Appendix A: Selected Topics in Computer Security

Originators of existing computer-based patient record systems have been faced with the problem of ensuring their systems will provide high levels of clinical access and utility for their personnel and still maintain the security and confidentiality of patient information. Data security and confidentiality y remain a central concern as the health care industry contemplates full automation and implementation of a networked computer system for individual health care information.[1] The need for information security and trust in health care information computer systems, as in computer systems generally, is described in terms of three fundamental goals: *confidentiality, integrity, and access.*[2] *Confidentiality* involves control over who has access to information. *Integrity* assures that information and programs are changed only in a specified and authorized manner, that computer resources operate correctly and that the data in them is not subject to unauthorized changes, A system meeting standards for *access* allows authorized users access to information resources on an ongoing basis.[3] The level of security provided may vary from one application to another.[4] For example, security in computer systems containing classified national security information may have different specifications than a computer system designed for a nondefense manufacturing company. Security in health care information systems would likely be designed somewhere along this spectrum. The emphasis given to each of the three requirements (confidentiality, integrity, and access) depends on the nature of the application, An individual system may sacrifice the level of one requirement to obtain a greater degree of another. For example, to allow for increased levels of availability of information, standards for confidentiality may be lowered. Thus, the specific requirements and controls for information security can vary.[5] Applications linked to external systems will usually require different security controls from those without such conections because access is more open.

A security *policy is* the framework within which an organization, e.g., a hospital, outpatient clinic, mental health facility, *or* health insurance company, establishes needed levels of information security to achieve,

[1] **Institute of Medicine,** *The Computer-Based Patient Record: An Essential Technology for Health Care,* Richard S. Dick, and Elaine B. Steen, eds., (Washington DC: National Academy Press, 1991), pp. 42-43,65-66, 83-85. This is a publication of the Committee on Improving the Patient Record, Division of Health Care Services. See also, Gretchen Murphy, "System and Data Protection" *Aspects of the Computer-Based Patient Record,* **Marion** J. Ball and Morns F. Cone% eds., (New York, NY: Springer-Verlog, 1992), p. 205.

[2] See Gretchen Murphy, op. cit., footnote 1. For general definitions of security terms and concepts, see Dennis Longley, Michael Shain, William Caelli, *Information Security: Dictionary of Concepts, Standards and Terms (New* York, NY: Stockton Press, 1992).

[3] Charles P. Pfleeger, *Security in Computing* (Englewood Cliffs, NJ: Prentice Hall, Inc. 1989), pp. 5-6.

[4] National Research Council, *Computers at Risk: Safe Computing in the Information Age* (Washington, DC: National Academy of Sciences, 199 1), p. 55. This is a publication of the System Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications.

[5] Ibid., p. 52.

among other things, the desired confidentiality goals. A policy is a statement of information values, protection responsibilities, and organizational commitment for a system. It is a set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive inforrnation.[6] A policy is implemented by taking action guided by management control principles and utilizing specific security standards, procedures, and mechanisms.[7] A security policy, to be useful, must state the security need (e.g., for confidentiality-that data shall be accessed only by authorized individuals) and also address the circumstances under which that need must be met through operating standards. Institutions must access the threats to a system, assign a level of concern to each, and state a policy in terms of which threats are to be addressed.[8]

Management controls are administrative, technical, and procedural mechanisms that implement a security policy. Some management controls are concerned with protecting information and information systems, but the concept of management controls is more than merely a computer's role in enforcing security. Management controls are exercised by users as well as managers. An effective program of management controls is necessary to coverall aspects of information security, including physical security, classification of information gauged to the desired levels of confidentiality and access, means of recovering from breaches of security, and training to instill awareness and user acceptance. There are trade-offs among controls. If technical controls are not available, procedural controls might be used until a technical solution is found.[9] Nevertheless, technical controls are useless without procedural controls and robust security policy.

