DOCUMENT RESUME

05640 - [B1246201]

Challenges of Protecting Personal Information in an Expanding Federal Computer Network Environment. LCD-76-102; B-146864. April 28, 1978. 42 pp. + 2 appendices (6 pp.).

Report to the Congress; by Elmer B. Staats, Comptroller General.

Issue Area: Federal Information: Protection of Information in ADP Systems (1403); Automatic Data Processing (100).
Contact: Logistics and Communications Div.
Budget Function: General Government: General Property and Records Management (804).
Organization Concerned: Office of Management and Budget.
Congressional Relevance: House Committee on Post Office and Civil Service; Senate Committee on the Judiciary; Congress.
Authority: Brooks Act (P.L. 89-306). Privacy Act of 1974.

The concept of a Federal computer network and the attendant benefits of economy and efficiency was recognized when the Brooks Act was enacted in 1965. Since the enactment of this legislation, public and private concern has grown over the ability of computer systems and networks to provide adequate protection for personal information maintained about U.S. citizens. Findings/Conclusions: The concept of a Government-wide computer network presents a dilemma: should the Government take advantage of the economies that may be possible from using multiuser teleprocessing systems rather than individual agency owned and operated data processing systems or protect the individual's right to privacy by prohibiting such networks? This dilemma could be solved and economies realized if adequate controls could be defined and established to ensure confidentiality of data. The major threat to privacy invasion stems from misuse of personel information by individuals having authorized access, and a secondary threat stems from individuals not allowed access to the information who have the technical ability to circumvent security measures. The risk to personal information varies with the type of data involved, the effectiveness of the controls exercised, and the configuration of the computer network. While absolute security cannot be assured, a high level of protection can be provided in a multiuser computer network. Recommendations: The Director, Office of Management and Budget, should take action to provide Federal agencies with comprehensive guidelines that: contain the definitions and criteria necessary to permit an assessment of their security requirements; provide the methodology to be used in conducting the assessment; identify the physical, administrative, and technical safeguards that should be applied in satisfying their security requirements; and specify the means to justify the associated cost. (RRS)

0201

BY THE COMPTROLLER GENERAL

Report To The Congress

OF THE UNITED STATES

Challenges Of Protecting Personal Information In An Expanding Federal Computer Network Environment

The Brooks Act (Public Law 89-306) recognizes the economic benefits of computer networks. However, a continuing concern has been expressed over the ability to protect personal information contained in these networks.

This report discusses problems involved and presents possible ways to provide a high level of protection for personal information. The Office of Management and Budget should expeditiously provide Federal agencies with comprehensive guidance.

UNITED STATES GENERAL ACCOUNTING OFFICE

LCD-76-102
APRIL 28, 1978

COMPTROLLER GENERAL OF THE UNITED STATES
WASHINGTON, D.C. 20548

B-146864

To the President of the Senate and the
Speaker of the House of Representatives

This report addresses the continuing concern, expressed by various congressional sources, over the ability to protect personal information in large computer networks. An overview of privacy and computer security problems is presented together with possible approaches which can provide protection for personal and other sensitive information.

We made our review pursuant to the Budget and Accounting Act, 1921 (31 U.S.C. 53), and the Accounting and Auditing Act of 1950 (31 U.S.C. 67).

We are sending copies of this report to the Director, Office of Management and Budget; Acting Director, Office of Telecommunications Policy; Secretary of Commerce; Chairman, Civil Service Commission; and the Administrator of General Services.

Elmer B. Staats

Comptroller General
of the United States

COMPTROLLER GENERAL'S
REPORT TO THE CONGRESS

CHALLENGES OF PROTECTING PERSONAL INFORMATION IN AN EXPANDING FEDERAL COMPUTER NETWORK ENVIRONMENT

D I G E S T

The concept of a Federal computer network, and the attendant benefits of economy and efficiency, was recognized when the Brooks Act (Public Law 89-306) was enacted in 1965. However, since the enactment of this legislation, public and private concern has been growing over the ability of computer systems and networks to provide adequate protection for personal information maintained about U.S. citizens. (See pp. 1 and 4.)

The first attempt to provide central access to information was made in the mid-1960s with the proposal to establish the National Data Center. This proposal met with concern over the potential for a large concentration of data to be misused resulting in an invasion of individual privacy. The joint General Services Administration (GSA) and U.S. Department of Agriculture computer acquisition project (commonly known as FEDNET) met similar opposition in 1974. Congressional action precluded both projects from materializing. (See pp. 7, 8, and 9.) More recently, the Internal Revenue Service's (IRS') proposed Tax Administration Systems was terminated in 1978 with privacy as one of the major issues. (See p. 1.)

This report attempts to summarize the lessons learned from GAO's various studies of computer systems and its research in the past several years into the problems and promises of computer networks to adequately protect private information.

The state-of-the-art in computer security is such that absolute security has not been achieved in a multiuser, teleprocessing environment. Considering the cost involved, absolute security is rarely practicable in any environment. Decisions must be made,

Tear Sheet. Upon removal, the report cover date should be noted hereon.

therefore, on that degree of protection beyond which the cost of subverting a system becomes greater than benefits to be gained. (See p. 10.)

Computer systems are extremely vulnerable to certain classes of threats to their security. GAO has categorized the various threats to put them in perspective. (See p. 14.)

GAO discusses some of the latest technology available to combat security problems that could arise where Federal agencies share computer hardware, data, and communications. (See pp. 19, 26, and 27.) And it cites one method which shows promise for acquiring a computer network where the security provided can be evaluated and subsequently validated. (See pp. 30 to 32.)

In summary, the merging of automatic data processing and communication resources into computer networks can be accomplished while providing reasonable protection for personal information from those unauthorized to have it. Use of today's advanced teleprocessing technology would facilitate achieving the efficiency and economy objectives of shared equipment, programs, and data as envisioned by the Brooks Act.

A careful application of the available technology, in compliance with the administrative practices and technical safeguards required by the Privacy Act of 1974, could reasonably protect the confidentiality of personal information while enabling the Government to realize the economies of networking and data sharing.

However, cost-effective protection of individual privacy is dependent upon resolving underlying problems pertaining to the methods and procedures for assessing and solving Federal agencies' security requirements. The full realization of economies from advanced teleprocessing technology continues to be hampered because of the lack of definitive guidance for agencies to apply in the requirements determination, procurement, and system development process. Because of the Privacy Act's mandates, this guidance is needed today. (See pp. 33 to 35.)

The Director, Office of Management and Budget, should take the necessary action to expeditiously provide Federal agencies with comprehensive guidelines that

--contain the definitions and criteria necessary to permit an assessment of their security requirements;

--provide the methodology to be used in conducting such assessment;

--identify the physical, administrative, and technical safeguards that should be applied in satisfying their security requirements; and

--specify the means to justify the associated cost.

Contents

ABBREVIATIONS

ADP	automatic data processing
CSC	Civil Service Commission
FEDNET	Federal Information Network
GAO	General Accounting Office
GSA	General Services Administration
NBS	National Bureau of Standards
OMB	Office of Management and Budget
OS	operating system
OTP	Office of Telecommunications Policy
TAS	Tax Administration System

CHAPTER 1

INTRODUCTION

In June of 1975, we issued our report on a proposed joint General Services Administration (GSA) and U.S. Department of Agriculture computer acquisition project. 1/ The project ultimately became known and received notoriety as the Federal Information Network (FEDNET).

The study was motivated by congressional concern that the project would bring together, in a single integrated network, various computer data bases containing private information on U.S. citizens, without adequate safeguards in the system's design for the protection of the information and thus, the privacy of individuals.

Since that time, there has been burgeoning public and private concern over matters of privacy and security of data in computer systems and networks. Such concerns were expressed most recently in the matter of the proposed computerized Tax Administration System (TAS), which was also the subject of one of our reports. 2/ The TAS proposal was terminated in 1978, with privacy as one of the major issues.

The Government's primary objectives in proposing the FEDNET and TAS systems were improved efficiency and economy through the use of modern computer-communications technology. If that same technology can provide adequate privacy and security safeguards to the data it so effectively stores and processes, then the potential improvements in productivity and efficiency, which are possible through modern computer systems, can be realized.

This report attempts to summarize the lessons learned from our various studies of computer systems and its research in the past several years into the problems and promises of computer networks to adequately protect private information.

As used in this report, privacy is a concept which applies to individuals. It is the right of individuals to

1/"Improved Planning--A Must Before a Department-wide Automatic Data Processing System is Acquired for the Department of Agriculture," (LCD-75-108), June 3, 1975.

2/"Safeguarding Taxpayer Information--An Evaluation of the Proposed Computerized Tax Administration System," (LCD-76-115), Jan. 17, 1977.

decide what personal information they wish to share with others. The privacy issue has not resulted from the development of computers, but the heightened interest in it can be attributed to the capability of computers for storing vast amounts of readily usable data about individuals. Although many of the matters discussed in this report apply to data regardless of the manner in which it is stored, our study focuses on the subject as it relates to computer networks.

While individuals may be required by law to furnish certain information about themselves to a Federal agency, they may not be willing to share the same information with other agencies or the general public. Recognizing this, the Congress included in the Privacy Act of 1974 a requirement for each agency to (1) establish appropriate technical, administrative, and physical safeguards to assure the security and confidentiality of records and (2) protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

This report presents an overview of privacy and security involving computer networks and some possible approaches which can provide protection for personal and other sensitive information. Technical terms used in this report are defined in the attached Glossary. (See app. II.)

