the vendor may be preferable.[53]

In these or other alternatives, evaluators could work on their own to develop new criteria. If too many differing criteria are developed for evaluating products, however, the market could be fragmented and vendors may be forced to develop and market many different products. Such fragmentation adds to cost, delays, and confusion for the buyer, defeating the purpose of the evaluations. In practice, relatively few sets of criteria may be widely used.

Meanwhile, the European Community follows its own product evaluation standard called the Information Technology Security Evaluation Criteria (ITSEC) or Europe's "White Book." These criteria are based in part on the U.S. Rainbow Series as well as earlier European standards. The ITSEC is less hierarchical and defines different categories of requirements depending on the application. The ITSEC was developed by France, Germany, the Netherlands, and the United Kingdom and was published in 1991.[54]

The differing European and U.S. criteria split the market for vendors, making products more expensive to develop and test, and possibly driving out some vendors. NIST and NSA, therefore, proposed anew set of criteria to promote international harmonization of criteria as well as improve the existing Rainbow Series criteria, and to address better commercial requirements. A draft of these proposed "Federal Criteria" was published in December 1992 and received comment throughout 1993.[55]

NIST and NSA have since subsumed this project to work with the European Community and Canada toward an international standard—the Common Information Technology Security Criteria, or draft "Common Criteria' '-expected in 1994. The Common Criteria would incorporate the experience gained from the existing U.S. Rainbow Series (and the comments received on the draft Federal Criteria), the European ITSEC, and the Canadian Trusted Computer Product Evaluation Criteria.

However, the resolution of an international agreement is not final. The proposal has met criticism for not incorporating foreign participation from Japan, Australia, and other countries. Critics also claim there is not enough participation from the private sector and that the intelligence sector, therefore, will drive any agreement too much toward protecting confidentiality rather than emphasizing other important features of safeguards. Even if agreement were completed, products that meet the Common Criteria will not be evaluated immediately as vendors must first interpret the

[53] National Research Council, op. Cit., footnote 6, p. 128.

[54] Commission of the Economic Community, *Information Technology Security Evaluation Criteria, Provisional Harmonized Criteria*, version 1.2, June 1991.

[55] U.S. Department of Commerce, National Institute of Standards and Technology, "Federal Criteria for Information Technology Security. " December *1992.*

new criteria and then evaluate existing products or develop new ones.

The trusted product evaluation process is not and will not soon be effective for delivering products that adequately protect networked information. Alternatives to the current approach appear promising, however, including (but not limited to) NIST's proposed Trusted Technology Assessment Program.

System Certifications and Accreditations

The evaluations described above evaluate products but not systems. A *product* can be defined as an off-the-shelf hardware or software product that can be used in a variety of operating environments. A *system*, on the other hand, is designed for a specific user and operating environment. "The system has a real world environment and is subject to real world threats. In the case of a product, only general assumptions can be made about its operating environment and it is up to the user, when incorporating the product into a real world system, to make sure that these assumptions are consistent with the environment of that system."[56] Product evaluations alone can overestimate the level of security for some applications, or if the product is not implemented correctly in the system.

> Increasingly, computers are becoming connected via networks and are being organized into distributed systems, In such environments a much more thorough system security analysis is required, and the product rating associated with each of the individual computers is in no way a sufficient basis for evaluating the security of the system as a whole. This suggests that it will become increasingly important to develop methodologies for ascertaining the security of networked systems, not just evaluations for individual computers. Product evaluations are not applicable to whole systems in general, and as "open systems" that can be interconnected relatively easily become more the rule, the need for system security evaluation, as distinct from product evaluation, will become even more critical. [57]

DOD examines systems—a process called *certification--to* technically assess the appropriateness of a particular system to process information of a specific sensitivity in its real-world environment.[58] A DOD certification is thus an analysis related to the system requirements.[59] The subsequent step of *accreditation* refers to the formal approval by a designated authority to use the system in that particular environment. The accreditation should take account of the results of the certification, but may not necessarily reflect it; the accreditation also takes account of nontechnical (business and political) considerations and is the ultimate decision regarding the system.

Certification attempts to encompass a systems approach to security and is a much more complex process than product evaluation. The National Research Council noted that

> ... Unfortunately, the certification process tends to be more subjective and less technically rigorous than the product evaluation process, Certification of systems historically preceded Orange Book-style product evaluation, and certification criteria are typically less uniform, that is, varying from agency to agency. . [60]

The report goes on to recommend that a set of generally accepted principles include guidelines

---

56 Krish Bhaskar, op. cit., footnote 6, p. 298.

57 National Research Council, op. cit., footnote 6, pp. 138-139.

58 National Computer Security center, *Introduction to Certification and Accreditation*, NCSC-TG-029(Fort George G. Meade, MD: National Computer Security Center, January 1994).

59 The *system* certification concept here is distinct from the *user* examination and certification, and the *key* certification concepts discussed in other sections.

60 National Research Council, Op. cit., footnote 6, p.137.

● *to institute more objective, uniform, rigorous standards for system certification." These principles are currently under development (see the following section).

Generally Accepted Practices and Principles

Generally accepted practices can be documented and adopted to help guide information security professionals and vendors. These practices would act much as Generally Accepted Accounting Principles standardize practices for accountants (see box 2-4). Such practices could help advance professional examinations; provide standards of due care to guide users, managers, and insurance companies; and give vendors design targets. To be comprehensive, however, the generally accepted practices must be defined at several levels of detail, and different sets of standards would apply to different users and applications. The establishment of generally accepted principles was suggested by the National Research Council in 1991.[61]

The Institute of Internal Auditors has a document "intended to assist management in evaluating cost/benefit considerations" as well as to "[p]rovide internal audit and information systems practitioners with specific guidelines and technical reference material to facilitate the implementation and verification of appropriate controls."[62] The Organization for Economic Cooperation and Development (OECD) has developed general guidelines to help member countries in information-security issues. The guidelines were adopted in 1992 by the OECD Council and the 24 member nations. These guidelines list nine general principles and several measures to implement them. The guidelines are intended to serve as a framework for both the private and public sectors.[63,64]

The Information Systems Security Association (ISSA) is in the process of developing a comprehensive set of Generally Accepted System Security Principles (GSSPs) for professionals and information-technology product developers to follow. The ISSA effort includes members from the federal government (through NIST), and representatives from Canada, Mexico, Japan, the European Community, and industry. The Clinton Administration has also supported NIST's efforts in GSSPs in its National Performance Review.[65] The success of these principles, when completed, will depend on their speedy adoption by government, industry, and educational institutions.

The ISSA has divided the principles into two sets. The first-the Information Security Professional GSSPs—is aimed at professionals, including managers, developers, users, and auditors and certifiers of users. The second group--the GSSPs for Hardware and Software Information Products—is aimed at products and the auditors and certifiers of products. Each of these sets of GSSPs has a three-tier hierarchy of *pervasive principles, broad operating/functional principles,* and de*tailed security principles.*

The pervasive principles adapt and expand on the OECD principles described above. The broad operating/functional principles are more specific and are based on many documents such as the NSA Rainbow Series, FIPS, Electronic Data Processing Auditor's Association Control Principles, and the United Kingdom's *Code of Practice for Information Security Management.*[66] The

---

61 Ibid.

62 See Institute of Internal Auditors Research Foundation, op. cit., footnote 35, pp. 1-4 to I -6.

63 Organization for Economic Cooperation and Development, Information, Computer, and Communications Policy Committee, "Guidelines for the Security of Information Systems," Paris, November 1992.

64 The United Nations has relatively specific guidelines for its organizations. See United Nations, op. cit., footnote 1.

