Computer Security

An Honors Thesis (ID 499)

by

Lynne R. Haberland

Thesis Director

Kathleen Paul

Ball State University

Muncie, Indiana

August 1985

Summer/1985

CONTENTS

Computer Security

INTRODUCTION

Throughout the ages, man has had a desire to ensure that certain information was available to only a select group of people. In the past, such information was stored on paper and kept behind locked doors. If an unauthorized individual wished to obtain this information, actual physical entry onto the premises had to be made and access to the room where this information was stored had to be gained. Today, however, a large amount of material is stored through the use of a wide variety of computers. Unauthorized access to information stored in this way is not only more subtle, but it can be accomplished from miles away. In an effort to prevent computer access by illegitimate individuals, a diverse collection of computer security methods have been developed. These computer security methods include facilities protection, technological measures and security program evaluation.

In the past few years, computer security has been drawing an increasing amount of attention. There are four primary reasons why this has happened. First, interest has been aroused in both the private and public sectors because of the increased amount of reporting of computer crimes that involve large amounts of money.

> Although some very serious incidents have occurred, the extent to which computers contributed is often exaggerated. Over $400 billion is transferred daily over U. S. electronic financial networks.

Since these transactions occur daily and involve such large amounts of money, such a regard for security is well-founded.[1]

Second, society tends to fear that which it does not understand or is unfamiliar with. Since a vast majority of the population is not computer-literate, it is afraid that computer technology may harm it in some way. "While we often tend to overreact to unfamiliar threats, it is healthy that we do not take them too lightly."[2] Third, some important computer-security oriented laws have been passed by the United States government. An attempt is being made to ensure that government agencies and contractors develop strong computer-security techniques and that these programs are evaluated upon occasion to guarantee that they are performing as well as desired. Fourth, and perhaps most importantly, "computer security is simply good business practice." While computer-security techniques are not free, they should be cost-effective.[3]

Before explaining the many different computer-security measures that are available, one must first define exactly what computer security is. In the discussion that follows, the term computer "will encompass large computers, medium (midi- and minicomputers) and microcomputers, as well as such office-automation devices as word processors, electronic mail, and voice processing devices."[4]

While some individuals refer to computer security as the protection against the unauthorized transfer of funds, it will be defined in a more liberal sense here. In the ensuing discussion, computer security consists of "both information security and physical-assets security."[5] It will deal with the protection of data, physical equipment, and personnel. Information security is defined as the "protection against unauthorized disclosure, manipulation, destruction, or alteration" of data. Physical-assets security is referred to as the "theft, destruction, or misuse of computer-system property (including computers, peripherals, and data-storage media)."[6] A computer-security program should also protect those individuals who are associated with computers. This protection of personnel serves two purposes. It helps guarantee both personal safety and also the availability of those who have the skills to make the computer a valuable tool for the organization.[7]

FACILITIES PROTECTION

An important part of any computer-security system is facilities protection. If the computer facilities are destroyed, then all other security measures are useless. Facilities must be protected from a wide variety of hazards. One of these potential dangers is fire. "Detection and suppression capability should always be provided. Extinguishers should be readily available and the staff instructed in their use."[8] In addition to the existance of fire extinguishers, automatic fire-suppression equipment may be installed to keep things under control until the fire department arrives. Such devices would include smoke or fire alarms to help aid in early detection. Water or Halon may be used to help put out the fire. "Halon is a halogenated hydrocarbon (Hydrogen atoms are replaced by atoms from the halogen series) that function as a flame-extinguishing agent." While Halon is effective, it is expensive and less reliable than other fire-suppression systems.[9]

Techniques must also be implemented that will protect against changes in the quality of power, environmental changes, and the detection of water. Backup, recovery, and service centers should also be available. The physical facility should be well-constructed to prevent damage from natural or unexpected disasters. Surveillance and intrusion detection devices should also be in existence. Such devices include security guards, locks, closed-circuit television, and alarms. Technical control centers may also be desirable. These centers consolidate many security functions.[10]

TECHNOLOGY

Technology plays a key role in computer security. In this discussion, technology will be defined as the "procedural techniques, hardware devices, and software routines that are based on analytical designs or developments."[11] Each of these three technological areas contain several alternatives. These methods will be explained in detail.