Breaches in security sometimes occur by outside sources, but most often by "insiders' '—individuals authorized to use the system. According to the report of the Workgroup for Electronic Data Interchange to the Secretary of the U.S. Department of Health and Human Services, the Health Care Financing Administration (HFCA) believes that the security technology available to systems developers is adequate to protect against breaches by an outside source, and does not consider a breach of the system by outsiders a great concern. HFCA'S concern lies with breaches of the system by ''insiders, '' individuals who are authorized to use the system.[10] Access control alone cannot prevent violations of the trust people and institutions place in individuals. Inside violations have been the source of much of the computer security problem in industry. Technical security measures may prevent people from doing unauthorized things, but cannot prevent them from misusing the capabilities with which they are entrusted to allow them to perform their job function. Thus, to prevent security problems resulting from violations of trust, one must depend primarily on human awareness of what others in an organization are doing and on separation of duties, as in regular accounting controls.[11] But even a technically sound system with informed, watchful management and responsible users is not free of vulnerabilities. The risk that remains must be managed by auditing, backup, and recovery procedures supported by alertness and creative responses. Moreover, an organization must have administrative procedures in place to bring suspicious actions to the attention of responsible persons who can—and will-inquire into the appropriateness of such actions.[12] In addition to these Precautions, damage can also be avoided through close personnel checks to avoid hiring employees with

---

6 See, Dennis Longley et al., op. cit., footnote 2, pp. 467468.

7 National Research Council, op. Cit., footnote 4, p. 50.

8 Ibid.

9 Ibid.

10 U.S. Department of Health and Human Services, Workgroup for Electronic Data Interchange, Report to the Secretary, July 1992, p. 29. However, the report later states that computer "hackers" have circumvented the security systems of a variety of computer systems; while access in some cases was limited to unauthorized 'browsing' through database records, other instances of access have been accompanied by alteration or deletion of data or disruption of system operations.

11 See U.S. Congress, Office of Technology Assessment, *Defending Secrets, Sharing Data:* New *Locks and Keys for Electronic Information,* OTA-CIT-310 (Washington DC: U.S. Government Printing Office, October 1987); Robert H. Courtney, Jr., "Considerations of Information Security for Large Scale Digital Libraries,' contractor report prepared for the Office of Technology Assessment, Mar. 27, 1993.

12 National Research Council, op. cit. footnote 4, pp. 50-51.

questionable backgrounds in areas where sensitive data are available, periodic analysis of the computer system and the sensitivity of its data, and separation of critical duties between employees.

Technical Safeguards

Technical safeguards, along with administrative and procedural measures, are best established within the system application or program, e.g., medical record system software, instead of relying on the network infrastructure for security. These technical provisions include the following:

Cryptography: can be used to encode data before transmission or while stored in a computer, provide an electronic signature and/or to verify that a message has not been tampered with. Cryptography can be used to 1) *encrypt* plain text to provide confidentiality 2) *authenticate* a message to ensure integrity and to prevent fraud by third parties, and 3) create a *digital signature* that authenticates a message and protects against fraud or repudiation by the sender.[13]

Personal identification and user verification techniques: help ensure that the person using a communication or computer system is the one authorized to do so and, in conjunction with access control systems and other security procedures, that authorized users can be held accountable for their actions.

Access control software and audit trails: can help protect information systems from unauthorized access and keep track of each user's activities.

Computer architecture: may be specifically designed to enhance security.

Communications linkage safeguards: can hamper unauthorized access to computers through phone lines or other networks. 14

CRYPTOGRAPHY

Cryptography is one method of protecting data vulnerable to unauthorized access and tampering. Cryptography, along with electronic signatures, can be used to protect confidentiality and integrity.

Confidentiality of information can be provided through encryption. *Encryption*[15] *is* a process of encoding a message so that its meaning is not obvious; decryption transforms an encrypted message back into its normal form.[16] When a message is encrypted, it is encoded in a way that can be reversed only with the appropriate *key.*[17] *Maintaining* confidentiality requires that only authorized parties have the decrypting key.