65 Office of the Vice President, Accompanying Report of the National Performance Review', *Reengineering Through Information Technology* (Washington, DC: U.S. Government Printing Office, September 1993).

66 Department of Trade and Industry, A *Code of Practice for Information Security Management,* 1993.

detailed principles address the practical application of the other principles, and are expected to change frequently to stay current with evolving threats. The detailed principles will include step-by-step procedures of common security tasks, prevalent practices, and so forth.[67]

Generally accepted principles have strategic importance to other aspects of networked information, such as for establishing due care guidelines for cost-justifying safeguards, as targets for training and professional certification programs, and as targets for insurance coverage. The current effort in GSSP will not produce immediate results, but the effort is overdue and OTA found wide support for its mission.

Professional Organizations and Examinations

The educational and career paths for information-security practitioners and managers are not so mature as in other fields, such as accounting or law. The field could benefit from the professional development of security practitioners and managers. Security professionals enter the field from widely diverse disciplines, and managers cannot necessarily compare the expertise of applicants seeking positions as security professionals. Professional recognition credits individuals who show initiative and perform well against a known standard. University computer science departments lack programs specializing in information safeguards; but professional examinations provide a target for institutions that graduate computer scientists or provide continuing education in safeguards.

Certifications[68] in other fields of computing include the Certified Systems Professional, the Certified Computer Programmer, and the Certified Data Processor (all from the Institute for Certification of Computer Professionals, or ICCP), and the Certified Information Systems Auditor (from the Electronic Data Processing Auditors Association). The Systems Security Examination of the ICCP allows professionals with diverse responsibilities to have a certification that includes information safeguards.[69] These organizations have extended or have proposed extending existing certifications to include information security, but none focus directly on it.

The International Information Systems Security Certification Consortium (ISC^2) is developing an information security certification in cooperation with the federal government (through NIST and NSA), the Canadian government, Idaho State University, the Data Processing Management Association, Electronic Data Processing Auditors Association, the Information Systems Security Association, the International Federation for Information Processing, the Canadian Information Processing Society, the Computer Security Institute, and others. The consortium expects to examine about 1,500 professionals per year up to an ongoing pool of about 15,000 certified professionals.[70]

Efforts to "professionalize" the information security field are important steps, but will not produce significant results for some time. Their success is also related to the success of Generally Accepted System Security Principles and their adoption in industry and government. It is unclear whether professional examinations and certifications will ever have a strong impact in an industry that is as dynamic and evolutionary as information

---

67 Information Systems Security Association, Inc., GSSP Committee, "First Draft of the Generally Accepted System Security Principles," Sept. 22, 1993.

68 The *user* certification concept here is distinct from the *system* certification and accreditation, and the key certification concepts discussed in other sections.

69 Corey D. Schou, W. Vic. Maconachy, F. Lynn McNulty, and Arthur Chantker, "Information Security Professionalism for the 1990's," *Computer Security Journal*, *vol. 1X, No.* 1, p. 27. See also Institute for Certification of Computer Professionals, "The Systems Security Examination of the Institute for Certification of Computer Professionals (ICCP)," *Computer Security Journal, vol.* VI, No. 2, p. 79.

70 Philip E. Fites, "Computer Security Professional Certification," *Computer Security Journal,* vol. V, No. 2, p. 75.

networking. Engineers in the information industry, for example, have not widely adopted the licensing of professional engineers. Engineering examinations and licenses are more effective in relatively stable fields, such as the construction and oil industries. Examinations and certifications are also effective, however, where liability and the protection of assets is involved, as in accounting and construction.

Public-Key Infrastructure

Information networks must include important clearinghouse and assurance functions if electronic commerce and other transactions are to be more widespread and efficient (see chapter 3).[71] These functions include the exchange of cryptographic keys between interested parties to authenticate each party, protect the confidentiality and/or the integrity of the information, and control a copyright (see box 2-3).[72] In all cases, the two communicating parties must share at least one key before any other transactions can proceed—if only to transmit other keys for various purposes. A means to do this efficiently is called a *public-key infrastructure.*

Each party could generate its own key pair and exchange public keys between themselves, or publish its public keys in a directory.[73] A key-distribution center can also distribute public keys electronically over a network, or physically transport them. While manual techniques are acceptable for small networks, they are unwieldy for large networks and electronic commerce where keys must be changed often over long distances and between parties that have never met.

Instead, experts envision broader use of electronic commerce and other transactions by developing trusted electronic systems for distributing and managing keys electronically. In order for the users to trust the keys they receive, some party must take responsibility for their accuracy. One way to do this is to embed each user's key in a digitally signed message (certificate) signed by a trusted third party. The two parties then authenticate each other with the public keys and proceed with their communications (see box 2-5).

The trusted third party is often referred to as a *certification authority* (CA), and plays an important role in these electronic commerce transactions.[74] The CA confirms the identity of each party at the beginning of the process, and presents the user with a certificate (signed by a digital signature) with the user's public key.[75] The CA also keeps a record of invalidated certificates; a user can check another user's certificate to see if it expired or was otherwise invalidated. The CA could also act as a notary public to certify that an action occurred on a certain date,[76] act as an archive to store a secure version of a document, or may be associated with key distribution, although other entities could also manage such functions.

---

71 Important clearinghouse functions include matching buyers to sellers, exchanging electronic mail, clearing payments, and so forth. See Michael S. Baum and Henry H. Perritt, Jr., *Electronic Contracting, Publishing, and EDI Law (New* York, NY: Wiley Law publications, 1991). See also U.S. Congress, Office of Technology Assessment, *Electronic Enterprise: Looking to the Future,* OTA-TCT-600 (Washington, DC: U.S. Government Printing Office, May 1994).

72 See the *Journal of the Interactive Mulitmedia Association Intellectual Property Project,* vol. 1, No. 1 (Anna@ is media Association, January 1994).

73 Morrie Gasser, op. cit., *footnote* 6, pp. 258-260. See also Walter Fumy and peter Landrock, "Principles of Key Management," *IEEE Journal on Selected Areas in Communications, vol. 11, No. 5,* June 1993, pp. 785-793.

74 The *key* certification concept here is distinct from the system certification and accreditation, and the user examination and certification concepts discussed in other sections.

75 See the explanation in Stephen T. Kent, "Internet Privacy Enhanced Mail," *Communications of the ACM,* vol.36, No.8, August1993, pp. 4859.

76 Barry Cipra, "Electronic Time-Stamping: The Notary Public Goes Digital" and "All the Hash That Fit To print," *Science,* vol.261, July 9, 1993, pp. 162-163.

BOX 2-5: How Are Cryptographic Keys Exchanged Electronically?

Whenever messages are encrypted in a network, there must be a method to safely exchange cryptographic keys between any two parties on a regular basis Two public-key methods described here allow frequent electronic key exchanges without allowing an eavesdropper to intercept the key.

In the "key transport" or "key distribution" method, a user (Carol) generates a session key, and encrypts it with the other user's (Ted's) public key (see figure 2-4) Carol then sends the encrypted session key to Ted, and Ted decrypts it with his private key to reveal the session key

To protect against fake or Invalid public keys, a party can send his or her public key in a certificate digitally signed by a certification authority (CA) according to its standard policy. If the other party doubts the certificate's validity, it could use the CA's public key to confirm the certificate's validity It also could check the certificate against a "hot list" of revoked certificates and contact the CA for an updated list.