SCOPE OF REVIEW

We discussed currently employed privacy and security safeguards with representatives of various Government agencies using both commercial and Government timesharing services. In evaluating the computer security problems and potential solutions, we consulted a large number of individual experts in computer and information security from the private sector who represent a wide range of knowledge, interests, and views.

We examined the provisions and legislative history of the Brooks Act (Public Law 89-306) and the Privacy Act of 1974 (Public Law 93-579) as they pertain to the issues of the review, and we looked at the executive branch's plans and actions for implementing the Privacy Act.

Although we obtained information on the actions being taken by the executive branch under the Office of Management and Budget's (OMB's) direction to comply with provisions of the Privacy Act, we did not examine the individual operating agencies' actions in any depth to evaluate the effectiveness of those actions; these matters will be addressed in our continuing reviews.

CHAPTER 2

FEDNET AND PRIVACY ISSUES

The economic advantages of teleprocessing were recognized by the House Committee on Government Operations as early as 1965. In its report on the Brooks Act, the Committee stated:

> "The potentials of the larger computers now in the offing which can be integrated with communications is so great that full utilization of one system's maximum capability is sufficient to fit the needs of scores of potential users. And, the use of the maximum potential of a third generation system under conditions of optimum efficiency can result in a phenomenal reduction in ADP [automatic data processing] cost to individual users. This greater potential and lower cost cannot be ignored by either business or Government.
>
> "As third generation time-sharing increases, the traditional agency-by-agency structure of the Government in terms of ADP management will become less apparent and less important. Systems design will depend more upon the functional requirements of the users than their identity or jurisdiction. The need for Government-wide evaluations as to acquisition and utilization of equipment will become so pronounced as to make any narrower approach prohibitive. The waste inherent in unused potential and errors in application or equipment selection will be staggering." 1/

The growth of individually owned computers has been rapid, and the cost of computers acquired for limited applications has been high. In the decade following the Committee's report, the number of computers in the Government increased from 2,412 in 1965 to 11,328 in January of 1978. The increase in cost is estimated in the billions. Considering that during this period in the development of computer technology, a potential of as much as four to eight times the computer power could be obtained

1/H.R. Rep. No. 802, 89th Cong., 1st. sess. 13 (1965).

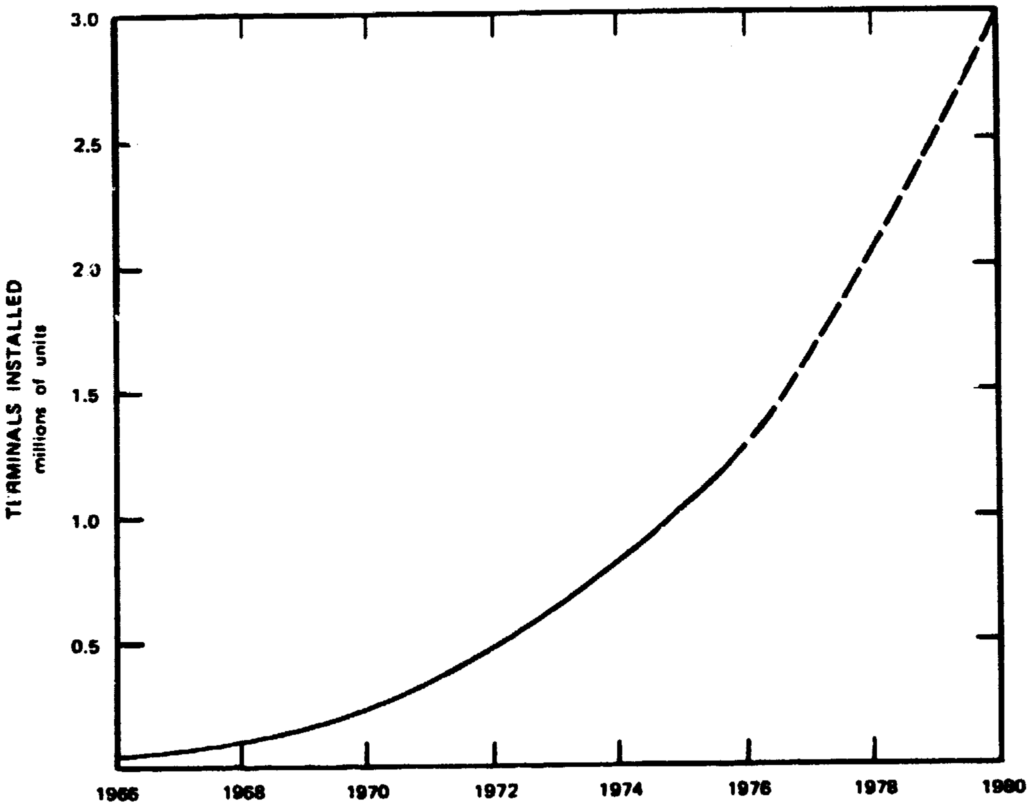
at only twice the cost,[1] the potential savings from shared resources by integrating and consolidating systems became substantial.

The fact that economies and efficiencies are available from computer and terminal networks has been widely accepted both by Government and the private sector. One study forecasted, as illustrated on the following page, a continuing growth, in computer input-output terminal devices from approximately 500,000 in 1972 to almost 3 million by 1980.[2] It is recognized that with the advances in technology and the development of small computers, some of the advantages of shared computer resources may have diminished in regard to certain applications. Nevertheless, the general consensus during our study was that sophisticated computer networks will continue to develop.

[1] "The most obvious argument for the sharing of a computer by several users is the economies of scale which exist in the computer-manufacturing process. For instance, computer power increases roughly with the third power of computer cost. In other words, an increase in computer cost by a factor of 2 may generate an increase in computing power by a factor of 2^3, or 8." John Dearden, F. Warren McFarland, and William M. Zani, Managing Computer-Based Information Systems, Richard D. Irwin, Inc.,: Homewood, Ill., 1971, p. 93.

[2] Stanford Research Institute, Data Processing Control Practices Report, The Institute of Internal Auditors: Altamonte Springs, Fla., 1977, p. 11.

DATA COMMUNICATION TERMINALS INSTALLED, 1966-1980 (U.S.)



SOURCE: SRI STUDY–SEE FOOTNOTE 2
P. 5.

PRIVACY ISSUE

The capability of computers to store vast amounts of readily usable data has given the privacy issue new dimensions. For example, Dr. H.R.J. Grosch stated in June 1974:

> "We can store three trillion binary digits, a five hundred word dossier for every man, woman, and child in the United States, in a commercially available machine small enough to go in an elevator * * *. Only the enormous expense of setting up data banks in the first instance holds us back from recording everything about everybody and keeping it forever." 1/

Considering the amounts of information about individuals currently maintained by various Government agencies, such as the Internal Revenue Service, Social Security Administration, and Veterans Administration, it is obvious that large data banks of personal information exist today. Disregarding cost and potential problems in identification of some individuals, only the inability to centrally access all of the information precludes the use of these sources to establish comprehensive individual dossiers.

Central access to information can be made possible through various methods, such as computer networking or physically consolidating data bases at a single computer facility. The first attempt to centralize Government-held computerized information was made in the mid-1960s with the proposal of research organizations to establish the National Data Center for the systematic collection of economic microdata. This proposal was supported by the Bureau of the Budget but met with concern over the potential for a large concentration of data which, through misuse, could result in an invasion of individual privacy.

A special subcommittee of the House Committee on Government Operations was formed to investigate the National Data Center's proposal and consider the impact of computerized information systems on the individual. Its concerns were expressed in the following statement of objectives:

1/Data Security and Data Processing, Vol. 3, Part 1, "State of Illinois: Executive Overview," IBM Corporation: White Plains, N.Y., 1974, p. 7.

> "What we are looking for is a sense of balance. We do not want to deprive ourselves of the rewards of science * * *. We would like to know just what information would be stored in a National Data Center; who would have access to it; who would control the computers; and most importantly, how confidentiality and individual privacy would be protected * * *." 1/

The congressional response to the proposed National Data Center was summarized in a 1968 report by the House Committee on Government Operations. 2/ The Committee concluded that the data center concept posed serious problems regarding the collection, use, and security of personal information. It strongly advised against establishing a National Data Center until the technical feasibility of protecting automated files could be fully explored and privacy guaranteed.

The joint GSA-Agriculture computer acquisitions project (FEDNET), although having a different objective, met similar opposition. There was widespread concern when the Congress learned of the project because it had not been fully informed of plans for a project this size and because of implications that the project could be expanded to link all modern computers in the Government. This in turn could pose a serious threat to the privacy of individuals involved in any Government operation or program. As a result, the scope of the project was reduced in July 1974 by canceling the telecommunications network and GSA's primary and optional data-processing installations.

Our June 1975 report (see p. 1) identified deficiencies in Agriculture's procurement planning, including the determination of data processing, communications, and security-privacy requirements. As a result of a congressional limitation on spending, in October 1975 Agriculture canceled its planned procurement and the request for proposals was withdrawn.

1/Hearings before a Special Subcommittee on Invasion of Privacy, House Committee on Government Operations, 89th Cong., 2d sess., (1966), p. 3.

2/House Committee on Government Operations, Report: Privacy and the National Data Bank Concept, 90th Cong., 2d sess., H. Rept. No. 1842, (1968), p.8.