Integrity can be provided through message authentication. An "authentic" message is one that is not a replay of a previous message, has arrived exactly as it was sent (without errors or alterations), and comes from the stated source (not forged or falsified by an impostor or fraudulently altered by the recipient). Encryption algorithms can be used to authenticate messages, but encryption in itself does not automatically authenticate a message.

Message authentication techniques are based either on public or secret knowledge. Authentication techniques based on public knowledge can check against errors, but not against malicious modifications. Message authentication using secret parameters means that a message cannot be forged unless the secret parameters are compromised or one of the parties is doing the forging.

Digital Signature & The trend away from paper-based systems into automated electronic systems has brought about a need for a reliable, cost-effective way to replace the handwritten signature with a digital signature. Encryption or message authentication alone

---

13 See *Defending Secrets,* op. *cit. !* footnote 11, **pp. 174-180. See also,** *Datapro Reports on Information Security,* "Host File Encryption Software **Overview, " 1S54-001-101, May 1992.**

14 See generally, *Defending Secrets,* op. cit., footnote 11. See also, *Datapro Reports on Information Security,* "Host Security Software," **1S50-140-103,** November 1992, and generally, Dennis Longley et al., op. cit., foomote 2,

15 Encryption is an essential method for ensuring the three goals of computer security: confidentiality, integrity, and access. Encryption provides confidentiality for data. Encryption can also be used to achieve integrity, since data that cannot be read, generally cannot be changed. Encryption is important in establishment of secure communication protocols (a sequence of steps taken by two or more parties to accomplish some task) between users. Some of these protocols are implemented to ensure access to data. *Defending Secrets,* op. cit., footnote 11, pp. 54-63. See also, *Datapro Reports,* op. cit., footnote 13.

16 The words encode and decode, or encipher and decipher, are often used instead of the verbs encrypt and decrypt. A system fOr encryption and decryption is called a cryptosystem. Charles P. Pfleeger, op. cit., footnote 3, p. 23.

17 Charles P. Pfleeger, op. cit., footnote 3, p. 23.

can only safeguard against the actions of third parties. They cannot fully protect one of the communicating parties from fraudulent actions by any other, such as forgery or repudiation of a message or transaction. Nor can they resolve contractual disputes between two parties. Like a handwritten signature, a digital signature can be used to identify and authenticate the originator of the information. A digital signature can also be used to verify that information has not been altered after it is signed, providing for message integrity.

In August 1991, NIST proposed the Digital Signature Standard (DSS) as a Federal Information Processing Standard (FIPS), suitable for use by corporations, as well as civilian agencies of the government. The DSS specifies a Digital Signature Algorithm (DSA) for use in computing and verifying digital signatures. NIST suggests that DSA can be used in such applications as electronic mail systems, legal systems, and electronic funds transfer systems. Some controversy surrounds NIST'S choice of the DSS techniques.[18]

Encryption Algorithms-The original form of a message is known as *plaintext,* and the encrypted form is called *ciphertext.* Messages are encrypted using mathematical algorithms implemented in hardware or software, and secrecy is provided through use of cryptographic keys. These keys are seemingly random sequences of symbols. The encryption algorithm is a mathematical process that can transform plain text into ciphertext and back again, with each transformation depending on the value of the key. *Symmetric ciphers* use the same key for encryption and decyption. One key, known to both the sender and receiver of a message, is used to both encrypt and decrypt the message. Symmetric keys present problems of key distribution, since secrecy in the key must be maintained by both parties to the communication. The traditional means of key distribution-through couriers-places the security of the cipher system in the hands of the courier(s). Courier-based key distribution presents challenges when keys need to be changed often.