In the Diffie-Hellman method, [1]each party (Alice and Bob) first generates his or her own private key (see figure 2-5) From the private key, each calculates a related public key The calculation is one-way—the private key cannot be deduced from the public key [2]Alice and Bob then exchange the public keys, perhaps through a clearinghouse that facilitates the operation

Alice then can generate a whole new key—the session key—by combining Bob's public key with Alice's own private key Interestingly, due to the mathematical nature of this system, Bob obtains the *same* session key when he combines Alice's public key with his private key [3]An eavesdropper cannot obtain the session key, since he or she has no access to either of Alice or Bob's private keys

---

[1]W Diffie and M E Hellman, "New Directions in Cryptography, " *IEEE Transactions on Information Theory*, vol 22, 1976, pp 644-654

2 In the Diffie-Hellman technique, the public key (y) is based on the exponentiation of a parameter with x, where x is the random private key The exponentiation of even a large number is a relatively easy calculation compared with the reverse operation of finding the logarithm of y

3Using the Diffie-Hellman technique, one party exponentiates the other's public key (*y*) with his or her private key (x) The result is the same for both parties due to the properties of exponents The reverse operation of finding the logarithm using only the public keys and other publicly available parameters appears to be computationally retractable

SOURCE Off Ice of Technology Assessment, 1994

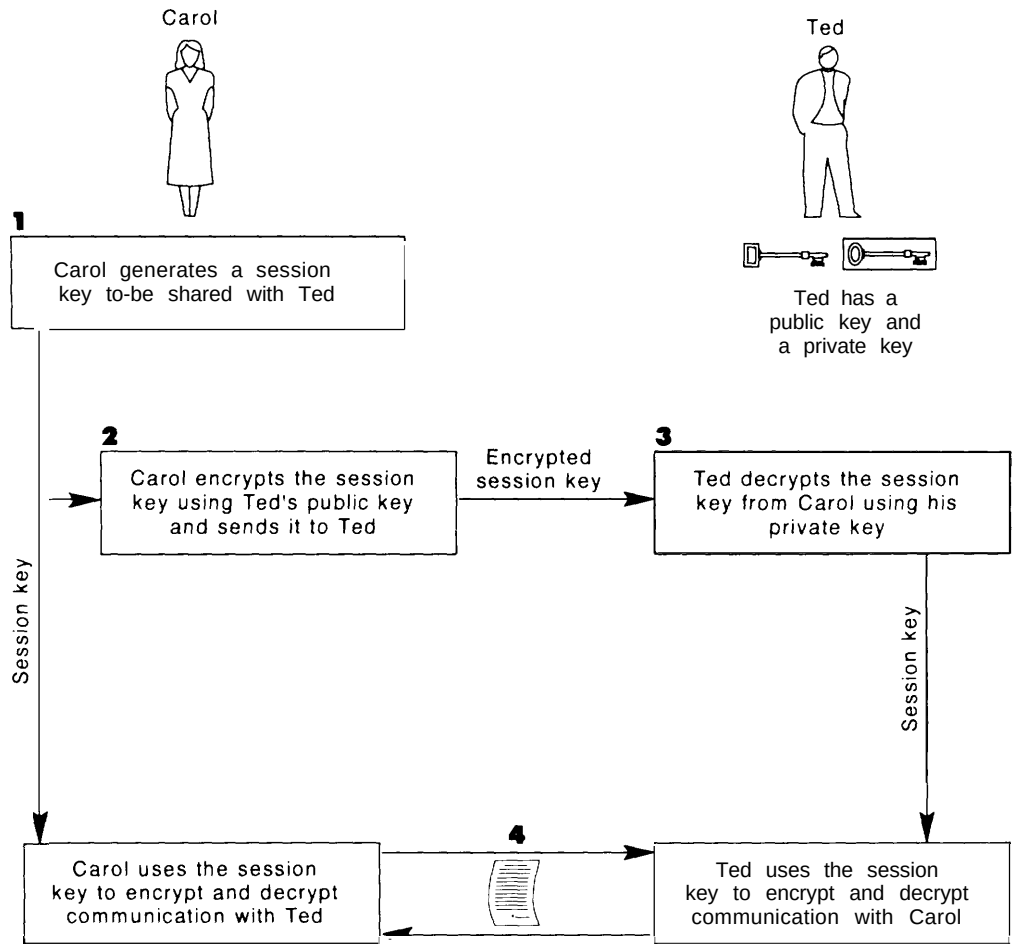
The two parties in a transaction might have different CAs depending on their location, function, and so forth. Each CA would then have to assure itself its underlying security policy assumptions are not violated when handing off from one intermediary to another. To do this, each CA would confirm that each other CA was authentic, and that the other CAs' policies for user authentication were adequate.

Certification authorities have been established for use with Internet Privacy-Enhanced Mail and other functions. The recently formed CommerceNet prototype, for example, will use public keys certified through existing and future authorities .77 "Value-added" telecommunication providers already perform several electronic data interchange (EDI) services such as archiving, postmarking, acknowledging receipt, and assuring interoperability with other value-added carriers. Such carriers typically concentrate in one business sector but could, in principle, expand to provide services to a larger and more diverse market. Banks also have experience with storing valuable documents

---

77For a description of CommerceNet, see John W. Verity, "'Truck Lanes for the Info Highway," Business *Week*, Apr. 18, 1994, pp. 112-114.

FIGURE 2-4: Secret-Key Distribution Using Public-Key Cryptography



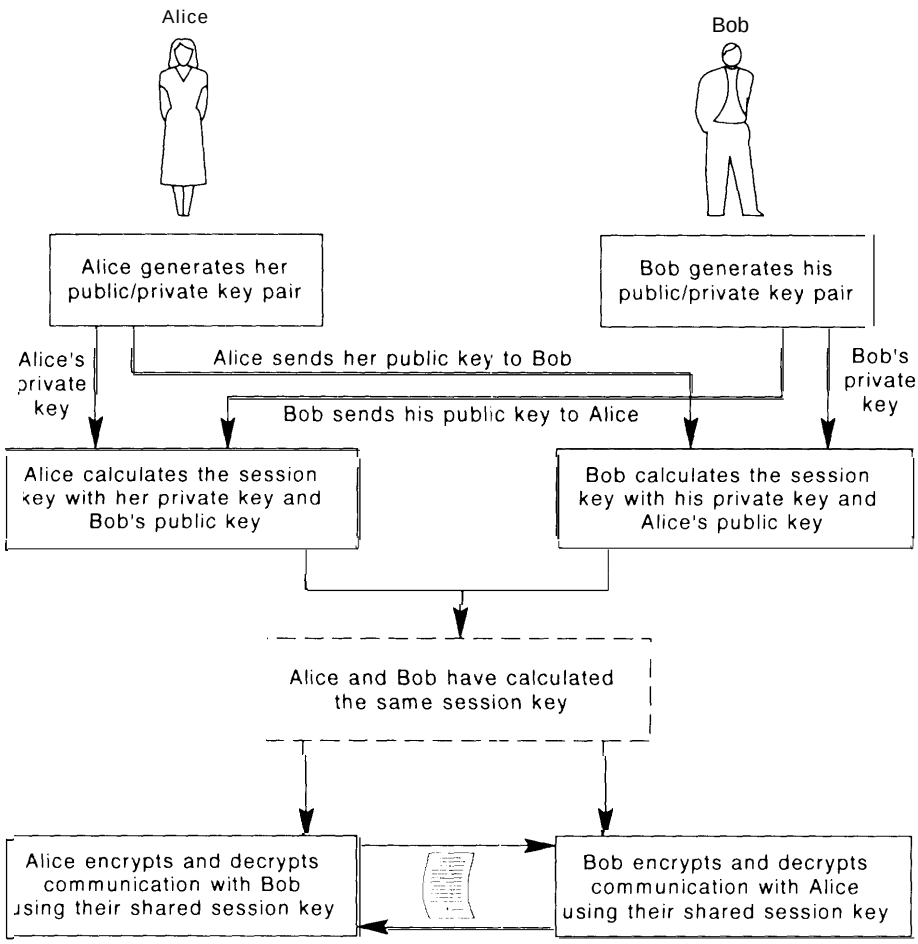
NOTE Security depends on the secrecy of the session key and private keys, as well as the authenticity of the public keys

(e.g., in safe deposit boxes), selling checks backed by their own funds, fulfilling conditions under trust agreements, and employing individuals who act as notaries public. Such experience could also be extended to electronic commerce to act as CAs or to perform other functions.