These actions settled the issue of whether the joint GSA-Agriculture computer acquisitions project might be expanded to become the Federal Information Network conceived by the Automated Data and Telecommunications Service of GSA in August 1973. However, the concept of linking various computer systems and/or consolidating their data into a single data base remains a possibility for the future as does the question of how to protect personal data in automated files without losing the benefits of teleprocessing networks. The remaining chapters of this report address these issues.

CHAPTER 3

THE COMPUTER SECURITY PROBLEM

The concept of a Government-wide teleprocessing network presents a dilemma: Should the Government (1) take advantage of the economies that may be possible from using multiuser teleprocessing systems rather than individual agency owned and operated automatic data processing systems or (2) protect the individual's right to privacy by prohibiting such networks, thus avoiding the risks considered by some to be inherent in any of today's large teleprocessing systems. It may appear that the Government must forgo the economies to protect the rights of the individual. However, the dilemma would be solved and economies realized if adequate controls could be defined, established, and maintained to reasonably ensure confidentiality of data.

NEED FOR DEFINING LEVEL OF PROTECTION FOR PERSONAL DATA

The state-of-the-art in computer security is such that absolute security has not been achieved. However, absolute security with functional effectiveness would rarely be practicable in any environment--human or computer--when the cost is considered in attempting to achieve the highest level of protection.

Decisions on security must essentially make the cost of subverting a system greater than the benefits--either in monetary or punitive terms. We believe that reasonable protection can be provided for personal information by (1) increasing the cost of subverting a system to an unacceptable level and (2) imposing heavy penalties for those who attempt unauthorized appropriation or disclosure of personal information.

While the Privacy Act of 1974 imposes certain criminal sanctions and civil remedies for unauthorized disclosure, it does not specify the level of protection personal information requires. Defining the level of protection for personal information is one of the major problems in computer security. The establishment of a uniform methodology for determining the levels of protection required for personal information is being studied, but underlying problems have yet to be resolved. Part of the difficulty is a choice of alternatives. Either (1) all personal data, regardless of how trivial, will be afforded protection at the same level or (2) data will be categorized by degree of sensitivity or confidentiality with a level of protection assigned to each category The second or categorical approach would appear to be the more logical since, for example, an individual's name and address as shown in a telephone or city directory would be less sensitive and require less protection than a record of psychiatric treatment.

ANALYZING THREATS AND VULNERABILITIES

The need for physical security against such hazards as fire, sabotage, and theft is well known and the subject of another one of our reports. [1] The National Bureau of Standards publication, "Guidelines for Automatic Data Processing Physical Security and Risk Management," (Federal Information Processing Standards Publication 31) should aid agencies in assessing their physical security and developing effective physical security programs. However, providing only physical security is no longer adequate for information protection. TRW Systems, Inc., in a study on computer system security, pointed out the following:

> "Third-generation computers introduced new capabilities that involved the concurrent processing of many jobs, extensive sharing of computer resources, and the use of remote terminals. While these new capabilities brought benefits of substantially lower cost, sharing of large data bases, and remote use of computers, they also introduce a complex security problem. With concurrent sharing of a computer system, the opportunity is present for inadvertent, accidental, or malicious acquisition of information by a user who has no right of access." [2]

In examining the risk to personal and other sensitive information maintained on data-processing systems, it appears that the threats stem from two sources: (1) authorized, but untrustworthy or dishonest users and (2) malicious penetrators. The untrustworthy user has authorized access to the data of interest, while the malicious penetrator does not. The penetrator may be an employee of the organization or an outside party.

[1] "Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities," (FGMSD-76-40), May 10, 1976.

[2] Richard B. Blue, Sr. and Gerald E. Short, Computer System Security Technology and Operational Experience, TRW Systems, Inc.: Redondo Beach, CA., (Report No. TRW-SS-74-15), Mar. 1974, pp. 1-3.

Untrustworthy Users

The problem of untrustworthy or dishonest employees represents the major threat to personal or sensitive information contained in any system of records. The potential for the misuse of information by individuals in positions of trust is not unique to automated data processing systems--the problem exists in manual systems as well. Nevertheless, the concentration of data in computer systems increases the magnitude of the risk over non-computerized systems.

Protection against untrustworthy or dishonest employees is indeed difficult. However, the risk can be substantially reduced through proper application of well-designed managerial controls, which include: segregation of employee duties, personnel screening, activity monitoring, and effective auditing. These and other managerial controls have been afforded extensive coverage in literature published over the years by universities, professional societies, and Government. (The employee problem is discussed further in ch. 4.)

Malicious Penetrators

Malicious penetrators present a different threat than untrustworthy employees in that the former must circumvent technical security measures. In order to place the threat from this source in perspective, it is necessary to understand how penetrators would achieve their objective and what skills they must possess.

Our study of the views of experts in the field indicates that skilled individuals generally penetrate a system by using an operating system function in a way unanticipated by designers, or by exploiting some anomalous behavior of the operating system. They are frequently aided by the fact that designers of operating systems have assumed that users will not deliberately attempt to force a malfunction of the system.

Penetrators may achieve their objectives by various methods, including (1) acquiring by any method a list of user identifiers and corresponding passwords or other identification and confirmatory information needed to gain access to the computer system or (2) obtaining supervisory (executive or master) control of the computer system. A number of means have been found to do this. For example, in one version of an operating system, registers are shared between the operating system and the user's application programs. In this particular case, the operating system, in releasing a register to the user's program, uses a storage location, provided by the user, to load the register before turning control over to the user's program. This is accomplished without the operating system checking to ensure that the storage location is within the user's assigned area. Consequently, the operating system will load the register with eight consecutive words of memory from any location specified by the user. This flaw could be exploited to set up a search through all of the computer's memory for the password of the executive user (i.e., the master operator) which, when found, would permit the penetrator to masquerade as the executive user and have extraordinary privileges.

Using the first method, the penetrator can then masquerade as any of the authorized users, while use of the second method gives him/her direct access and control of any file or program in the system

In order for penetrators to accomplish their objective by either method, it is necessary that they be (1) at least moderately skilled in programming, (2) expend time and effort to understand rather complex operating systems, and (3) have knowledge of the limitations that occur in the design and implementation of the systems. Such knowledge suggests to penetrators where to look for possible errors and design flaws. If they have access to system documentation, their ability is considerably enhanced.

Against such individuals, contemporary computer-operating systems frequently fail to provide adequate protection for personal or sensitive information. The question is: Why?

It appears that this weakness is rooted in at least two causes. First, most operating systems that are available today were designed originally at a time when security issues were not being fully considered. As a result, the security elements were normally scattered throughout the operating system in a variety of apparently unrelated ways. In such systems, there is no assurance that all of the security-related parts have been examined and tested for flaws. In fact, known flaws exist in several commercially available operating systems currently in use. [1]

[1] R.P. Abbott, et al, Security Analysis and Enhancements of Computer Operating Systems, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D.C. (Report No. NBSIR-76-1041), April 1976.

Second, there are no comprehensive criteria for security to guide those designing and implementing operating systems for computers. Compounding the difficulty is the fact that security is usually stated in negative terms such as, "Data should not be accessible in an unauthorized way." Requirements that can be used in design and implementation must translate such negative statements into positive criteria which specify how a system should react under various conditions.

From the above discussion, it would appear that computer systems are extremely vulnerable; and indeed they are, but only against certain classes of threats. In order to place the various threats in perspective, it is necessary to understand their source, which can be expressed in terms of functionality--i.e., what one can do with or on a system.

Deliberate penetration risk

1. User functionality

None: Users are consumers of data-processing products produced for themselves by others.	Virtually None: Consumers are isolated from data system.
Limited: User supplies parameters for program either offline or online--single function applications, simple transaction systems, etc.	Limited: Dependent upon how well the application program anticipates user "errors," and the level of complexity of the system as seen by the user.
Moderate: User selects programs, supplies parameters, uses a data base management system with an ad hoc query capability. Uses multifunction transaction system in online or offline environments.	Moderate to Extensive: Dependent upon how well application system is designed, whether users are isolated from real machine functions, and whether applications have built-in user authorization controls.
Unrestricted: Users can program and/or have access to any system function.	Extensive: In most third generation computer systems, user-programming capability permits wide variety of attacks to gain access to data or to gain control of the system.

2. Operators and System Programmers	Unlimited: No system barriers exist.

It can be concluded that contemporary computer systems are most vulnerable to penetration from application and system programmers as well as console operators. However, the resultant risk to personal information is dependent upon the degree of centralization of personal data and the configuration of the network involved as discussed below.

NETWORKS

When the term "network" is used, anything from a simple common carrier public communications facility to an automatic resource-balancing computer network (see p. 17.) can be implied. The security risk and potential threat to personal privacy vary with the type of network employed. For the purpose of this report, networks are categorized in a way which, in our opinion, approximates the increasing order of risk for general application as shown below. It should be recognized that the degree of risk can shift between the type or category of networks, depending upon the scope and the nature of the applications and safeguards employed.

1. Common Carrier (communications only)
2. Single computer, multiple user
   a. Dedicated hardware
   b. Shared hardware
   c. Shared data
3. Multiple computer user
   a. Fixed allocation of resources
   b. Automatic resource balancing

Common carrier

This form of network, which provides only data communications, is the most common and probably the least vulnerable to the compromise of any form of personal information because of the resources and skills necessary to effect a successful interception. While experts agree that it is possible to electronically intercept or tap common carrier data links, no evidence indicates that this technology has ever been used to obtain personal information from a computer system. Furthermore, the data that may be available by electronic interception is generally unpredictable. Without the ability to address specific data, the cost of such interceptions may well exceed the value of any information obtained. Where it is determined that personal information warrants a higher level of protection, cryptography can be employed to secure the communication links and solve the problem. (See p. 28.)