Asyrnrnetric ciphers use different but related keys. One key is used to encrypt and another to decrypt a message.[19] A special class of asymmetric ciphers are public-key ciphers, in which the "public" encrypting key need not be kept secret to ensure a private communication. Rather, Party A can publicly announce his or her public key, PKA, allowing anyone who wishes to communicate privately with him or her to use it to encrypt a message. Party A's "secret" decrypting key (SKA) is kept secret, so that only A or someone else who has obtained his or her decrypting key can easily convert messages encrypted with PKA back into plaintext.

Determining g the secret decrypting key is difficult, even when the encrypted message is available and the public key is known; in practice only authorized holders of the secret key can read the encrypted message. If the encrypting key is publicly known, however, a properly encrypted message can come from any source, and there is no guarantee of its authenticity. It is thus crucial that the public encrypting key be authentic. An impostor could publish his or her own public key, PKI, and pretend it came from A in order to read messages intended for A, which he or she could intercept and then read using his or her own secret key, SKI.

Therefore, the strength of a public key cipher system rests on the authenticity of the public key. A public key system can be strengthened by providing means for certifying public keys via digital signature, a trusted third party, or other means.[20]

Techniques for encrypting messages based on mathematical algorithms vary widely in the degree of security they provide. The various algorithms differ in the following ways:

- The mathematical sophistication and computational complexity of the algorithm itself. More complex algorithms may be harder for an adversary to break.
- Whether the algorithm is for a symmetric cipher or for an asymmetric one.

---

18 NIST originally chose DSS, in part because of patent considerations. Some critics of the choice (including the company marketing the RSA system) have asserted that the RSA algorithm is superior and that NIST deliberately chose a weaker cipher. In late 1991, NIST's Computer Security and Privacy Advisory Board went on record as opposing adoption of the proposed DSS.

19 *Defending Secrets,* op. cit., footnote 11, p. 176.

20 *Defending Secrets,* op. cit., footnote 11, p. 180.

- The length of the key used to encrypt and decrypt the message. Generally, for an algorithm of a given complexity, longer keys are more secure.
- Whether the algorithm is implemented in software or hardware.
- Whether the algorithm is open to public scrutiny. While some argue that users have more confidence in an algorithm if it is publicly known and subject to testing, the National Security Agency and others assert that secret algorithms are more secure.[21]

Data **Encryption Standard (DES)--The U.S. Data** Encryption Standard (DES) is a well-known example of a symmetric cryptosystem and probably the most widely known modern encryption algorithm. DES was developed to protect unclassified computer data in Federal computer systems against passive and active attacks in communication and computer systems.[22] DES is the result of a National Bureau of Standards initiative to create an encryption standard. Based on an algorithm developed by IBM, DES was officially adopted as a Federal Standard in November, 1977, and endorsed by the National Security Agency.[x] After over 10 years of the public scrutiny, most experts are confident that DES is secure from virtually any adversary except a foreign government.[x] DES is a private key cryptographic algorithm, which means that the confidentiality of the message, under normal conditions, is based on keeping the key secret between the sender and receiver of the message.[25] DES specifies a cryptographic algorithm that converts plaintextrttext to ciphertext using a 56-bit key. Encryption with the DES algorithm consists of 16 "rounds' of operations that mix the data and key together in a prescribed manner. The goal is to so completely scramble the data and key that every bit of ciphertext depends on every bit of the data plus every bit of the key.[26]

In early 1993, the executive branch announced its policy to implement a new encryption device called "Clipper Chip," discussed in box A-1.