The U.S. Postal Service has proposed that it also become a certification authority.[78] Those desiring distribution of public keys would identify themselves at a Post Office in the same manner that identification for passports is accomplished today. The certificates would be available online through existing networks such as the Internet and would be authenticated with a Postal Service public key. Additional transaction services would be provided for time and date stamping and archiving, all authenticated with the Postal Service

78 Mitre Corp., "Public Key Infrastructure Study," contractor report prepared for the National Institute of Standards and Technology, April 1994.

FIGURE 2-5: Diffie-Hellman Key Exchange



NOTE An authentication scheme for the public keys may be used

public key.[79] Proponents point out that the Postal Service is already trusted with important documents and is widely located. Critics note that although it provides certified mail services, the Postal Service has no real experience in electronic commerce; important details remain to be resolved regarding liability and accountability.

The establishment of a system of certification authorities and legal standards is essential for the development of a public-key infrastructure, Which, in turn, is strategic to electronic commerce and to networked information in general (see chapter 3). Current proposals for a public-key infrastructure need further pilot testing, development, and review, however, before successful results can be expected.

79 Richard Rothwell, Technology Applications, U.S. Postal Service, personal communication, June 15, 1994.

Emergency Response Teams

Any network benefits from having a central clearinghouse for information regarding threats to the network. In small networks, the "clearinghouse" may be simply the system administrator who manages the net work. Larger net works often have a team of individuals who collect and distribute information for the benefit of system administrators for its member networks. Such clearinghouses-called "emergency response teams" or "incident response teams"--are vital to large networks of networks such as the Internet.

The most prominent of these is the Computer Emergency Response Team (CERT), sponsored since 1988 by the Software Engineering Institute at Carnegie Mellon University and the Department of Defense's Advanced Research Projects Agency (ARPA). CERT provides a 24-hour point of contact available by telephone, facsimile, or electronic mail. CERT collects information about vulnerabilities; works with vendors and developers, universities, law-enforcement agencies, NIST, and NSA to eliminate the vulnerabilities and threats; and disseminates information to systems administrators and users to eliminate vulnerabilities where possible. According to its policy, CERT does not disseminate information about vulnerabilities without an associated solution (called a "patch") since malicious users could exploit the vulnerability before the majority of users had time to develop their own repairs. Some claim, however, that CERT could be more effective by readily disseminating information about vulnerabilities so that users can design their own patches, or perhaps if no solutions are found after a fixed period of time.

CERT is not the only emergency response team. The Defense Data Network (DDN) Security Coordination Center, sponsored by the Defense Communications Agency and SRI International, is a clearinghouse for vulnerabilities and patches on the MILNET.[80] The Computer Incident Advisory Capability was established at Lawrence Livermore Laboratory to provide a clearinghouse for classified and unclassified information vulnerabilities within the Department of Energy, including those relating to the Energy Science Network (ESnet).[81]

These and other emergency response teams form the Forum of Incident Response and Security Teams (FIRST), created by ARPA and NIST. The forum is intended to improve the effectiveness of individual and overall response efforts. Its members include groups from industry, academia, and government, both domestic and international.[82]

The Administration has proposed that NIST, in coordination with the Office of Management and Budget and NSA, develop a governmentwide crisis response clearinghouse. This clearinghouse would serve existing or newly created agency response teams to improve the security of agency networks.[83]

Emergency response efforts are vital to safeguarding networked information, due to the relative lack of shared information about vulnerabilities in information networks. Expanding current efforts could further improve the coordination of system administrators and managers charged with protecting networked information.

---

80 In 1983 the military communications part of the original ARPANET (sponsored by the Advanced Research Projects Agency in the Department of Defense) was split off to form the MILNET. The remaining part of the ARPANET was decommissioned in 1990, but Its functionality continued under the National Science Foundation's NSFNET, which in turn became a prominent backbone of what is called today the Internet.

81 The Department of Energy 's Energy Science Network (ESnet) includes a backbone and many smaller networks that are all connected to the Internet. similar to the operation of the National Science Foundation's NSFNET, and the National Aeronautics and Space Administration's Science Internet (NSI).

82 L Dain Gary, Manager, Computer Emergency Response Team Coordination Center, testimony before the House Subcommittee on Science, Mar. 22, 1994.

83 Office of the Vice President, op. cit., footnote 65.

Users, Ethics, and Education

Unauthorized use of computers by authorized users is estimated to be the second largest source of losses (after human error), but users nevertheless must be trusted not to wrongly copy, modify, or delete files. Auditing and other security features do not always catch violations by trusted personnel, or may not act as a deterrent. The security of any system will always require that its users act in an ethical and legal manner, much as traffic safety requires that drivers obey traffic laws, although in practice they often do not (see box 2-6).

Ethical and legal use of computers and information is not clearly defined, however. Computer networks are entirely new media that challenge traditional views of ownership of information, liability, and privacy (see chapter 3). Who is or who should be liable if a computer system fails, or if an "expert" computer program makes a poor decision? When can or when should employers or the government be able to monitor employees and citizens? When is or when should the copying of computer software be illegal? For these and other issues, it is not always clear when society should extend traditional (paper-based) models to networks, and when society should devise new rules for net works where they seem necessary.[84] Should ethics--and the laws based on ethics—be rule-based or character-based, or based otherwise?

Ethical questions also extend to what constitutes proper behavior or acceptable use on publicly available networks. As the Internet reaches more people, commercial enterprises are exploring it for uses other than education and research. Using the Internet for unsolicited commercial promotions has historically met great opposition from users, but recent events indicate a desire on the part of some to change this tradition. Now that more commercial enterprises are attaching to the Internet and the "backbones" for the large part are removed from the oversight of the National Science Foundation, the old rules for acceptable use of the Internet could change.[85] Who defines ac-

BOX 2-6: Why Is It So Difficult To Safeguard Information?

The Office of Technology Assessment asked the advisory panel for this study why it is so difficult to safeguard networked information, There are many reasons; many of them are discussed in detail in this report, Here is a sample of the panelists' responses:

- Safeguards involve a tradeoff with cost and utility (However, the alternative-not using safeguards-can have catastrophic consequences and cost much more than the safeguards!)
- Successes in safeguarding information rarely produce measurable results, and successful managers are poorly rewarded, Failures can produce sensational results and managers are put on the defensive.
- Information is abstract, its value is only now becoming understood, Information cannot be seen, and losses or disclosures can go undetected.
- The user is often trusted to protect information that does he or she does not "own,"
- Information safeguards are relatively new and must evolve with the rapidly changing information industry.