PROCEDURAL TECHNIQUES

One area of computer technology that must be protected involves the procedural techniques used by a system. These include such things as accessing the computer, accessing files, communicating with personnel, training employees, establishing formal procedures, and developing a contingency plan. Computer access control measures are designed to ensure the following:

> only designated individuals are allowed entry into a physical area, the use of a computer in a particular mode, or the use of specific data in computer memory.

Most protective access control procedures involve testing either what a person knows, what he has, what he is, or what he is capable of doing. Regardless of the technique or techniques used, any access control procedure should be reliable, convenient, acceptable to the user, and inexpensive.[12]

Two common techniques of computer access control are passwords and algorithms. The use of passwords as a security control measure is very common. A password is a string of letters or numbers which must be entered by the user before access can be obtained. "Passwords may be user-generated or system-generated." System-generated passwords are usually the most desirable in an environment where there are a large number of users. In such an environment, passwords must be changed frequently for several reasons. One reason is high user turnaround. With today's job market, people change jobs very often.

To maintain good security, passwords should change whenever there is a change in the user environment. Another reason for passwords to be changed frequently is that the more people who know the password the higher the likelihood that an unauthorized person will discover it.

Usually, to gain access to the computer, the user must first enter some type of indentification followed by the password. All of the identifiers and corresponding passwords are stored in memory. If the password and its accompaning identifier do not match up, the user is denied access. In many systems, if three unsuccessful access attempts occur in succession, "the system will lock the terminal and alert the local security administrator." One of the major weaknesses of passwords as a security device is that they will only keep out the casual intruder. They will not keep out anyone who is determined to gain access.[13]

Algorithms are programmable routines and can be used without or with password systems. "The intent is to require the user to do prescribed tasks that only the identified person could do." This could involve the completion of either an access quiz or a computation. An access quiz consists of asking the user a randomly selected question or series of questions during the login process. These should be questions that only the identified user would know, "such as a wife's maiden name, mother's birthday, or a pet's name." If a computation is to be performed to gain access, the user is given an equation which he must solve using his secret predetermined numbers.[14] Similar security procedures should also be developed to protect file access.

It is important that both communication with personnel and the training of personnel should involve the discussion of computer security. Memoranda, visual aids, security patrols, newsletters, bulletin boards, and assistant computer-security officers all help to keep both old and new employees informed of the rules and regulations that govern computer usage, as well as why computer security is necessary and important.[15]

To help ensure that the standards of computer security that have been established are met, formal procedures need to be developed. These procedures include the use of computer security plans, reviews and tests. A computer-security plan provides documentation on how computer security is to be handled. This plan should include information about the procedures, hardware, software, and personnel that are involved in the security system. Every computer security system should be reviewed and audited periodically to be sure that it is functioning as desired. Security systems should also be tested to guarantee that security measures are working as expected.[16]

All security systems should also have some type of contingency plan. A contingency plan should ensure the security and intergrity of information. It should also anticipate and prepare for such things as expected losses, unwanted or unexpected events such as fires or tornados, costs resulting from losses, and possible responses to any problems that might occur. Each person involved with the system should know what his responsibility is if anything should go wrong. Such a plan should also have a list of its weaknesses. "Any contingency plan is only as good as the preparation that went into it." While there may only be a few times when the contingency plan will be implemented, its existence will make those times of crisis proceed much more smoothly.[17]

HARDWARE DEVICES

Another area of computer technology that aides in computer protection are the hardware devices. Hardware is defined as "the computer and all related and attached machinery, such as mechanical, magnetic, electrical, and electronic devices, used in data processing."[18] The main objective of hardware security "is to ensure that the equipment is not destroyed (either accidentally or intentionally), modified, stolen, sabotaged, vandalized, employed in a criminal scheme, or damaged in any fashion."[19]

Hardware security consists of access control and information protection. Hardware access control security measures are designed to allow only authorized personnel admittance "to computers, facilities, rooms, terminals, data, or privileges (such as financial transactions)."[20] Some of the security measures for hardware access control include fingerprint analysis, signature analysis, palmprint analysis, hand geometry measurement, eye blood-vessel patterns, voiceprint analysis, biometric research, coded keys, transmitters, cards, locks, silicon-chip cards, dial-up control and a variety of other miscellaneous access-control devices.[21]

Fingerprint analysis is usually done by an automated device. When using such a device, finger position is important and some time is necessary for the scan to be completed. "The identification is potentially reliable." Tests have shown that the denial of access to authorized personnel is about 0.37 percent and granting access to unauthorized individuals is less than 0.03 percent.