RSA—RSA is a patented public key encryption system that has been in use since 1978. It was invented at the Massachusetts Institute of Technology (MIT) by Ronald Rivest, Adi Shamir, and Leonard Adelrnan. These three inventors formed RSA Data Security, Inc. in 1982, and obtained an exclusive license for their invention from MIT, which owns the patent. The firm has developed proprietary software packages implementing the RSA cipher on personal computer networks. These packages, sold commercially, provide software-based communications safeguards, including message authentication, key management, and encryption. RSA relies on the difficulty of factoring large numbers to devise its encryption codes. Asymmetric cipher systems (like RSA) are more efficient than symmetric ones for digital signatures.[27]

9 Personal Identification and User Verification

The purpose of user verification systems is to ensure that those accessing a computer or network are authorized to do so. Personal identification techniques are used to strengthen user verification by ensuring that the person actually is the authorized user.[28] Authenti-

21 *Defending Secrets,* op. cit., footnote 11, pp. 54-55.

22 U.S. Department of Commerce, National Institute of Standards and Technology, NCSL Bulletin, *Advising Users oft Computer Systems Technology,* June 1990.

23 Charles P. Pfleeger, op. cit., footnote 3, p. 107.

24 According t. NIST, appropriate applications of DES include electronic funds transfer, privacy protection of personal information, personal authentication password protection, access control, etc., U.S. Department of Commerce, National Institute of Standards and Technology, NCSL Bulletin, *Advising Users on Computer Systems Technology,* June 1990, pp. 1-2.

25 *Defending Secrets,* op. cit., footnote 11, p. 55.

26 Ibid.

27 Ibid., p. 63. See also, *Datapro Reports on Information Security,* ''Microcomputer Encryption and Access Control: Technology Overview,' 1S31-001-125, April 1991, and Dennis Longley et. al., op. cit., footnote 2, pp. 165-171.

28 *Defending Secrets,* op. cit., footnot 11, p. 72. See also, *Datapro Reports on information Security,* ''Host Access Control Software Overview,' 1S52-001-103, July 1992,

Box A-l–The CLIPPER Chip

On April 16,1993, the White House announced anew initiative to create encryption technology that can be used to protect proprietary information, and the privacy of personal phone conversations and electronically transmitted data. The technology is also aimed at preserving the ability of Federal, State, and local law enforcement agencies with legal authorization to conduct a wiretap to intercept phone conversations. The system involves establishment of a "key-escrow" system, in which each device containing the chip will have two unique "keys" to decode messages encoded by the device. When the device is manufactured, the two keys will be deposited separately in two "key-escrow" databases that will be established by the Attorney General. Access to these keys would be limited to government officials with legal authorization to conduct a wiretap.

As of this writing, public debate about the technology involved in CLIPPER Chip, as well as about the legal implications of implementing such a system continue. However, the National institute of Standards and Technology has released the following information about the CLIPPER Chip:

The CLIPPER Chip was developed by the National Security Agency. It is a hardware oriented, cryptographic device that implements asymmetric encryption/decryption algorithm and what is referred to as a "law enforcement satisfying" key escrow system. While the key escrow system design is not completely designed, the cryptographic algorithm (called SKIPJACK) is complete as of this writing (and classified SECRET).

According to the information provided by NIST, the cryptographic algorithm has the following characteristics:

1. **symmetric, 80-bit key encryption/decryption algorithm;**
2. **similar in function to Data Encryption Standard (DES);**
3. **32 rounds of processing per single encrypt/decrypt operation; and**
4. **design started by NSA in 1985; evaluation completed in 1990.**

The CLIPPER chip is just one implementation of the cryptographic algorithm. The CLIPPER Chip designed for the AT&T commercial secure voice product has the following characteristics:

1. **functions specified by NSA; logic designed by MYKOTRONX; chip fabricated by VLSI, Inc.; manufactured chip programmed (made unique) by MYKOTRONX security equipment**

cation technology provides the basis for access control in computer systems. If the identity of a user can be correctly verified, legitimate users can be granted access to system resources. Conversely, those attempting to gain access without proper authorization can be denied. Once a user's identity is verified, access *control* techniques may be used to mediate the user's access to data.