SOURCE Office of Technology Assessment, 1994

84 Tom Forester and Perry Morrison, *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing* (Cambridge, MA: MIT Press, *1990).*

85 Users are expected to use the federally subsidized portions of the Internet-such as the NSFNET backbone—only for nonprofit research or education purposes. This policy is called the Acceptable Use Policy, analogous to acceptable practices used in amateur radio. Those portions not subsidized by the federal government have no such restrictions, but a user culture exists that discourages use of the Internet for unsolicited electronic mail and other uses. The Coalition for Networked Information is expected to adopt guidelines to acceptable advertising practices on the Internet. Ethical principles endorsed by the Internet Activities Board are listed in Vint Cerf, "Ethics and the Internet," *Communications of the ACM, vol. 32, No. 6,* June 1989, p. 710.

ceptable use and proper etiquette? What is the balance between threatening or misleading behavior and free speech? What new practices might be necessary to control fraud?

Experts note that users generally want to know where the line is drawn regarding ethical use of information, and may only need some simple but memorable guidelines. For example, relatively few users probably know what constitutes fair use of copyrighted information, but would appreciate knowing what they can legally copy and what they cannot. Children are taught early on that writing in library books is an unethical practice; straightforward, ethical computer practices can also be taught to children at an early age. Training in the workplace also can help users to understand ethical principles, but such programs are only effective if they are well-developed, do not appear superficial or insincere, and are repeated.[86]

Group behavior is particularly important since groups of users do not necessarily behave in the same manner as individuals. Even relatively secure networks rely on the cooperation of users to alert system managers to problems or threats. A strategic employee who never takes a vacation, for example, may be a worker who cannot leave work for a single day without risk of becoming discovered in a security violation. An unannounced change in a program's operation may indicate that it has been altered. Fellow users can note this and other unusual net work behavior that may signal an intruder in the system, a virus that is taxing network resources, or a design fault. "Just as depersonalized 'renewed' cities of high-rises and doormen sacrifice the safety provided by observant neighbors in earlier, apparently chaotic, gossip-ridden, ethnic neighborhoods," group behavior determines whether users work positively to protect the network, or whether they act as bystanders who lack the motivation, capability, or responsibility to work cooperatively.[87]

User education, therefore, requires progressive approaches to steer the group behavior to be supportive and participatory.[88] Such approaches include using realistic examples and clearly written policies and procedures, and emphasizing improvements rather than failures. Management should seek to inspire a commitment on the part of employees rather than simply describing policies, and it should conduct open and constructive discussions of safeguards rather than one-sided diatribes. Security managers should build on one-to-one discussions before presenting issues at a meeting, and monitor more close] y the acceptance of policies and practices by "outliers''--employees who are the most or least popular in the group-since they are less likely to comply with the group behavior.

The Computer Ethics Institute was created in 1985 to advance the identification and education of ethical principles in computing, and sponsors conferences and publications on the subject. Groups such as the Federal Information Systems Security Educators' Association and NSA are also working to produce curricula and training materials. The National Conference of Lawyers and Scientists (NCLS) is convening a series of two conferences on legal, ethical, and technological aspects of computer and network use and abuse and the kinds of ethical, legal, and administrative frameworks that should be constructed for the global information infrastructure.[89] A consortium of private- and public-sector groups recently announced a National Computer Ethics and Responsibilities Campaign to raise public awareness of

86 See also National Research Council, op. cit., footnote 6, p. 7 10.

87 Ibid., p. 164.

88 M.E. Kabay "Social Psychology and Infosec: Psycho-Social Factors in the Implementation of Information Security Policy," *Proceedings of the 16th National Computer Security Conference* (Baltimore, MD: Sept. 20-23, 1993), p. 274.

89 National Conference of Lawyers and Scientists, "Prospectus: NCLS Conferences on Legal, Ethical, and Technological Aspects of Computer and Network Use and Abuse," Irvine, CA, December 1993.

the social and economic costs of computer-related crimes and unethical behaviors and to promote responsible computer and network usage.

The promulgation of ethical principles in computer networks has heretofore received relatively little attention, and would benefit from broader support from schools, industry, government, and the media. With the rapid expansion of the networked society, there is a great need to support reevaluation of fundamental ethical principles—work that is current] y receiving too little attention. More resources also could be applied to study and improve the methods and materials used in teaching ethical use of networked information, so that more effective packages are available to schools and organizations that train users. Finally, more resources could be devoted to ethical education for all types of users—including federal employees, students, and the public at large.

Legal Sanctions and Law Enforcement

The rapid pace of technological change challenges criminal and liability laws and regulations that were conceived in a paper-based society (see also chapter 3).[90] An error, an insider violation, or an attack from outside can debilitate an organization in many cases, as can the obstruction of regular business from an improperly executed law-enforcement action. Computer cracking and other malicious behavior is likely to increase, and the perpetrators are likely to become more professional as the Internet and other components of the infrastructure mature. Safeguards may become more widespread, but the payoffs will also increase for those who seek to exploit the infrastructure's weaknesses.

However, misconduct or criminal behavior may arise most from opportunities presented to otherwise loyal employees who do not necessarily have significant expertise, rather than from the stereotypical anti-establishment and expert "cracker." Violators may perceive that detection is rare, that they are acting within the law (if not ethically), and that they are safely far from the scene of the crime. Also, some crackers who were caught intruding into systems have sold their skills as security experts, reinforcing the image that violators of security are not punished. Many of these insiders might be deterred from exploiting certain opportunities if penalties were enforced or made more severe.

It is not clear, however, that increasing criminal penalties necessarily results in less computer crime or in more prosecutions. Considerable legislation exists to penalize computer crimes. but criminals are difficult to identify and prosecute. Law-enforcement agencies lack the resources to investigate all the reported cases of misconduct, and their expertise generally lags that of the more expert users. In some cases where alleged violators were arrested, the evidence was insufficient or improperly obtained, leading to an impression that convictions for many computer crimes are difficult to obtain. Better training of law-enforcement officers at the federal, state, and local levels, and more rigorous criminal investigations and enforcement of existing laws maybe more effective than new laws to strengthen sanctions against violators.[91]

Organizations for their part can also clarify internal rules regarding use of networked information, based on the organization's security policy. The organization can use intrusion detection and other tools to identify misconduct and apply its own sanctions in cases where sufficient evidence is discovered. The monitoring of employees raises questions of privacy, however, with some employers preferring to warn employees when they are monitoring them or obtaining written permission beforehand. Some security professionals claim the need for an escrowed key in the hands of the organization's security officers (in place of

---

90 See Ian Walden, "Information Security and the Law," in *Information Security Handbook,* William Caelli, Dennis Longley, and Michael Shain (eds.) (New York, NY: Stockton Press, 1991), ch. 5.

91 For a review of specific examples, see Bruce Sterling, *The Hacker Crackdown (New* York, NY: Bantam Books, 1992).

or in addition to safekeeping by law-enforcement officials). In case of an investigation, the security officers could use the escrowed key, but all other employees would be exempt from random monitoring.[92]

Criminal and civil sanctions constitute only one aspect of safeguarding networked information. Further study is needed to determine the effectiveness of such sanctions, as opposed to improving the effectiveness of federal, state, and local law-enforcement agencies to act on existing laws.

Regulatory Bodies

Given the fragmentation of the telecommunications industry and other developments in the last decade, existing federal oversight over telecommunications is less comprehensive than in the past. Many modem telecommunications providers such as value-added carriers and Internet providers are not reviewed by the traditional entities, although such providers are increasingly important to businesses and government.

Existing federal agencies that already review different aspects of the security and reliability of the public-switched telephone networks include the National Security Telecommunications Advisory Council (NSTAC), the National Communications System (NCS), and the Federal Communications Commission (FCC).[93] NCS was established in 1963 to coordinate the planning of national-security and emergency-preparedness communications for the federal government. NCS receives policy direction directly from the President and the National Security Council, but is managed through the Department of Defense and includes member organizations from many other federal agencies. NSTAC was established during the Reagan Administration to advise the President on national-security and emergency-preparedness issues, and is composed of presidents and chief executive officers of major telecommunications and defense-information-systems companies. NSTAC works closely with NCS.