> The access procedure typically requires identification of a user at a terminal connected to a host computer. The fingerprint data of the individual identified is retrieved from the host database and delivered to the fingerprint reader, where it is compared to the data being derived during the current scan.

Thus, fingerprints, which have been used to identify people for over a century, can be used as a method of access control for hardware security.[22]

Another type of access control involves the use of signature analysis. This process not only analyzes the letter patterns, but pressure deviation, acceleration, and a time record as well. While signatures are unique, forgery is possible. By analyzing all of the signature dynamics listed above, forgery becomes more difficult.[23]

Palmprints are also unique to each individual. This type of access control is very reliable. The false acceptance rate is 0.00025 percent. "This extremely low rate is achieved with the aid of a keyboard number entry...."[24] Another method of access control is based on the measurement of hand geometry. "Hand geometry identification is based on the length of four fingers on each hand, and on translucency of fingertips and webbing." Forgery is usually difficult as a result of the translucency measurement.[25]

Three other types of access control methods that use parts of the body for identification are eye blood-vessel patterns, voiceprint analysis and biometric research. Eye blood-vessel patterns are recorded by scanning "the retina through a binocular eye camera." The light patterns recorded are then matched with those in storage before access is granted. Voiceprints "are detectable electronically and are difficult to imitate successfully." Biometric research has involved using other parts of the body for identification purposes. Examples include "ear size and shape, facial structure, brain waves, electrocardiograms, blood characteristics, and lip patterns." Thus, the body is very functional as an identifier for access control.[26]

Other types of access control devices are coded keys, transmitters, cards, locks, and silicon-chip cards. Coded keys are similar to magnetic-stripe cards. They look like regular keys, but contain coded data that controls access to computer hardware. Transmitters are small and function on a low amount of battery power. They are used to turn a terminal on automatically when the user is near. They have a short battery life in case they are lost or stolen and therefore must be left at work every-night to be recharged. There are several types of access-control cards. These include photo-badge cards, magnetic-spot cards, and magneticstripe cards. Access control locks can have many forms. They can be either key, spin combination, cypher, or sophisticated tumbler locks. Silicon-chip cards are cards that contain all of the necessary access information on a silicon chip.[27]

Dial-up controls and other miscellaneous controls are also used to regulate access. Dial-up control can be achieved by restricting the use of telephone lines to authorized personnel only. This is difficult to do. Other access control methods include walking characteristics or terminal typing dynamics. Thus, there are numerous security measures that will limit access to computer hardware.[28]

Information protection is accomplished primarily through the use of encryption hardware. Encryption refers to the process of coding for secrecy. One assumes that the code breakers will know as much about the coding methods as the designers do. "This assures that the protection of encoded data is not based on the secrecy of the encoding method but on the secrecy of each key that is used and on code-breaking com-plexity." This idea that forms the basis for the above concept of designing encryption procedures is used in many areas of computer security. Simply stated, it is as follows: do not rely on the secrecy of the mechanism of a safeguard but rely instead on the complexity of the measure and the effort that will be required to break it.[29] There are many types of encryption devices available. Other types of hardware information protection devices include electromagnetic shielding, coupling and interface; direct electrical effects protection; information disposal devices; and partitioned hardware.[30]

SOFTWARE ROUTINES

In addition to procedural techniques and hardware technology, software routines can also aid in computer security. Some of the different types of protective software technology included access-control software, encryption software, comparators, audit software, kernalized systems, risk analysis, and banking backup software.[31] Software consists of "computer programs, procedures, and associated documentation concerning the operation of a computer system.[32]