Single computer, multiple user computer networks

Dedicated hardware. This type of computer network is in common use today and can be described as an in-house time-sharing system where all users belong to the same organization. Of course, unauthorized access to personal data can also occur in non-computerized systems. The added risk in the automated system is due to the concentration of data that must be kept readily available to meet the demands of the various users. Also, users can access the system by telecommunications with an additional degree of anonymity. The extent of risk resulting from the use of a common carrier network was discussed in the preceding paragraph.

Shared hardware. Several agencies sharing the same hardware in a computer network is analogous to a commercial time-sharing service. The risk to personal information is increased over the dedicated system as the number of agencies increase. The increased risk is due to the added volume and variety of personal information and the increase in user population. The technical threat to this kind of network comes from programmers who may be able to penetrate the operating systems and circumvent the security controls as previously discussed in this chapter. (See pp. 12 and 13.)

Shared data. This form of a computer network is an outgrowth of the shared hardware scheme. Where several agencies accumulate similar data, it is frequently more economical to integrate the common data into a single data base to permit data sharing. Economy is achieved by reducing or eliminating duplication in data acquisition, entry, and processing. The capability for extensive file sharing exists in most manufacturers' software support and commercial time-sharing services.

Added risks are introduced if inadequate procedures are used to authorize the sharing of data between two or more agencies. If appropriate oversight were provided by a designated Federal authority, and due consideration were given to the type of data to be shared and the validity of the agencies' requirements for shared data, the increase in risk over the shared hardware network could be significantly reduced.

Multiple computer, multiple user networks

Fixed allocation of resources. This type of network is similar to the aborted joint GSA-Agriculture computer acquisitions project. (See p. 8.) Such a network has a number of computer centers and a variety of users. While sharing common communications, each center may operate as an independent entity serving a given set of users with a given workload. The computers in the network may or may not have the capability to interface users' application systems to permit data sharing.

Where only communications are shared, the risk in this type of network is approximately that of the shared, single computer network. The additional risk in a network with a fixed allocation of resources is the increased opportunity of accidental exposure due to the transfer of information between computer centers. If the computers in the network are dissimilar, and the protocols between them are ill-defined or non-existent, there may actually be less real risk than in multiagency sharing of the same physical hardware.

Where the computers in the network communicate directly, the risk is increased over that of a single computer, shared data network with respect to the particular network resources to be shared, i.e., hardware, software, or data. This is due to the possibility of developing a program for one computer to subvert another. However, a well-designed system could require the expenditure by a skilled perpetrator of resources greater than the value of the information to be obtained.

Automatic resource-balancing network. This form of network does not yet exist in any significant form in the Federal establishment. It is a fully integrated, multiple computer network which automatically shifts workload between computers and employs data and program sharing. It would appear as a single "giant" computer even though composed of a number of individual units.

The primary difference between this form and the single computer, shared data network is one of magnitude. The centralization of vast quantities of personal data greatly increases the risk.

CONCLUSIONS

The major threat to personal privacy stems from the misuse of personal information by individuals having authorized access. A secondary threat originates from those individuals who are not authorized access to the information in question but have the necessary technical ability and resources to circumvent the security measures employed.

The risk to personal information varies with the type of data involved, the effectiveness of the controls exercised, and the configuration of the computer network. Generally, the potential for misuse of personal data increases as (1) more personal data is centralized, (2) user population increases, and (3) greater volumes of common data are shared.

CHAPTER 4

ADDRESSING THE SECURITY PROBLEM

Computer systems offer varying degrees of risk of unauthorized access to personal information and, therefore, to individual privacy. A legal definition of what constitutes reasonable protection for personal data has not been resolved because a legal precedent has not been established in this relatively new area. In the absence of precedent, agency determinations of reasonable protection must consider the potential threats to data and the available administrative, physical, and technical safeguards. It seems logical that progress toward more secure hardware and software will be accelerated to the extent that Federal agencies place such demands upon the computer industry.

The most obvious way to provide protection for personal information is to never place such information on a shared computer network but instead, employ hardware dedicated to a single activity's use. (See p. 16.) Through proper design and implementation, a dedicated system operated in a benign environment can provide a high degree of protection for information. With the advent of the minicomputer and its continued reduction in cost, dedication of a system to sensitive information is a viable alternative to the shared computer network. However, informational and operational requirements may well render such an alternative impractical in many situations. The following sections discuss some of the various methods for achieving a high level of protection where shared hardware, shared data, and shared communications are involved.

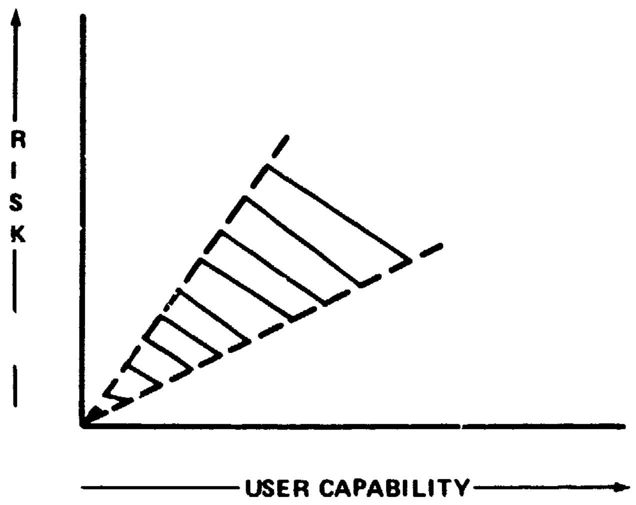
SHARED HARDWARE

A system or application programmer can do more damage to a system with less chance of being caught than almost any other person involved in data processing. It is therefore necessary to isolate the system from the programmer in order to provide any degree of security. While current research in the technical community is directed to the development of operating systems and mechanisms that will provide protection from skilled programmer penetration attacks, there is no consensus on its achievement in the immediate future. Today, it is possible to attain a high level of data security by (1) reducing the threat from those individuals with the technical training necessary to circumvent security safeguards and (2) segregating sensitive data and its processing from all other data, hence the adoption of a policy of isolation.

An isolation policy can be applied in either of two ways: (1) by isolating the system from the threat or (2) isolating sensitive data within the system.

Isolation of the system from the threat

Generally, the risk of a successful penetration increases with the capability provided to users of the system as shown below:



Most multiuser teleprocessing systems attempt to provide the user with maximum capability under the premise that this makes the systems more desirable and useful. Such systems can be highly vulnerable to penetration.

In order to significantly reduce the risk, the users' capability must be sharply curtailed. This can be done by permitting the terminal users to process transactions while removing their programming capability. Such a system--termed a transaction system--can, if properly designed and implemented, effectively isolate the system from the threat posed by the programmer.

An airline reservation system is an example of a transaction system. The terminal operator can enter, change, and retrieve data according to a limited number of command codes. Each command code performs a specific function in relation to the information entered and the data maintained on the system. For example, one command code assigned to a reservation clerk may cause all available flights between two cities to be displayed, while another may reserve a seat on a particular flight.

The users' capability in a transaction system can be further reduced through the use of employee and terminal profiles. Such profiles can restrict the command codes and terminals an employee can use to only those necessary to perform specifically assigned duties only. For example, a cargo clerk and the computer terminals located in the air freight department may be denied the use of command codes necessary to access passenger reservation information.

While this limits terminal users to transaction processing, it is also necessary that programs and their modifications be placed on the system under highly controlled conditions. Here it is necessary to isolate programmers from the system by requiring all programs and program changes to be submitted to an independent test and evaluation group. This group, which is a buffer between the application and system programmers and the operational programs, controls the programming function by reviewing, validating, and approving all programs and program changes placed on the system. Where it is impractical to establish a formal and independent test and evaluation group, such as in a small organization or where the programming function is relatively small, mandatory peer review can provide a measure of control.

This approach provides a high level of protection to personal information by isolating the system from the programmer and reducing the risk by restricting the user to only those functions necessary to process authorized transactions. Where users are presented with only the functionality of one or more transaction systems, the security of such systems can be developed without necessarily relying on security features and mechanisms supplied by a vendor. Therefore, the security of a transaction system is dependent upon the adequacy of the system design, operating procedures, and program testing.

Isolation of sensitive data

Where user requirements demand the flexibility of normal programming capability, the policy of isolation requires effective separation of sensitive data and its processing from all other data. To accomplish this, isolation mechanisms must be present that cannot be bypassed by users exercising normal user-programming control of the system. In this context, user-programming control extends to all of the supervisory, monitor, or operating-system programs executed on behalf of a user's program.