The FCC plays a strong role in reliability and privacy issues regarding the public-switched telephone network. The Network Reliability Council was established in 1992 by the FCC to provide it advice that will help prevent and minimize the impact of public telephone outages.[94] It is composed of chief executive officers from telephone companies, representatives from state regulatory agencies, equipment suppliers, and federal, corporate, and consumer users.

The federal government can also issue policies and requirements regarding the security of information stored in and exchanged between financial institutions, for example, for physical security, or contingency planning in the event of a natural disaster. Finally, the federal government regulates vendors through export controls.

In other industrial sectors (e.g., transportation), the federal government uses safety regulations to protect consumers. Some have suggested that this function could be extended to critical hardware and software products for information systems, in

[92] Donn B. Parker, SRI, Inc., "Crypto and Avoidance of Business Information Anarchy," Menlo Park, CA, September 1993.

[93] The availability, reliability, and survivability of the public-switched telephone network have been the subject of other studies and therefore is not the focus of this repro. See, e. g., National Research Council, *Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness* (Washington, DC: National Academy Press, 1989). See also Office of the Manager, National Communications System, "The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications—An Awareness Document," Arlington, VA, Sept. 30, 1993; Richard Kuhn, Patricia Edfors, Victoria Howard, Chuck Caputo, and Ted S. Phillips, "Improving Public Switched Network Security in an Open Environment," *IEEE Computer*, August 1993, pp. 32-.35; and U.S. Congress, Office of Technology Assessment, *Critical Connections: Communications for the Future*, OTA-CIT-407 (Washington, DC: U.S. Government Printing Office, January 1990), ch. 10.

[94] The council itself recently requested that the FCC disband the council, but the FCC rejected the request, offering instead that senior officers from the organizations could attend in place of the chief executive officers. The FCC also proposed a revised charter for the council, to terminate in January 1996.

order to provide safe and secure systems and a safer infrastructure overall, and to strengthen the market for "secure" products that are currently too risky for individual vendors to produce. Vendors, on the other hand, argue that regulation makes products more expensive and slows their development.[95]

These issues are beyond the scope of this report, but further study is warranted. Further study is also needed on product quality and liability issues, including guidelines or requirements for contingency plans, adoption of standards or generally accepted practices, establishment of liability for hardware and software products and services, and restrictions on the use of personal, proprietary, and copyrighted information that travels over networks. Such oversight could come from existing bodies as well as new bodies such as a privacy board (see chapter 3).

Research and Development

Much of existing knowledge in information safeguards—and in networking technology, including the Internet itself—arose from research by the federal government through the Advanced Research Projects Agency (ARPA), NIST, NSA, and other agencies, as well as from the private sector. While some of the work is applicable to civilian applications, most of the work has been oriented toward defense.[96] The National Science Foundation also has supported many research activities related to information networks through its management of the NSFNET, but security has not been a major activity. NSF has essential] y commercialized the operation of the NSFNET, but considerable work remains to safeguard the Internet and other networks.

The National Performance Review has called for NIST to coordinate development of a government-wide plan for security research and development including a baseline assessment of current research and development investment.[97] Such research and development would address many of the other areas discussed in this chapter, such as risk analysis, formal models, new products, solutions to existing vulnerabilities, standards, product evaluations, system certifications, generally accepted principles, training and certification of information security professionals, the public-key infrastructure, emergency response, and ethical principles and education.

The National Research Council has also called for research by ARPA, NSF, and others in problems concerning secure firewalls, certification authorities, and other areas.[98] The National Research Council also found that "there is a pressing need for a stronger program of university-based research in computer security. Such a program should have two explicit goals: addressing important technical problems and increasing the number of qualified people in the field. This program should be strongly interconnected with other fields of computer science and cognizant of trends in both theory and uses of computer systems."[99] The report further suggested that attention be given to cost-benefit models, new techniques, assurance techniques, computer safety, and other areas with a practical, systems approach as opposed to viewing the topics overly theoretically or in isolation.

With the Clinton Administration's effort in the National Information Infrastructure program, research and development in safeguards for networked information could take a new direction

---

95 National Research Council, op. cit., footnote 6, pp. 165-173.

96 The Internet itself grew out of ARPA's efforts in the ARPANET going back to the 1970s. The ARPANET research was intended to provide a distributed information system able to survive an attack that could eliminate a central information system.

97 Office of the Vice President, op. cit., footnote 65.

98 National Research Council, *Realizing the Information Future* (Washington, DC: National Academy Press, 1994), pp. 78-84, 101-102.

99 National Research Council, op. cit., footnote 6, Pp. 206-215.

both in the private sector and in government. Additional resources could be applied to develop and implement many of the efforts discussed in this chapter.

GOVERNMENT'S ROLE IN PROVIDING DIRECTION

The Clinton Administration is promoting the National Information Infrastructure (NII) initiative to accelerate the development of the existing infrastructure and to facilitate, for example, electronic commerce and the transfer of materials for research and education.[100] The Administration specifically calls for, among other things: review and clarification of the standards process to speed NII applications; review of privacy concerns; review of encryption technology; working with industry to increase network reliability; examining the adequacy of copyright laws; exploring ways to identify and reimburse copyright owners; opening up overseas markets; and eliminating trade barriers caused by incompatible standards.

In a separate effort to "make government work better," the Clinton Administration also is promoting its National Performance Review (NPR), which includes other actions that impact the safeguarding of networked information such as development of standard encryption capabilities and digital signatures for sensitive, unclassified data, and emphasizing the need for information security in sensitive, unclassified systems.[101] However, the specific efforts to achieve these actions mayor may not align with the NH or other efforts within the Administration, or with the wishes of the Nation at large as represented by Congress.

The National Research Council recently produced a report at the request of the National Science Foundation on information networking and the Administration's National Information Infrastructure program.[102] The report supports work by ARPA, NSF, and other groups on problems such as developing secure firewalls, promoting certification authorities and the public-key infrastructure, providing for availability of the networks, and placing stronger emphasis on security requirements in network protocol standards. The report notes that progress in security does not depend on technology alone but also on development of an overall architecture or plan, education and public attitudes, and associated regulatory policy. The report recommends a broader consideration of ethics in the information age, perhaps housed in NSF or a national commission.

An earlier report by the National Research Council on computer security called for, among other things, promulgation of generally accepted system security principles, formation of emergency response teams by users, education and training

---

100 The NII program has nine principles and objectives: 1) promote private-sector investment; 2) extend the "universal service" concept; 3) promote innovation and applications; 4) promote seamless, interactive, user-driven operation; 5) ensure information security and network reliability; 6) improve management of the radio frequency spectrum; 7) protect intellectual property rights; 8) coordinate with other levels of government and other nations; and 9) provide access to government information and improve government procurement. See Information Infrastructure Task Force, "The National Information Infrastructure: Agenda for Action," National Telecommunications and Information Administration, Washington, DC, Sept. 15, 1993. More generally, one White House official proposes that the NII initiative "will provide Americans the information they need, when they want it and where they want it—at an affordable price." (Mike Nelson, Office of Science and Technology Policy, speaking at the MIT Washington Seminar Series, Washington DC, Mar. 8, 1994.) Vice President Gore has noted that this does not mean the federal government will construct, own, or operate a nationwide fiber (or other) network, however. He notes that most of the fiber needed for the backbones is already in place, but other components need support such as switches, software, and standards. See Graeme Browning, "Search for Tomorrow," *National Journal, vol. 25, No. 12*, Mar. 20, 1993, p. 67.