The traditional method for authenticating users has been to provide them with a secret password, which must be used when requesting access to a particular system. However, authentication that relies solely on passwords has often failed to provide adequate protection for computer systems for a number of reasons, including careless use and misuse--e.g., writing passwords on the terminal, under a desk blotter, etc. Where password-only authentication is not adequate for an application, a number of alternative methods can be used alone or in combination to increase the security of the authentication process. User verification systems generally involve a combination of criteria, such as something in an individual's possession, e.g., a coded card or token (token-based authentication), something the individual knows, e.g., a memorized

manufacturers willing to follow proper security procedures for handling and storage of the programmed chip;
2. reportedly resistant to reverse engineering, even against a sophisticated, well funded adversary;
3. 15-20 megabit per second eencryption/decryption constant throughout once cryptographic synchronization is established with distant CLIPPER Chip;
4. the chip programming equipment writes (one time) the following information into a special memory (called VROM or VIA-Link) on the chip:
   a. (unique) serial number
   b. (unique) unit key
   c. family key
   d. specialized control software
5. Upongeneration (or entry) of a session key in the chip, the chip performs the following actions:
   a. Encrypts the 80 bit session key under the unit key producing an 80 bit intermediate result;
   b. Concatenates the 80 bit result with the 25 bit serial number and a 23 bit authentication pattern (total of 128 bits);
   c. Enciphers this 128 bits with family key to produce a 128-bit cipher block chain called the Law Enforcement Field (LEF)
   d. Transmits the LEF at least once to the intended receiving CLIPPER Chip.
   e. The two communicating CLIPPER chips use this LEF to establish cryptographic synchronization.
6. Once synchronized, the CLIPPER chips use the session key to encrypt/decrypt data in both directions;
7. The chips can be programmed to not enter the secure mode if the LEF field has been tampered with (e.g., modified, superencrypted, replaced);
8. CLIPPER Chips are expected to be available from a second source in the future;
9. CLIPPER Chips are expected to be modified/ungraded in the future;
10. According to NIST CLIPPER chips presently cost $16.00 (unprogrammed) and $26.00 (programmed),

SOURCE: National Institute of Standards and Technology, Press Release, May 1993.

password or personal identification number (password authentication), or some physical characteristic of the user, e.g., a fingerprint or voice pattern (biometric authentication) .29

Token-based authentication requires the system user to produce a physical token that the system can recognize as belonging to a legitimate user. These tokens typically contain information that is physically, magnetically, or electronically coded in a form that can be recognized by a host system. The most sophisticated tokens take the form of smart cards,' and contain one or more integrated circuits that can store and, in some cases, process information.[30] Token-based systems reduce the threat from attackers who attempt to guess or steal passwords, because the attacker must either fabricate a counterfeit token or steal a valid token from a user and must know the user's password.

Biometric authentication relies on a unique physical characteristic to verify the identity of system users. Common biometric identifiers include fingerprints,

29 Department of Commerce, National Institute of Standards and Technology, CSL Bulletin, *Advising Users on Computer Systems Technology,* November 1991.

30 For further discussion of use of smart card systems for health care information, see ch. 3.

written signatures, voice patterns, typing patterns, retinal scans, and hand geometry. The unique pattern that identifies a user is formed during an enrollment process, producing a template for that user. When a user wishes to authenticate access to the system, a physical measurement is made to obtain a current biometric pattern for the user. This pattern is compared to the enrollment template in order to verify the user's identity, Biometric authentication devices tend to cost more than password or token-based systems because the hardware required to capture and analyze biometric patterns is more complicated. However, biometrics provide a very high level of security because the authentication is directly related to a unique physical characteristic of the user that is difficult to counterfeit. At the same time, passwords, authentication tokens, and biometrics are subject to a variety of attacks.