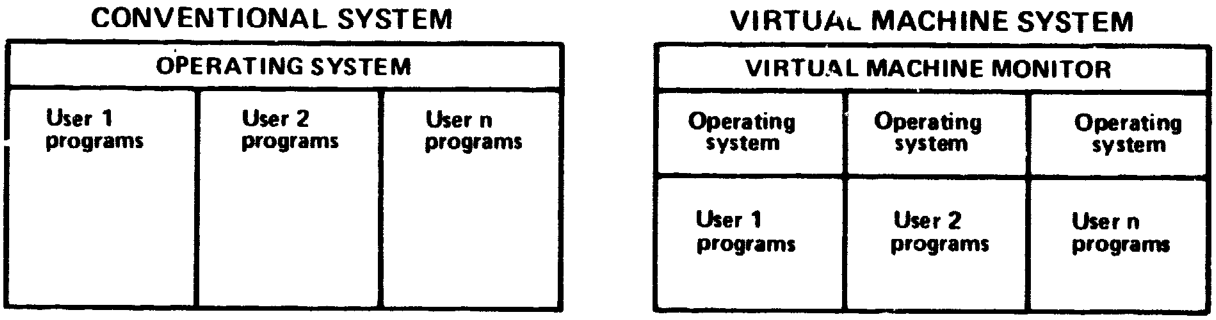
There have been two basic architectural approaches to provide this type of isolation--virtual machine systems and descriptor-based systems. These and other approaches to secure operating systems are discussed below.

Virtual machine systems

Virtual machine systems create an isolated environment through techniques which have the effect of creating for each user a complete system dedicated solely to the user's purpose. The software that creates this environment is generally known as a "virtual machine monitor." The monitor consists primarily of programs that provide (1) interpretive execution of privileged instructions, (2) minimal controls to initiate and discontinue virtual machines, and (3) the controls to cause several virtual machines to function in a single set of hardware.

The monitor permits each user to functionally have an operating system restricted to the individual user. Ignoring cost considerations, each user could have a unique operating system and thus completely close off any possibility of interaction between any two users of the system.

The following illustrates how conventional systems and virtual machine systems differ:



From a security viewpoint, a well-designed virtual machine system provides protection from a malicious programmer by isolating the operating systems of two or more users. It also reduces the need to be concerned with the security-worthiness of an existing operating system because the operating system can be considered as belonging to a single user.

Due to the limited functions the monitor performs, it can be quite small and relatively simple compared to typical operating systems. Therefore, it is theoretically possible to subject the monitor to thorough testing and validation of design.

Virtual machine technology is available today and can be applied to many existing systems with only minor hardware modifications. However, the use of this technology has several disadvantages that could limit the circumstances in which the virtual machine concept is applicable. Two major disadvantages are that (1) the overhead burden associated with virtual machine systems which can add materially to the system's operational cost and (2) the virtual machine approach does not adequately provide for high-volume sharing of data, or computer programs, among users.

Descriptor based systems

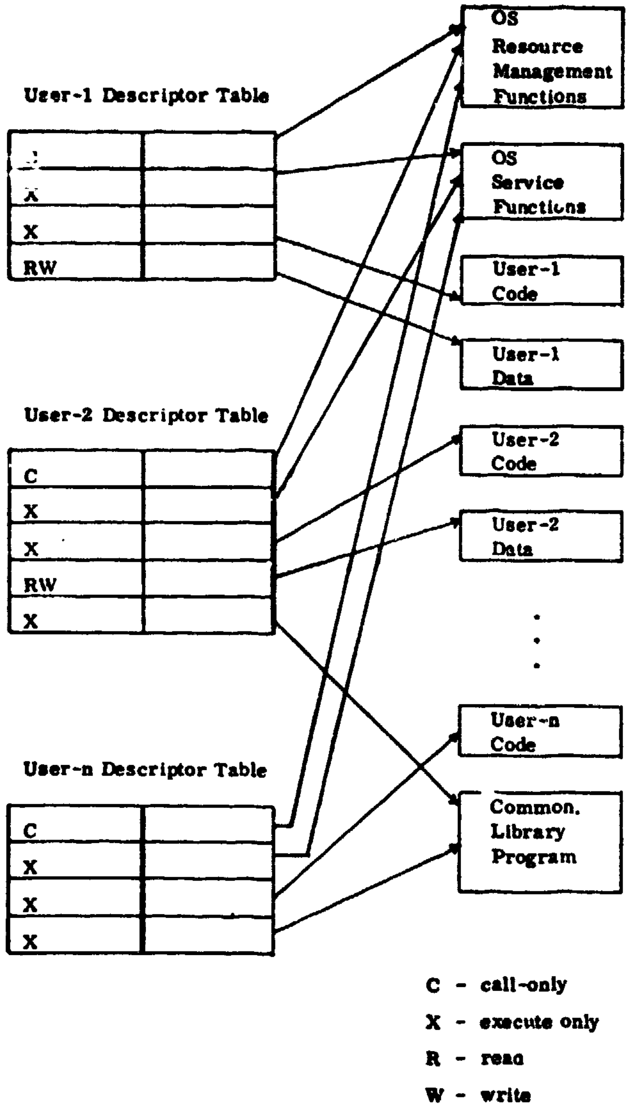
Another approach to isolating users is to use descriptor architecture to provide each user with a totally independent address space.

An absolute address within a computer is a specific designation assigned to a storage location by the machine designer. Indirect addressing is a method of computer cross referencing in which one memory location contains information as to the absolute address of an object or where such an address can ultimately be found. A descriptor can be described as a computer word that acts as a form of an extended indirect address.

When a descriptor is referenced by a computer program, information contained in the descriptor is interpreted in hardware to control the completion of the reference. It is therefore possible to represent an object's protection requirements in its descriptor and be assured that there will be automatic hardware controlled validation.

The major benefit from use of a descriptor-controlled approach is the ability to control sharing of programs or data by including the object to be shared as a descriptor in the sharing program with the descriptor containing the protection information as to how the object may be referenced--such as read only for execution, read-only, write, append, etc.

The following diagram is a simplification of how controlled sharing can be accomplished in descriptor-based systems. As indicated, each user program can (1) execute the operating system (OS) service functions and its own code within the addressing context established by the descriptor table, (2) can call on the operating system resource management functions, and (3) read and write its own data. Common library programs can also be shared among different programs as can data. With a descriptor capability, a variety of systems can be developed that will provide a high level of data protection.

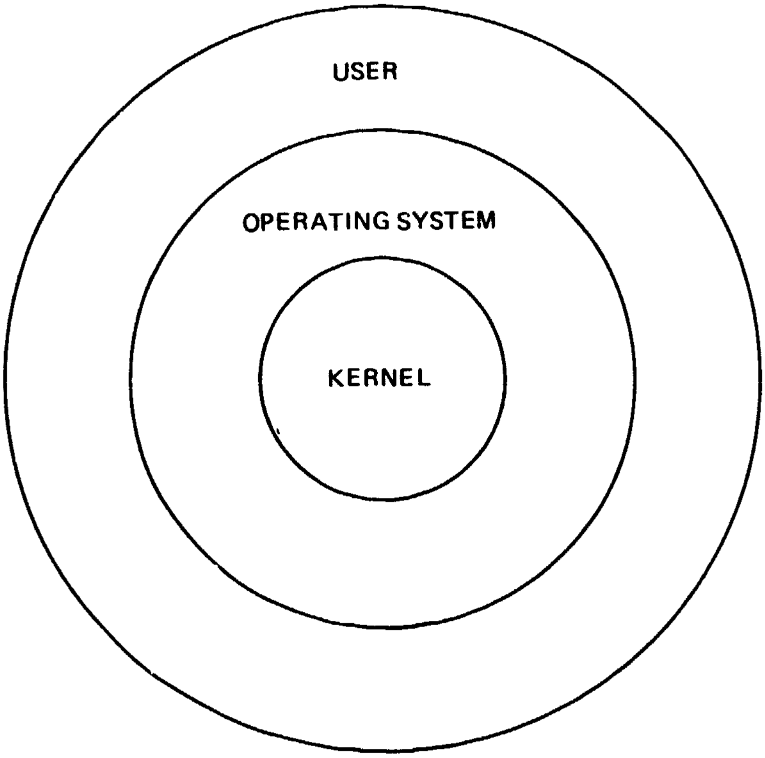


SOURCE: JAMES P. ANDERSON & CO.

Protection domains and the kernel concept

There have been several different approaches to the design and development of secure operating systems. One such approach employs what has been termed "protected domains." Most third-generation computer systems support two domains--a privileged supervisor state and a non-privileged problem state. In the privileged state, access rights are defined for such functions as scheduling and allocating the system's resources. In the non-privileged or problem state, the central processing unit cannot execute input/output and other privileged instructions. While these two protection domain mechanisms could theoretically provide a basis for security against deliberate subversion of the system, in practice, the problems of securing a computer system are so complex that many researchers have concluded that more sophisticated protection mechanisms are needed.

One approach that has been taken is increasing the number of protection domains, thus adding additional barriers that must be circumvented for a successful penetration. A three-domain approach has been used to structure the system into three environments--the user environment, the operating system environment, and the kernel environment--as shown in the following illustration.



To be effective, all security-sensitive elements of an operating system must be located in the security kernel. The kernel is placed at the very highest level of protection, or innermost section of the system, while other functions of the operating system are placed at lower levels. Under this approach, the proper functioning of protection is isolated from the remainder of the operating system and is not dependent upon the behavior of the outer layers (or less protected levels) of the system.

A methodology exists for proving the security worthiness of operating systems employing the kernel concept but has not been applied to large systems. Research is continuing in this area at several locations.

Other approaches

Operating systems have been developed with security as one of the objectives and have attempted to achieve this objective by creating a foundation, through good design, for establishing the reliability of existing security features. In these systems, the security-sensitive elements are normally scattered throughout the system as opposed to the grouping of such elements as discussed above in the kernel concept. The reliability of such systems can be demonstrated only through detailed study and use of penetration techniques. Unfortunately, successful penetration proves the presence of protection failures, but does not prove that all flaws have been detected. Nevertheless, these operating systems are purported to offer a higher level of protection than other such generally available systems.

