The Interactions of COMPUTERS and PRIVACY

*A. Michael Noll**
*Executive Office of the President***
Office of Science and Technology
Washington, DC, US

A survey of the existing relationship between computer usage and confidentiality, security, and privacy. The new problems raised by technology show gaps and inadequacies in laws, and it is argued that technology has not injured privacy but rather escalated it as a critical issue. The vulnerability of computerized files to theft and misuse is shown by comparison to conventional files, which then leads to an exposition of the various forms of attack and counterprocedures. Technical, administrative, legislative, and policy aspects are all covered to give a coherent picture of what present steps and future research must be undertaken.

*Present address:
Bell Telephone Laboratories, Inc.
Murray Hill, NJ, US

**The views expressed in his paper are those of the author and do not necessarily reflect the official policy or opinion of the Executive Office of the President or any other Federal agency.

INTRODUCTION

The digital computer, with its capabilities for storing, manipulating, and retrieving extremely large amounts of data, has been accused of being a new threat to privacy. Privacy in its interactions with technology is rightfully a complicated issue, but (from my viewpoint, and in the opinion of others), technology has not offended privacy -- technology has only quickened the pace and need for well-defined descriptions of privacy and adequate policies to protect the right of privacy. Technology has been the driving force in the escalation of privacy into an issue of national significance.

Because people are the ultimate users of information, people -- not computers and technology -- are the real potential violators of privacy. Computer technology only makes it easier and more efficient to gather, store, retrieve, and process large quantities of information; but, with the development of appropriate methods, computer technology will also protect the information stored within computerized files.

The vast amount of information stored in computerized files has created a situation in which it is very difficult, if at all possible, to assign a cost or value to information. The large number of different users, all with their own very large files, even makes it extremely difficult to know all the forms and types of information that might be accessible from a computer, and networking of computers makes this a nearly impossible task. This volume and variety of information will be a strong motivation for some persons to expend considerable efforts in an attempt to gain unauthorized information from some computerized files.

In some computer applications, physical protection of the computer itself will be sufficient to protect the information stored within the computer system, as only authorized users will have physical access to the computer. However, in many other applications a large number of users with different degrees of access to specified files will wish to use the computer, and control of the physical accessibility of the computer itself will be insufficient. Access to the files themselves will also have to be controlled, and this means that the computer system itself will have to control file access for different users. Computer hardware and software designed with security as one of the initial requirements will be required to obtain such control.

Thus, although the extremely large amount of information stored within a computer system is a lucrative target for theft, with appropriate computer security mechanisms the access to all this information could be so thoroughly controlled that bribing one of the users would be the cheapest way to steal information from the computer system.

Reproduced with permission from The Honeywell Computer Journal, Vol. 7, No. 3, 1973, pp. 163-172,

Ultimately the development of computer hardware and software for protecting information stored within a computer system would grant an ability to monitor and control the flow of information which would not be possible with manual systems, with thousands of file cabinets scattered throughout the country. Appropriate software and hardware controls would make it virtually impossible for an individual to gain unauthorized access to the information stored in the computer and steal the equivalent of either a single document or a large number of documents.

The essential problem of computer security is to protect sensitive information within the computer from accidental or deliberate modification, disclosure, or destruction.

The prime conclusion of this paper is that solving the technical problems of computer security will result in a new level or form of protection for sensitive information. Thus computer technology ultimately can serve to protect information from accidental or deliberate misuse, and thus help to de-escalate certain aspects of privacy as an issue.

PRIVACY, TECHNOLOGY, AND THE LAW

Privacy

Privacy is an elusive subjective term used to describe the state or quality of being free from the observation of others. Many forms of animal life on this planet seem to have acquired a strong need for this freedom from observation, and man most certainly has been no exception. However, privacy because of its subjective nature and apparent foundations at the natural law level is very difficult to guarantee, define, or even describe in formal legal terms.

How simple it would be if the US Constitution had explicitly guaranteed the right of privacy, but quite unfortunately the word "privacy" is not even mentioned in this document. The authors of the Constitution most certainly could not have foreseen ultraminiature transistorized electronics, ultrasensitive highly-directional microphones, and the other technological advances which are often construed as threats to privacy. Most certainly the founding fathers could not have foreseen the confusion and great debates that resulted from their failure to guarantee the right to privacy. However, certain manifestations of what might be construed to be violations of privacy, for example, illegal searches and seizures, were explicitly forbidden in the Constitution.

If privacy is claimed to be a right, albeit by vague permeation within the Constitution or by a stretching of natural law, then its explicit absence in the Constitution does not deny privacy its status as a right, because the Ninth Amendment to the Constitution states that the enumeration in the Constitution of certain rights shall not be construed to deny or disparage others retained by the people. And the people consider privacy to be a right retained by themselves.