101 Other privacy and security actions promoted are establish a *Privacy* Protection Board; establish uniform privacy protection Practices: develop general] y accepted principles and practices for information security; develop a national crisis response clearinghouse for federal agencies; reevaluate security practices for national security data; foster the industry-government partnership for improving services and security in public telecommunications; implement the National Industrial Security Program; develop a comprehensive Internet security plan and coordinate security research and development. (Office of the Vice President, op. cit., footnote 65.)

102 National Research Council, op. cit., footnote 98, pp. 78-84,101-102,148-171.

BOX 2-7: What Are Clipper, Capstone, and SKIPJACK?

SKIPJACK is a classified, symmetric-key, encryption algorithm that was developed by the National Security Agency to provide secure voice and data communications while allowing lawful access to those communications by law-enforcement.[1] According to the Clinton Administration, one reason the algorithm is classified is to prevent someone from implementing it in software or hardware with the strong algorithm, but without the feature that provides law enforcement access [2] SKIPJACK is specified in the federal Escrowed Encryption Standard (EES—see chapter 4),

Like the Data Encryption Standard (DES—see box 4-3), SKIPJACK transforms a 64-bit input block into a 64-bit output block, and can be used in the same four modes of operation specified for the DES The secret-key length for SKIPJACK is 80 bits, however, as opposed to 56 bits for the DES, thereby allowing over 16,000,000 times more keys than the DES [3] SKIPJACK also scrambles the data in 32 rounds per single encrypt/decrypt operation, compared with 16 rounds for the DES,

Mykotronx currently manufactures an escrowed-encryption chip-the MYK78, commonly known as the Clipper chip-that implements the SKIPJACK algorithm to encrypt communications between telephones, modems, or facsimile equipment The chip is intended to be resistant to reverse engineering, so that any attempt to examine the chip will destroy its circuitry The chip can encrypt and decrypt with another synchronized chip at the rate of 5 to 30 million bits per second depending on the mode of operation, clock rate, and chip version,

The chip is initially programmed with specialized software, an 80-bit *family key* (as of June 1994 there was only one family of chips), a unique 32-bit serial number (the *chip identifier),* and an 80-bit key specific to the chip (called the *chip unique key)* The chip unique key is the "exclusive or" combination of two 80-bit *chip unique key components,* one component is assigned (with the chip identifier) to each of the escrow agents chosen by the Attorney General [4]

The Clipper chip is currently implemented in the AT&T Surity Telephone Device 3600 When a user (Alice) wishes to secure her conversation with another user (Bob) using their Model 3600 devices, she pushes a button and the two devices first generate an 80-bit *session key* using a proprietary, enhanced version of the Diffie-Hellman public-key technique In this way, each device can calculate the session key without actually sending a complete key over the network where it could be intercepted

---

[1] See Dorothy E Denning, "The Clipper Encryption System, " *American Scientist*, vol 81, July-August 1993, pp 319-322, and Dorothy E Denning, Georgetown University, "Cryptography and Escrowed Encryption, " Nov 7, 1993

[2] "Addltlonally, the SKIPJACK algorithm is classified Secret-Not Releasable to Foreign Nationals This classification reflects the high quality of the algorithm, i e , it incorporates design techniques that are representative of algorithms used to protect classified information Disclosure of the algorithm would permit analysis that could result in discovery of these classified design techniques, and this would be detrimental to national security " Ernest F Brickell et al , "Skipjack Review Interim Report The Skipjack Algorithm," July 28, 1993, p 7

[3] The "exhaustive search" technique uses various keys on an input to produce a known output, until a match Is found or all possible keys are exhausted The DES's 56-bit key length yields over 72 trillion possible keys, while SKIPJACK' s 80-bit key length yields over 16 million more times as many keys as DES According to the SKIPJACK review panel, if the cost of processing power is halved every 15 years, it will take 36 years before the cost of breaking SKIPJACK through the exhaustive search technique will equal the cost of breaking DES today Ibid

[4] The creation of the chip unique key components is a very important step, if an adversary can guess or deduce these components with relative ease then the entire system is at risk These key components are created and the chips are programmed inside a secure facility with representatives of each escrow agent The specific process is classified, and an unclassified description was not available as of this writing

(continued)

BOX 2-7 (cont'd.): What Are Clipper, Capstone, and SKIPJACK?

The devices then exchange the Law Enforcement Access Field (LEAF) and an "initialization vector" The LEAF contains the session key (encrypted with the chip unique key), the chip identifier, and a 16-bit authentication pattern, which are all encrypted with the family key Each device then decrypts the LEAF, confirms the authentication data, and establishes an active link. The session key is then used to encrypt and decrypt all messages exchanged in both directions

Each device also displays a character string. If the characters displayed on Alice and Bob's devices are different, this reveals an interception and retransmission of their communication by an eavesdropper, in what is called a "man-in-the-middle" attack

Law-enforcement agents are required to obtain a court order to monitor a suspected transmission If they begin monitoring and ascertain that the transmission is encrypted using the Model 3600, agents first must extract and decrypt the LEAF (using the family key) from one of the devices The decrypted LEAF reveals the chip Identifier With the chip identifier, they can request the chip unique key component from each of the two escrow agents With both components, they can decrypt session keys as they are intercepted, and therefore decrypt the conversations [5]

The Capstone chip also Implements the SKIPJACK algorithm, but Includes as well the Digital Signature Algorithm (used in the federal Digital Signature Standard—see chapter 4), the Secure Hash Standard, the classified Key Exchange Algorithm, circuitry for efficient exponentiation of large numbers, and a random number generator using a pure noise source Mykotronx currently manufactures the Capstone chip under the name MYK80, and the chip is also resistant to reverse engineering Capstone is designed for computer and communications security, and its first implementation is in PCMCIA cards for securing electronic mail on workstations and personal computers

[5] The initial phases of the system rely on manual procedures for preventing law enforcement frOm using escrowed keys affer the court order expires or on communications recorded previous to the court order For example, the officer must manually enter the expiration date into the decrypt processor, manually delete the key when the court order expires, and manually complete an audit statement to present to the escrow agents The target system aims to enforce the court order by including with the escrowed keys an electronic certificate that is valid only for the period of the court order The decrypt processor is Intended to block the decryption when the certificate expires, and automatically send an audit statement electronically to theescrowagents As of June 1994, the design was not complete (Miles Smid Manager, Security Technology, NIST, presentation at NIST Key Escrow EncryptIon Workshop, June 10, 1994)

SOURCE Office of Technology Assessment, 1994, and sources cited below

programs to promote public awareness, review for possible relaxation of export controls on implementations of the Data Encryption Standard, and funding for a comprehensive program of research.[103]

In this environment, the federal government has several important roles that affect the safeguarding of networked information. Even though these roles are all intended to promote the needs of the nation's individuals and organizations,

[103] National Research Council, op. cit., footnote 6.

sometimes there are conflicts.[104] These conflicts are sometimes so polarizing or so important that attempts to resolve them at an administrative level can lead to poor decisions, or endless legal and operational problems from implementing a policy that has only weak support from stakeholders. While many of the *details* involve technology, the *fundamental debates* about national values and the role of government in society can only be resolved at the highest levels (see boxes 2-7 and 2-8).[105]

Thus, networked information poses a particularly difficult dilemma for government policymakers: good security is needed to protect U.S. personal, business, and government communications from domestic and foreign eavesdroppers. However, that same security then may hinder U.S. intelligence and law-enforcement operations. Aspects of this dilemma are manifested in specific issues as the technology develops, such as the following examples:

- Cryptography policy is the focus of several debates, including export controls on cryptography and development of federal cryptographic standards (see chapter 4).
- Digital Telephony legislation[106] has been proposed that would require telecommunications carriers "to ensure that the government ability to lawfully intercept communications is not curtailed or prevented entirely by the introduction of advanced technology.''[107] (A discussion of digital telephony is outside the scope of this report.)
- Anonymous transactions. Many privacy advocates argue that certain monetary or other transactions (such as request of library materials) be

104 These roles are as follows: First, government can provide a democratic framework for resolving debates and writing law to regulate activities. Second, it is a buyer and user of products and services; because of its size it can sometimes move the market in ways no other single buyer can, and it must also safeguard its own agency networks. Third, it is a supplier of products and services, such as census and other information. Fourth, it is at times a catalyst that can enter the marketplace to stimulate research and development or establish new institutions and standards that eventually operate on their own. Finally, it intercepts communications for law-enforcement purposes and intelligence gathering.