SHARED DATA

Data sharing among users at the same sensitivity level is possible today. However, the current state-of-the-art in computer security will not permit what is termed "hierarchical data sharing"--a technique that allows users with higher level access authorization to obtain lower level sensitive material but not the converse. This will hamper efforts in the implementation of any multilevel privacy classification scheme that may be developed in the future. (See p. 10.)

Controlled data sharing at the same sensitivity level can be accomplished between dedicated computers and virtual machines through an external system interface whereby the output of one system is used as the input to another. With prcper controls, this technique can provide a high level of protection. Transaction and descriptor-based systems that have been properly designed and implemented can also permit reasonably secure data sharing. Further, other operating systems have been designed that purport to provide a higher level of protection than other conventional operating systems in general use, where high-volume data sharing is required.

It appears that some form of data sharing between agencies can be conducted in a reasonably secure technical environment. However, the administrative problems involved--such as what data is to be shared, who may authorize sharing, and how oversight is to be provided--have been more formidable.

The administrative problems have been significantly reduced with the enactment of the Privacy Act of 1974. This act (1) precludes inter-agency sharing of personal identifiable data without the individual's consent unless specifically authorized by law (which includes the specific exclusions contained in the act) and (2) makes OMB responsible for oversight to ensure proper implementation of the act by the various agencies.

SHARED COMMUNICATIONS

Safeguards against unauthorized use of the communications network to access computer systems can be provided through such design and procedural requirements as identification, access control, and access auditing.

A network can be so constructed as to allow or deny access to any terminal user, or between any terminal and computer, based on criteria separate from that used for controlling access to the ADP system. These network controls are similar to those already in use for computer systems. In fact, computers are used to provide the network safeguards.

A network can be constructed to produce automatically, and maintain records of usage and incorrect or improper attempts at access. Positive action can be taken to disconnect a user who fails to provide acceptable responses when challenged and a human controller can be notified when such attempts are made. Any user can thereby be restricted to communicating with only a designated ADP system or systems. Therefore, access of an ADP system by another can also be controlled by the network, and potential threats to privacy--through the trading of information--can be controlled. In addition, modern communication networks are well suited to the use of cryptography.

Our report entitled "Vulnerabilities of Telecommunications Systems to Unauthorized Use" (LCD-77-102, Mar. 31, 1977) noted that telecommunications systems were vulnerable to various penetration techniques that may be used for (1) gaining access to the system and (2) intercepting and interpreting communications traffic carried over the system or inserting traffic into the system. The report further noted that the difficulty of penetration was dependent upon such factors as the adequacy of administrative controls, the competence and integrity of telecommunications personnel, the physical security maintained over telecommunications facilities, the technical security resulting from telecommunications technology, and the penetrator's technical knowledge and financial resources. Where it is determined that the vulnerabilities of a given telecommunications system are unacceptable, cryptography can be employed to secure the communication links.

Data encryption

Cryptography in a computer network involves the use of an encryption device at the point of data transmission and a decryption device at the point of data reception. This means that these devices and related control equipment are required at all remote terminals or terminal controllers as well as at the computer facility.

The National Bureau of Standards published the Data Encryption Standard on January 15, 1977, (Federal Information Processing Standard Publication 46). This standard specifies an algorithm to be implemented in electronic hardware devices used for the cryptographic protection of computer data. It became effective on July 15, 1977, and applies to all Federal data processing systems and associated telecommunication networks under development as well as to installed systems when it is determined that cryptographic protection is required.

Encryption is expensive; therefore, it is important that a definite need be established, through a formal threat analysis, prior to a decision to employ this technology. The National Bureau of Standards recommends that other security safeguards, such as identification, access controls, and access auditing be implemented before sophisticated encryption devices are procured for the protection of personal data.

CONCLUSIONS

While absolute security cannot be assured, a high level of protection can be provided personal information in a multiuser computer network. Such protection is contingent upon the configuration and design of the network. A policy of isolation can be implemented and security established as a system objective.

The major problem to be resolved by users is the definition of the proper trade-off between (1) economies achievable through the use of modern computer/communication technology and (2) the added cost of obtaining the level of protection for personal information that is appropriate for the threat involved. By properly addressing this problem and with appropriate oversight as provided for in the Privacy Act of 1974, we believe a balance can be drawn between the use of modern technology and the protection of individual privacy.

CHAPTER 5

SECURITY CONSIDERATIONS

IN FUTURE COMPUTER PROCUREMENTS

It is possible to write a request for proposals in such a way as to acquire a computer network that provides an acceptable level of security. However, this is possible only when security is established as a system objective and a method exists to determine that the objective has been obtained.

The practice of merely including various security-related features and mechanisms in a request for proposals provides little assurance that the resultant system will in fact provide an adequate level of protection. Further, the failure to properly evaluate an offeror's capability to meet mandatory security requirements contained in requests for proposals has resulted in several bid protests. [1]

This chapter discusses one approach to acquiring a computer-operating system where the level of security provided can be evaluated and subsequently validated.

STRUCTURED DEVELOPMENT OF SPECIFICATIONS AND SYSTEM EVALUATION

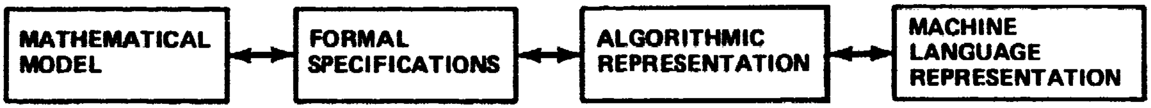
After analysis has been made of the functions that a system is to perform and the environment in which it is to operate, the security requirements should be stated in terms of positive statements of what is expected from the system and consolidated into a formal statement of security. Such a statement should define what kind of data is being protected and how the computer would recognize such data. Further, the statement should include a strict definition of who is to be authorized to access protected data, and how the system would recognize an authorized user.

The formal statement of security is then translated into system specifications. The problem is to verify that

[1] PRC Computer Center, Inc., et al., 55 Comp. Gen. 60 (1975); and Computer Network Corporation, et al., 56 Comp. Gen. 245 (1977): as modified by Computer Network Corporation, et al., 56 Comp. Gen. 694 (1977).

these specifications are complete and consistent with the stated requirements, and that they will function as intended in an operating environment.

One possible solution, based upon work sponsored by the Air Force and conducted by the Mitre Corporation, [1] involved (1) use of a mathematical model to convert the security requirements into specifications. The following are the components of such a scheme:



A mathematical model is constructed which represents those security requirements for which formal statements have been prepared. From the mathematical model, it is possible to formally specify a program which implements the mathematical model on a computer. From the formal specifications, an algorithmic representation of the program can be prepared which is then converted into machine language. At each of these steps--mathematical model, formal specifications, algorithmic representation, and machine language representation--compliance with the security requirements must be verified. The compliance determination will involve, in some steps, the use of mathematical proof techniques and in others, specifically the machine language representation, thorough testing.

BENEFITS OF THE FORMAL APPROACH

The foregoing process would be a dramatic departure from the current process of procuring computer systems--citing specifications for security related features. The following are the two major benefits of the formal approach.

First, the formal approach of developing requirements in terms of what a system has to do in order to implement a

[1] Edmund L. Burke, Synthesis of a Software Security System, The Mitre Corporation: Bedford, Mass., August 1974.

given policy is only slightly different from the approach used in other procurements. The formality of the process is somewhat different, but is within the state-of-the-art and training of a large number of computer scientists both inside and outside of Government.

Second, the formal approach obtains meaningful proposals by permitting prospective vendors to respond in a way best suited to their product line. This is accomplished by providing the vendors with the formal specifications and requiring them to develop the algorithms and establish the correspondence between the formal specifications, algorithms, and their software.

The complexity of this process of obtaining a computer-operating system that meets a desired security policy will depend on the degree of sharing intended for the system and the extent the system architecture addresses the protection issue. The benefit of using a formal method is that the protection provided is precisely defined and capable of being tested. The disadvantage is the effort required to develop the formal specifications and evaluate the vendors' proposals.

CONCLUSIONS

The process described above provides one method for acquiring computer software meeting specific security requirements which shows promise. However, at this time, we cannot be certain that it will prove appropriate for general use. Other approaches may be developed that will be equally or more effective. Regardless of the approach, it is important that the specifications contained in the request for proposals fulfill the users' security requirements. It is equally important that a reliable method be used to test the software for compliance with the specifications before selection is made.

CHAPTER 6

CONCLUSION AND RECOMMENDATION

CONCLUSION

Today's advanced teleprocessing technology provides the capability to store and retrieve vast amounts of information maintained about individuals and, as such, can pose a serious threat to privacy if not properly controlled. To reap the benefits of this technology while providing a high level of protection to personal information, definitive policies and guidance are needed as a basis for detailed procedures for resolving fundamental problems facing Federal agencies.

In structuring a computer system containing personal information, it is possible for the agencies to identify and describe the data to be protected including the: (1) volume to be processed, (2) frequency and types of accesses, (3) amount of sharing required, and (4) communications needed. A formal risk assessment and threat analysis can be conducted, and security requirements can be developed in terms of positive statements of desired system performance. Formal specifications that meet the users' security requirements are possible, as are the methods used to ensure that the hardware and software reasonably conform to the specifications. To accomplish this in a cost-effective way, further studies are needed to resolve the following problems.