New technologies and microelectronics, which are more difficult to counterfeit, have emerged to overcome these problems. These technologies have also enabled the merging of the identification criteria, so that one, two, or all the criteria can be used as needed. Microelectronics make the new user identification methods compact and portable. Electronic smart cards now carry prerecorded, usually encrypted access control information that must be compared with data that the proper authorized user is required to provide, such as a memorized personal identification number or biometric data like a fingerprint or retinal scan.[31] Merging criteria allows authentication of the individual to his or her card or token and only then allows access to the protected computer or network. This can increase security since, for example, one's biometric characteristics cannot readily be given away, lost, or stolen. Biometrics permit automation of the personal identification/user verification process.

ACCESS CONTROL SOfTWARE AND AUDIT TRAILS

Once the identity of a user has a been verified, it is still necessary to ensure that he or she has access only to the resources and data that he or she is authorized to access. For host computers, these functions are performed by access control software. Records of users' accesses and online activities are maintained as audit trails by audit software. Access control methods include user identification codes, passwords, login controls, resource authorization, and authorization checking, These methods, as well as use of audit trails and journaling techniques, are discussed in box A-2.

COMPUTER ARCHITECTURE

The computer itself must be designed to facilitate good security, particularly for advanced security needs. For example, it should monitor its own activities in a reliable way, prevent users from gaining access to data they are not authorized to see, and be secure from sophisticated tampering or sabotage. However, while changes in computer architecture will gradually improve, particularly for larger computer users, more sophisticated architecture is not the primary need of the vast majority of current users outside of the national security community. Good user verification coupled with effective access controls, including controls on database management systems, are the more urgent needs for most users.[32]

COMMUNICATIONS LINKAGES SAFEGUARDS

Computers are vulnerable to misuse through the ports that link them to telecommunication lines, as well as through taps on the lines themselves. As computers are linked through telecommunication systems, the problem of dial-up misuses by hackers may increase.

For purpose of this study, of particular interest in the area of medical information are port protection devices. [33] One means of limiting misuse via dial-up lines has been dial-back port protection devices. Newer security modems are microprocessor-based devices that combine features of a modem with network security features, such as passwords, dial-back, and/or encryption, and offer added protection. For some computer applications, misuse via dial-up lines can be dramatically reduced by use of dial-back port protection devices used as a buffer between telecommunication lines and the computer. In addition to these

---

31 CSL Bulletin, op. cit., footnote 29.

32 *Defending Secrets,* op. cit., footnote 11, pp. 88-89. See also, Dennis Longley et al., op. cit., footnote 2, p. 464.

33 Discussion of other communications linkage safeguards can be found *in Defending Secrets,* op. cit., footnote 11, pp. 89-92. See also, Dennis Longley et al., op. cit., footnote 2, p. 408.

Box A-2–Access Control Software and Audit Trails

Access control determines who can access the system, what system resources they can access, and how they may use those resources. Adequate access control prevents users from intentionally or accidentally obtaining data without prior permission.

At the host, access control usually involves two forms of security, system *access control,* which prevents unauthorized users from logging onto the system, and *data access contro/,* which prevents authorized users from accessing and/or modifying a particular file unless the user has been given prior permission.

The following is a brief descriptive list of access control methods:

User identification. The user identification code (ID) identifies the terminal users or application programs to other applications, data, devices, or services. Access to the system or application is denied if the user name or identification code is not listed in the access control file. User IDs also enable the system to report the activities of each individual logged onto the system.

Passwords. Passwords provide for verification of the identity of users. Passwords, secret and unique codes known only tot heir owners and recognizable only to a related target system, are intended to identify the user and ensure authorized access. Permission to access a system is typically denied until the individual supplies the password assigned to the user name and access type. A system file stores passwords with the user names they reference.

Host access control software packages attempt to prevent individuals f rom guessing or otherwise improperly obtaining a password. To do this, they may:

1. specify a minimum length for passwords to prevent the creation of overiy simple passwords;
2. require users to change their passwords at regular intervals;
3. limit the number of login attempts;
4. record unsuccessful login attempts;
5. require users to accept machine-generated passwords, which can offer more security than self-generated passwords because they are randomly generated pseudo words not found in the dictionary;
6. cancel passwords that have not been used for a specified period of time;
7. perform password trapping to capture users with stolen passwords; and
8. one way encrypt the password in the system's protected password file.