105 See also Lance J. Hoffman and Paul C. Clark, "Imminent Policy Considerations in the Design and Management Of National and International Computer Networks," *IEEE Communications Magazine,* February 1991, pp. 68-74; James E. Katz and Richard F. Graveman, "Privacy Issues of a National Research and Education Network," *Telematics and Informatics, vol. 8, No. 1/2,* 1991; Marc Rotenberg, "Communications Privacy: Implications for Network Design," *Communications of the ACM, vol. 36, No. 8,* August 1993, pp. 61 -68; and Electronic Privacy Information Center, *1994 Cryptography* and *Privacy Sourcebook*, David Banisar (cd.) (Upland, PA: Diane Publishing, 1994).

106 The proposed Digital Telephony and C$_{ommuni}$c$_{at}$io$_{ns}$ privacy Act of 1994 was in draft at *this* writing. Modern digital switches are actually very fast computers that arrange and bill calls using complex software and pack thousands of calls together into optical fibers. The Clinton Administration claims that not all such technology has been designed or equipped to meet the intercept requirements of law enforcement. It claims that law enforcement should be able to intercept those communications in certain circumstances, provided that a court order is obtained and officials use appropriate measures. Critics charge that legislation is unnecessary or costly at best, and undesirable at worst; many argue that individuals and corporations should have the right to absolutely secure their conversations if they choose.

107 See Dorothy E. Denning, "To Tap or Not To Tap," and related articles in *Communications of the ACM,* vol. *36, No.* 3, March 1993, pp. 24-44.

BOX 2-8: Fair Cryptosystems—An Alternative to Clipper?

The Clinton Administration's key-escrow encryption initiative (e.g., Clipper and the Escrowed Encryption Standard) is the most publicized escrowed-encryption scheme to date Other schemes for third-party "trusteeship" of keys are possible, however One so-called *fair cryptosystem* scheme claims to resolve many of the objections to the Administration's proposal.[1]

Fair cryptosystems allow the user to split a secret key into any number of key components that can be assigned to trusted entitles The user (e g , a corporation) might spilt the key and assign one piece to a federal government agency and the other to a trusted third party, such as a bank Each trustee would receive a signed message from the user, with the key component and its "shadows "The shadows demonstrate to the trustee that the key component is indeed associated with the corresponding components assigned to the other trustees—without revealing the other components The certificate would also indicate where the other key components are held In a criminal Investigation, following due process, a law-enforcement agency could obtain the key components from the two trustees

Other combinations are possible, for example, the user could design a system such that any three of four key components might be sufficient to decrypt its communications For each secure telephone, the user might also keep a complete secret key for internal investigations, or in case of loss or sabotage of data

The algorithms used to Implement fair cryptosystems could Include a time variable so that the deposited key components change periodically Or, the key components could be made to calculate a set of session keys (which could change periodically) that would be valid for only the prescribed time. The user would choose the actual algorithm, which could be one of many that are subject to public review.

Fair cryptosystems also could be Implemented in software to reduce cost In a software implementation of a fair public-key cryptosystem, the user would be motivated to assign the key components to trustees in order to obtain permission to post his or her "public keys" in a key distribution or certification system The public keys are used to initiate communications and to perform electronic transactions among parties who have not agreed in advance on common secret keys Thus, the user has a great incentive to have his or her public keys made available Without such permission from certification authorities, the user would have to distribute his or her public keys in a less efficient fashion In a hardware Implementation, chips can be programmed to require proof that deposit of key components with trustees has taken place [2]

This and other related schemes[3] claim to address both corporate[4] and law-enforcement needs The Escrowed Encryption Standard proponents note that the fair cryptography schemes require an action on the part of the user to submit the key components to trustees, while the EES does not—users cannot keep the escrowed keys from its escrow agents. Critics of the EES proposal note, however, that criminals and adversaries can, nevertheless, superencrypt over EES encryption (or any other scheme) Foreign companies and governments, and many others, also may find key-escrowed encryption objectionable if the U S government keeps the escrowed keys

[1] Silvio Micali, Laboratory for Computer Science, Massachusetts Institute of Technology, "Fair Cryptosystems," MIT Technical Report MIT/LCS/TR-579 b, November 1993 See also Silvio Micali, "Fair Cryptosystems vs Clipper Chip A Brief Comparison," Nov 11, 1993, Silvio Micali, "Fair Cryptosystems and Methods of Use," U S Patent No 5,276,737 (Jan 4, 1994), and U S Patent No 5,315 658(May 24, 1994) NIST announced a non-exclusive licensing agreement in principle with Silvio Micali The license for the 737 and 658 patents would cover everyone "using a key escrow encryption system developed for authorized government law enforcement purposes" (NIST press release, July 11, 1994)

[2] Frank W Sudia, Bankers Trust Company, personal communication, Apr 22, 1994

[3] M J B Robshaw, RSA Laboratories, "Recent Proposals To Implement Fair Cryptography," No TR-301, Oct 191993

[4] Dorm B parker, SRI International Menlo Park, CA, "Crypto and Avoidance of Business information Anarchy, 'September 1993

SOURCE Office of Technology Assessment, 1994, and cited sources

kept anonymous.[108] On the other hand, some businesses and law enforcement have an interest in maintaining the electronic trail for billing, marketing, or investigative purposes. In one example, a debate could arise over the privacy or anonymity of electronic monetary transactions over information networks. Such "electronic cash" or other transactions would need strong safeguards to assure that the cash was exchanged without tampering or monitoring and could be made anonymous to protect individual privacy.[109] These safeguards might also eliminate the paper trail that exists in many current transactions, facilitating money laundering and extortion.[110] In such an event, law-enforcement authorities may seek to implement provisions that allow such transactions to be monitored in certain cases. (See OTA, *Information Technologies for Control of Money Laundering,* forthcoming 1995.)

- Electronic commerce. Digital signatures and other cryptographic techniques can be used to protect electronic documents and enforce electronic contracts. The development of a public-key infrastructure is strategic to further expansion of electronic commerce. Cryptographic techniques and other safeguards may be used to secure or track copyrighted documents, bill users, collect fees, and so forth. (See chapter 3.)

---

108 Issues relating t. anonymity and "digital libraries" are discussed in U.S. Congress, Office Of Technology Assessment, *Accessibility and Integrity of Networked Information Collections,* background paper prepared for OTA by Clifford A. Lynch, BP-TCT- 109 (Washington, DC: Office of Technology Assessment, July 1993).

109 See David Chaum, "Achieving Electronic Privacy," *Scientific American,* August 1992, pp. 96-101.

110 Sebastiaan von Solms and David Naccache, "On Blind Signatures and perfect Crimes," *Computers and Security,* vol. *1 I,* No. *6,1992,* p. 581.