1. How is personal data to be recognized? It would appear that some form of labeling is necessary in order to permit ready identification in both manual and electronic processing. Labeling, as currently used for national security information, alerts the user to the need for appropriate safeguards.

2. What level of protection does personal information demand? Regardless of whether all personal information is to be protected at the same level or a classification system is desired, the appropriate degree of protection must be clearly defined. Without such a definition of the requirement, procedures cannot be developed that will provide adequate protection uniformly throughout the Government.

3. What security standards are necessary to safeguard personal information at a desired level of protection? Such standards provide a means of

determining if adequate security has been provided. They are imperative to guide both those designing- and implementing-computer systems and those verifying the security of the systems. Further, such standards could preclude the acquisition of costly security features and devices which would not contribute to achieving the required level of protection.

4. What automation and information technologies and products are needed in order that computer systems can meet established standards? Such identification is necessary to permit the agencies to obtain or develop the hardware and software required.

Pending continued study and resolution of these problems, a policy of isolation, as discussed in chapter 4, can be adopted which will provide a high level of protection to personal or sensitive data. Once adopted, the policy sets the general parameter for the agencies to use in designing and procuring their information systems.

We believe the merging of modern automatic data-processing and communication resources into computer networks can be accomplished while providing a high level of protection for personal information. Use of today's advanced teleprocessing technology would facilitate achieving the efficiency and economy objectives of shared equipment, programs, and data as envisioned by the Brooks Act. A careful application of the available technology, in compliance with the administrative practices and safeguards required by the Privacy Act of 1974, could reasonably protect the confidentiality of personal information while enabling the Government to realize those efficiencies and economies.

However, cost-effective protection of individual privacy is dependent upon resolving the underlying problems pertaining to the methods and procedures for assessing and solving Federal agencies' security requirements. The full realization of economies from advanced teleprocessing technology continues to be hampered because of the lack of definitive guidance for agencies to apply in the requirements determination, procurement, and system development processes. Because of the Privacy Act's mandates, this guidance is needed today.

RECOMMENDATION

We recommend that the Director, Office of Management and Budget, take the necessary action to expeditiously provide the Federal agencies with comprehensive guidelines that (1) contain the definitions and criteria necessary to permit an assessment of their security requirements; (2) provide the methodology to be used in conducting such assessments; (3) identify the physical, administrative, and technical safeguards that should be applied in satisfying their security requirements; and (4) specify the means to justify the associated cost.

COMMENTS ON ISSUES DISCUSSED IN THIS REPORT

We obtained comments on the issues discussed in this report from individuals knowledgeable in the subject as well as from Federal agencies with responsibilities for these matters.

Because of their respective roles in the executive branch as central management agencies and their special knowledge and interest in implementing policies and programs of the subject legislation (i.e., the Brooks Act or the Privacy Act), we requested reviews and comments from the following agencies:

--Office of Management and Budget.

--Office of Telecommunications Policy (OTP).

--General Services Administration.

--Department of Commerce.

--Civil Service Commission (CSC).

--Privacy Protection Study Commission.

The comments have been considered in appropriate places throughout the report and are briefed in the following parts of this chapter.

Acknowledgement of comments by selected individuals

We obtained comments from a large number of individuals who, because of their varied experiences and associations, were able to offer a wide variety of viewpoints on the issues covered in the report. (See app. I.) We appreciate their cooperation and are grateful for the significant contributions they made. These technical review comments, in most instances, described the report as an adequate, accurate statement of the current status and future of computer security technology. However, the reviewers were not always in agreement on all matters. In particular, opinions varied on the prognosis for future developments in computer-networking and security techniques. Where the reviewers did not fully agree with parts of the report, they usually made specific, useful suggestions for clarifying or expanding areas of discussion. We made certain revisions and additions to the report to the extent that it was needed, in our judgment, for accuracy and completeness.

AGENCY COMMENTS AND OUR EVALUATION

OMB comments

The Director, Office of Management and Budget, stated that OMB generally agreed with our recommendation. He said that OMB shares the dual concerns expressed in the report that (1) more definitive guidelines and standards are required to assure that the use of advanced information technology does not result in abuses of personal privacy and, on the other hand, (2) advanced technology be employed wherever it can contribute to the efficient operation of Government.

He stressed, however, that it should be understood that several years may pass before definitive guidance can be issued in some areas, particularly for measuring data sensitivity. OMB was concerned that people in the technical (ADP and telecommunications) community may be expecting semiautomated substitutes for the managerial judgment which they are required to exercise in defining security requirements. We agree that definitive guidance will take time to develop and that agencies should be cautioned not to be overly optimistic in their expectations for more specific guidance if OMB determines that it can not practically be produced in the future.

The Director's letter acknowledged that the Privacy Act of 1974 was in part the result of public and congressional concern that increased use of sophisticated information technology presented an imminent threat of unwarranted invasions of individual privacy. OMB cited the agencies' direct responsibilities to prevent such abuses under the act's provisions and stated that agencies are required to

> "* * * establish adequate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats of hazards to their security or integrity which could result in substantial harm to any individual on whom information is maintained * * *" 1/

OMB believes this language is necessarily general, leaving to each agency a great deal of discretion in defining its security requirements. OMB believes the act is premised on a concept of agency accountability, that each agency can best determine the level of safeguards required to protect the information which it maintains. While recognizing the need for central guidance and the development of technical standards, wherever possible, to assist agencies in complying with the act, OMB feels its responsibilities under the act are and will be adequately met by delegations to the National Bureau of Standards (NBS) and other central agencies in specific functional areas. We basically agree with OMB's approach and views. However, we believe that the efficiencies and economies attainable through modern computer technology will not be realized until computer security problems are addressed and solutions have been achieved. Therefore, we believe that guidance to agencies should receive a high priority and level of effort by OMB and the agencies to which it delegates such tasks.

OMB said that approaches to securing software in shared network systems (e.g., the "security kernel" and virtual machines) are more in the nature of "theoretical possibilities" and are the subject of heated debates among researchers both as to their practicability and the level of security which they can provide. We have incorporated certain revisions to chapter 4 to cover this comment. These revisions reflect the extensive advice and views we obtained from many individuals in the technical community who were asked to review and comment on the report.

OMB predicted that for the immediate future, determinations of computer security requirements--particularly in highly sophisticated systems--are likely to continue to be judgmental, while OMB pursues the development of more definitive security standards and objective measures of security requirements. Until such standards are issued, OMB is satisfied that adequate control mechanisms are in

1/5 U.S.C. 522a (e) (10).

place through (1) the program and budget review process, (2) the procurement process, and (3) reviews of new systems now required under the act. OMB believes the outlined course of action is consistent with the letter and spirit of the act and the recommendations in our report. Although we concur with OMB that a primary emphasis of the act places responsibilities directly on the agencies to meet cited requirements of the legislation, the act also requires adequate central guidance and oversight which must ultimately be measured in terms of agencies' performance and compliance.

OMB said it particularly welcomes any additional specific proposals to improve the quality of executive branch compliance with the act. While this was not the main purpose of the present report as discussed in the introduction and scope (ch. 1), our plans for further reviews are expected to focus more attention on compliance with the act. Reviews of selected systems will be directed toward specific ways for more effective implementation by agencies. Other reviews are planned to further examine opportunities for improving central guidance and oversight of the act.

OTP comments

OTP's letter states its generally favorable reaction that the report evidences careful scrutiny of its subject and expresses the hope that the report would bring a realization to Federal agencies of the important responsibilities imposed upon them by the act.

OTP feels the purpose of the report should be clearly stated. (See introduction and scope in ch. 1.) In this regard, it believes a clear distinction should be made between the principal focus of the act on limiting the amount and scope of data collected and the distinctly different but related issue of protecting personal information stored and processed in Government computer data bases.

OTP points out further that the act focuses on the activities of Government agencies related to expanded data collection/dissemination rather than increased vulnerability of stored data as the major potential threat. OTP acknowledged, nevertheless, that once collected, Government data must be safeguarded from misuse by Government employees and outsiders. OTP feels the more relevant threats are internal and of a nature that would not be protected against by the security measures discussed in the report.

One concern expressed by OTP is that if the internal aspect of the data security problem is not given more attention, it may be neglected by agencies. The threats and protective measures we discussed in chapters 3 and 4 can be applied in controlling access to data against both internal and external threats. We agree, however, that agencies must devise broadly scoped systems of internal control and accountability which are not limited to the security techniques discussed in this report. These measures are being addressed in our other reviews of selected agency systems.

OTP expressed a second concern that presentations in chapter 4 could encourage agencies to expend more resources in security than would otherwise be justified to counter threats which may not even exist. It acknowledges, however, our suggestion that a formal threat analysis be made prior to and as justification for employing costly protective features. (See p. 28.) Because we share OTP's concern that protective measures must be justified, our report also places special emphasis on the need for defining the level of protection appropriate for personal data. (See p. 10.)

In summary, OTP expressed its hope that this report will be an initial effort toward raising the general level of consciousness about the larger issue of protection from invasions of privacy, which OTP sees as less well defined than the issue of data security treated in the present report.

GSA comments

GSA's letter said that GSA supports our continuing efforts in the area of computer security and privacy. GSA also said that it is greatly concerned with the issues raised in this and our other recent GAO reports. GSA plans to be working with us, OMB, NBS, and the Senate Government Operations Committee in a concerted effort to improve the security of Federal computer installations.