Login Control Login controls specify the conditions users must meet for gaining access. In most cases, access will be perm itted only when both a username and password are provided. More complex systems grant or deny access based on the type of computer login, i.e., local, dial-up, remote, network, batch, or subprocess. The security system can restrict access based on the type of terminal or remote computer—access will only be granted when the user or program is located at a designated terminal or remote system. Also, access can be defined by time of day and day of the week. As a further precaution, the more complex systems monitor unsuccessful logins, send messages to the system operator and disable accounts when a break-in occurs.

Resource Authorization. User profiles, resource profiles, and access control lists created and maintained by t he host access control software identify the system resources to be protected, describe who can use resources, and detail the manner in which resources can be used. The protection is typically applied to applications, files, data sets, and system utilities. ft may also be applied to program processes, system commands, individual application transactions, and workstations, i.e., terminals and printers. Users and programs can have read, write, execute, delete, alter, or control access, or a

(continued on nexfpage)

Box A-2–Access Control Software and Audit Trails-Continued

combination thereof. Access authority is granted to a user or program based on whether it is an individual with unique needs or a member of a registered group.

***Authorization Checking.*Host access control packages control all interaction between the user and protected resources. The software:**

1. **intercepts access requests for resources from the operating system;**
2. **determines if the resource is protected by host access software;**
3. **references the security rights database for access profiles;**
4. **determines if the user's access request is a valid request based on the permission assigned to the user; and**
5. **passes the status of there quest tothe operating system, which then grants orden'bstheaccess request.**

***Auditing. She* breaches of security can occur *from* within an organization, and many systems can also be compromised if improper access is gained by an authorized party, accountability is key to security protection. Auditing allows a system to record significant events. Since auditing is generally tied to authentication and authorization, every authorization and attempted access is usually recorded. Examination of audit trails may also reveal suspicious patterns of access and allow detection of improper behavior by both legitimate users and impostors.**

Events that may be audited are:

1. **selected uses of files and hardware devices;**
2. **logins, logouts and break-in attempts;**
3. **activities of specific, individual users;**
4. **changes to passwords;**
5. **disk and tape value changes;**
6. **selected transaction types;**

dial-back systems, security modems can be used to protect data communication ports. These security modems are microprocessor-based devices that combine features of a modem with network security features, such as passwords, dial-back, and/or encryption.[34]

[34] *Datapro Reports on Information Security* "Protecting Information by Authentication and Encryption," 1S50-140-103, June 1993.

7. issuance of system commands; and
8. changes to security profiles.

Some systems allow selection of the specific security-relevant events to be recorded. In addition, security alarms (electronic messages) can be generated to be sent immediately to the security administrator or system operator when specific events take place.

Journaling.Journaling involves recording all system activities and uses of a system resource. By analyzing this activity, the security administrator can:

1. identify access violations and the individual accountable for them,
2. determine security exposures,
3. track the activities of selected users, and
4. adjust access control measures to changing conditions.

Program and Data Integrity. Several types of controls and functions address program and data integrity:

1. Dataset naming conventions separate production data from test data. The assignment of unique types of dataset names for separate categories of data ensures that the difference between test and production data is maintained.
2. Naming conventions are also used for unique and specifically defined program names, job names, and terminal usage.
3. File placement ensures that files reside on the proper direct access storage device so that datasets do not go to a wrong device by accident
4. Program control allows only assigned programs to run in production and eliminates the problem of test programs accidentally entering the production environment.
5. Separation of production and testing ensures that no test data or programs are used in normal production.

SOURCE: Datapro Reports on Information Security, "Host Access Control," IS52-21O-1O3, July 1992.