Access control software and encryption software packages are available. These routines function on the same principles as their hardware counterparts described earlier.[33] "A comparator is a computer code comparison routine that details the differences between old and new versions of the code." A comparator is used to prevent the unauthorized changing of software. "Audit packages provide information appropriate for audit examination." Kernalized systems help keep authorized users from getting unauthorized information. Risk analysis is used to assess the cost of the vulnerability of a security system. Backup routines are valuable in keeping losses at a minimum when things go wrong. Thus, software can protect in a variety of ways.[34]

EVALUATION

In order to ensure that a computer-security system is performing as expected and that it is the best available for the computer system in operation, all of the computer security methods being used should be evaluated periodically. There are a variety of evaluation techniques which may be used. These include EDP auditing, file and transaction monitoring, log examination, password pickup, incident reporting, security tests, data analysis, and most importantly, selecting the appropriate computer security measures for the computer system and environment that are involved.[35]

SUMMARY

An awareness that a need for computer security exists is expanding rapidly. This is the result of four primary reasons. All computer security systems include facilities protection and a collection of technological measures. These protective measures can be chosen from a wide variety of alternatives. Every security system should also have its performance evaluated periodically. By following the procedures just detailed, a computer-security system should function effectively. One can expect that the area of computer security will keep expanding in the future. This expansion will develop new and improved ways of protecting the computer and its resources.

NOTES

[1] James Arlin Cooper, Computer-Security Technology, (Lexington, MA: Lexington Books, 1984), p. 3.

[2] Cooper, pp. 3-4.

[3] Cooper, p. 4.

[4] Cooper, p. 5.

[5] Cooper, p. 4.

[6] Cooper, p. 4.

[7] Cooper, p. 5.

[8] August Bequai, How to Prevent Computer Crime, (New York: John Wiley & Sons, 1983), pp. 188-190.

[9] Cooper, p. 86.

[10] Cooper, pp. 90-92.

[11] Cooper, p. 5.

[12] Cooper, pp. 37-38.

[13] Royal P. Fisher, Information Systems Security, (Englewood Cliffs, New Jersey: Prentice-Hall, INC., 1984), pp. 100-101.

[14] Cooper, p. 41.

[15] Cooper, pp. 43-44.

[16] Cooper, pp. 45-46.

[17] Bequai, pp. 188-190.

[18] Bequai, p. 290.

[19] Bequai, p. 194.

[20] Cooper, p. 49.

[21]Cooper, pp. 50-57.

[22]Cooper, pp. 50-51.

[23]Cooper, p. 51.

[24]Cooper, pp. 51-52.

[25]Cooper, p. 52.

[26]Cooper, pp. 52-53.

[27]Cooper, pp. 53-55.

[28]Cooper, pp. 56-57.

[29]Donn B. Parker, Computer Security Management, (Reston, Virginia: Reston Publishing Company, Inc., 1981), p. 173.

[30]Cooper, pp. 78-83.

[31]Cooper, pp. 93-102.

[32]Bequai, p. 291.

[33]Cooper, pp. 93-96.

[34]Cooper, pp. 96-102.

[35]Cooper, p. 104.

REFERENCES

Becker, Hal B. Information Integrity. New York: McGraw-Hill Book Company, 1983.

Bequai, August. How to Prevent Computer Crime. New York: John Wiley & Sons, 1983.

Burnham, David. The Rise of the Computer State. New York: Random House, 1980.

Cooper, James Arlin. Computer-Security Technology. Lexington, MA: Lexington Books, 1984.

Elam, Phillip G. Checklist/Guide for Assessing Data Processing Safeguards. Babylon, New York: Pilot Industries, INC., 1983.

Fisher, Royal P. Information Systems Security. Englewood, Cliffs, New Jersey: Prentice-Hall, INC., 1984.

Parker, Donn B. Computer Security Management. Reston, Virginia: Reston Publishing Company, Inc., 1981.

Perry, William E. Computer Control and Security. New York: John Wiley & Sons, Inc., 1981.

Schjolberg, Stein. Computers and Penal Legislation. Oslo: Universitetsforlaget, 1983.

Ware, Willis H. Information Technology, Crime and the Law. Santa Monica, CA: The Rand Corporation, 1982.