GSA's letter specifically ,upports our recommending that OMB issue guidelines containing criteria and methodology for (1) assessing security requirements and (2) identifying the safeguards and cost justifications to be applied in satisfying them. Toward this purpose, GSA offered to (1) assist OMB in the formulation of overall executive branch policy, (2) participate with NBS in the development of the necessary technical guidelines, and (3) establish the operational policies and procedures to ensure their implementation.

We believe GSA's suggestions for a joint and cooperative effort has merit. GSA can make this larger contribution toward implementing the recommendation because of its unique central management role for ADP in the executive branch. GSA can particularly broaden its contribution in the area of devising and implementing policies and procedures when procurements of equipment, software, or services are planned in systems being developed by agencies. This would be on the basis of responsibilities authorized by the Brooks Act.

Other comments were directed to specific discussion in the report in the following areas:

--GSA believes that the report could more strongly emphasize the ability of a modern communications network to improve security, and it provided additional details of how this can be accomplished. (See pp. 27 and 28.)

--GSA agrees that writing security needs into procurement documents is a problem which must be solved. (See p. 30.)

Commerce comments

The letter from the Assistant Secretary for Science and Technology, Department of Commerce, observed that Commerce has also recognized the privacy problem and that NBS has had a program dealing with it since 1972. The Assistant Secretary said that the report performs a valuable service by giving a proper perspective to the problems that can occur in computer network environments by emphasizing that the potential for misuse of personal data increases as more personal data is centralized and shared by many organizations.

Commerce agrees with the conclusions and recommendations in the report and, in particular, feels that comprehensive guidelines and standards are needed to help agencies apply existing security techniques and develop new, more cost-effective techniques. While technical guidance is only one aspect of the overall problem, Commerce feels that the efforts carried out by NBS are making significant contributions toward the recommendation and will continue to do so.

Work at NBS was listed in three areas:

1. With respect to our recommending a methodology to be used in conducting an assessment of security requirements, draft guidelines on security risk

analysis were undergoing agency coordination. (Published as an internal NBS document, NBSIR 77-1228, Mar. 1977.)

2. A guideline on automated personal identification techniques was pending publication. A report on use of unique identifiers and a survey of approaches that could be used in designing and implementing operating systems were also being published. (Published as a Federal Information Processing Standards Publication, FIPS PUB 48, Apr. 1, 1977.)

3. A model has been published to help determine the cost of alternative approaches to protecting personal information. (NBS Technical Note 906; June 1976.)

Commerce observed that the computer security problem is very complex and is further complicated by the great variety of different computers and computer network environments. It acknowledged there are many areas where the underlying technical problems have not been resolved. Commerce did not say whether the rate of progress toward resolving the technical problems needed to further perfect guidance to agencies could be accelerated. It did not comment as to whether increasing the funding for research and giving these efforts a higher priority would be feasible in view of the long timeframe normally required.

CSC comments

CSC's letter advised that CSC had no specific comments relative to the substance of the report but furnished the following additional information on its activities to carry out training responsibilities under OMB's Privacy Act implementation guidelines. CSC has:

--Conducted multiple interagency training sessions.

--Prepared and distributed to all agencies (in Mar. 1975) a training module on the Freedom of Information and Privacy Acts for use with or independent of formal training courses and redistributed revisions to the module in June 1976.

--Provided clearing house assistance to agencies in locating and developing slide-tape, video-tape, film, and other types of presentations.

CSC's training activities can contribute significantly to the effective implementation by broadening its focus. The activities directed toward short indoctrination courses for large numbers of people and related instructor training are important because this quickly and effectively spreads information about the Privacy Act's requirements widely into agencies. In its longer range plans for continuing the training into the future, however, CSC should also consider focusing more instruction in greater depth in areas of physical security and computer system security for agency personnel who are involved in developing and operating or administering information systems containing personal data. This can be done either by adding these subjects to the course offerings or restructuring the content of selected courses given in the past in more traditional areas of ADP.

Privacy Protection Study Commission comments

The Commission's Chairman said that it would not be practical for the Commission to issue a formal response to the report. Personal responses were obtained from one of the Commissioners (Vice-Chairman) and its staff's technical advisor expressing their individual views. These comments, which were not offered as the Commission's views, were considered in appropriate places throughout this report.

COMMENTS OBTAINED

FROM SELECTED INDIVIDUALS

We obtained comments from a large number of individuals with varied experience on the matters covered in this report. We appreciate their cooperation and are grateful for their significant contributions.

The reviewers in nearly all instances agreed that the report presents an objective view of the issues involved and the current status, problems, and likely future of computer security technology. However, all of the reviewers were not in agreement on all matters. In particular, opinions varied on the prognosis for future developments in computer-networking and security techniques. Where the reviewers did not fully agree with parts of the report, they usually made specific, useful suggestions for clarifying or expanding areas of discussion. We made certain revisions and additions to the report to the extent it was needed, in our judgment, for accuracy and completeness.

The names and affiliated organizations of the individuals selected to review the report are listed on the following pages of this appendix. While we requested these comments from individuals selected mainly because of their technical expertise, some directly or indirectly expressed a point of view of their firm or organization. Others stated they were commenting only as individuals.

LIST OF TECHNICAL REVIEWERS

AND THEIR AFFILIATED ORGANIZATIONS

James P. Anderson:
James P. Anderson & Company
(contract consultant to GAO for this report)

Edmund L. Burke:
Group Leader, Intelligence and Information
Systems, The Mitre Corporation

Arthur A. Bushkin:
Manager, Statutory Impact Assessment
Projects and Staff Technical Advisor
Privacy Protection Study Commission

Ruffin R. Cooper:
Central Security Service
National Security Agency

Robert H. Courtney, Jr.:
Systems Research Institute
IBM Corporation

Robert H. Follet:
Federal Policy Coordination
IBM Corporation

John Gosden:
Vice President, The Equitable Life Assurance
Society of the United States

Dr. Carl Hammer:
Director, Computer Sciences
Univac Division, Sperry Rand Corporation

Donald G. Heitt:
Program Director, Federal Systems
Operations, Honeywell Information Systems

Dr. Paul W. Howerton:
Consultant

Robert V. Jacobson:
Assistant Vice President
Chemical Bank, New York, NY

Steven B. Lipner:
The Mitre Corporation

Patrick McGregor:
Director, Washington Operations
Network Analysis Corporation

Dr. Edward F. Miller, Jr.:
Director, Science Applications, Inc.

W. H. Murray:
Advisory Product Administrator
Data Security Support Programs
IBM Corporation

Dr. Eldred C. Nelson:
Director, Technology Planning and Research
Systems Engineering and Integration Division
TRW Systems, Inc.

Dr. Peter G. Newmann:
Senior Research Engineer
Stanford Research Institute

Donn B. Parker:
Senior Information Processing Analyst
Stanford Research Institute

Bruce Peters:
Systems Development Corporation

Dr. Philip A. Tenkhoff:
Vice President, Engineering & Communications
Computer Sciences Corporation

Shigeru Tokubo, RISOS Project:
Lawrence Livermore Laboratory
University of California

Willis H. Ware:
Vice-Chairman, Privacy Protection
Study Commission

Dr. Douglas A. Webb, RISOS Project:
Lawrence Livermore Laboratory
University of California

Henry M. Williams, Jr.:
Executive Services Administrator
AT&T Company

GLOSSARY

Access

The ability and the means to communicate with (input to or receive output from), approach, or make use of. Data access is often categorized by combinations of read, write, or execute.

Algorithm

A statement of the steps to be followed in the solution of a problem.

Application program

A computer program designed to accomplish a specific job or application, such as payroll, inventory, etc.

Authentication

The act of verifying the eligibility (i.e., authorization) of users and their agents (e.g., programs, terminals, etc.) to access specific categories of information.

Authorization

The granting to a user, a program, or process the right to access.

Capability

The right to access granted to an individual, program, or process.

Controlled access

The concept that all authorized users of a system be permitted access to that information and resources to which they are authorized, but to no more.

Data base

(1) The entire collection of information available to a computer system and (2) a structured collection of information as an entity or collection of related files treated as an entity.

Encryption

The transformation of data into secret, coded symbols.

Integrity

The state that exists when there is complete assurance that a system works as intended under all conditions. That is, the system reflects the logical correctness and reliability of the operating system, the logical completeness of the hardware and software that implement the protection mechanisms, and the consistency of the data structures and accuracy of the stored data.

Isolation

The containment of users, data, and resources in an operating system such that users may not access each other's data and resources and may not manipulate the protection controls of the operating system.

Memory

The storage that is considered integral, internal, and primary to the computing system.

Offline

Pertaining to operations that are independent of the main computer.

Online

Pertaining to (1) equipment or devices under control of the central processing unit or (2) a user's ability to work with a computer.

Operating system

Software that controls computer operations including scheduling, debugging, input and output control, accounting, storage assignments, data management and related services. Sometimes called the supervisor, executive, monitor, or master control program.

Parameter

A variable that is assigned a constant value for a specific purpose or process. For example, parameters may determine the number of characters in a field.

Password

A protected word or a string of characters that identifies or authenticates a user, a specific resource, or an access type.

Register

A memory device capable of containing one or more computer lists or words.

Transaction-oriented system

As used herein, a transaction-oriented system is one that permits a user only to input and receive specified data. The input and receipt of data is controlled by application programs. The users' interaction with application programs is achieved by means of macroinstructions which isolate the user from direct access to such programs.

User identifier

That information maintained on the computer system and used to identify authorized users and to authenticate their eligibility to access specific categories of information.