The United Nations is a reasonably new organization, and privacy was an issue when that organization was formed. Therefore, not surprisingly, privacy was not ignored, and Article 12 of the United Nation's Universal Declaration of Human Rights explicitly granted to everyone the right to protection of the law against subjugation to arbitrary interference with his privacy. A recently approved amendment to the California State Constitution also specifically guarantees the right to privacy. However, in both these cases a formal definition of privacy is not given, and therefore the exact legal meaning of privacy remains hazy.

The net result of the lack of any formal legislative definition of a right of privacy is that the courts must decide all privacy issues, and the amassing of such court decisions and precedents forms an ever-evolving law on privacy. Although this "make it as you go" philosophy might be bothersome to some people, it nevertheless is basic to the American legal tradition, and enables the law and its interpretation to change to reflect society's needs.

Interactions of Technology and Privacy

Presently, threats to privacy often involve complicated technology and technology-oriented issues. Unfortunately, the legal profession is often a victim of its lack of affinity towards technology, but such technological ignorance only leads to confusion in the courtroom. Thus the popular attitude that technology has somehow injured privacy is easily reinforced as the courts and legal profession continue to wrestle with issues resulting from the interactions of technology with privacy. These interactions have quickened the pace with which privacy has become an important national issue.

The escalation of privacy as a national issue was indeed quickened by the availability of new tools created by science and technology. These scientific and technological tools either were developed in response to specific needs -- or needs were later discovered to justify the availability of the tools. At the risk of seeming too cynical, it will be assumed in the following discussion that the technology drove the needs -- this approach, though really immaterial to the discussion, is perhaps a little more entertaining and unfortunately is all too often true!

Many years ago, science and technology developed polygraphs, wiretapping, truth drugs, and many other techniques which were all useful in fulfilling needs to combat threats to security. Unfortunately, these tools could also be used in ways that many people would consider as violations of their right of privacy.

Representative Cornelius Gallagher and Senator Sam Ervin were quick to point out the dangers to privacy from these technologies, in hearings conducted by their respective committees. Alan Westin, in his book *Privacy and Freedom,* continued the analysis of the threats to privacy which could occur, and perhaps had occurred, by misuses of these technological tools. However, as time passed, privacy as an issue involving these particular tools slipped slowly from public attention.

More recently, science and technology produced computers, data banks, and communications networks to enable almost instant transmission of information to a remote location. These tools were needed by government and industry to gather and assimilate the information required to implement, operate, and provide services and products for the people. Vast amounts of statistical, administrative, and intelligence information could be efficiently and effectively handled with these tools.

Though unfortunate, yet not completely without justification, the public's image of computers is a never-forgetting, never-forgiving, all-powerful, cold, methodological, decisionmaking machine. All the fears of computers, fortified by the fantasies of Orwell's *1984,* seemed to become reality in the mid-1960s when the White House Bureau of the Budget proposed a national data bank containing information on all citizens. The result was a vociferous cry against this new perceived potential for possibly further invasions of the privacy of the people.

Ultimately, the greater common good that potentially might result from the use of computers for maintaining very large centralized data banks was forced to defer, for the time being, to even the most minute risk of a violation of a claimed right of the people. The proposal for a national data bank quickly disappeared in the files of the bureaucracy amidst claims that the Nation had been saved once again from the technologists.

Previous privacy issues primarily involved the privacy of the people. Within the past few years, science and technology developed timesharing, remote terminals, and data communication networks for computers. To operate computers efficiently and effectively, sensitive and nonsensitive information might exist together in the same computer and be accessible from remote locations. The result, for example, could be a "line" into the computers of such "sensitive" Federal agencies as the Atomic Energy Commission, the Central Intelligence Agency, and the Federal Bureau of Investigation. Obviously, governmental agencies and many industrial firms are seriously concerned about the "privacy" of their own information. To the people's concern for privacy has now been added a government and industry concern for the privacy of information about themselves!

The prime conclusion is that technology per se has not injured privacy but has rather escalated it as an issue.

INFORMATION AND COMPUTERS

A fair amount of insight into the nature of the problems encountered in protecting information stored in computerized files can be gleaned by observing the similarities and dissimilarities between computerized and conventional manual files.

Conventional Files

Files consist of information which, in conventional files, is usually in the form of written or printed documents. If the information in the documents is private, then the documents themselves are classified according to their sensitivity. Elaborate procedures are then instituted along with appropriate numbering schemes for keeping track of the documents as they are transmitted from person to person.

The access of people to these documents is controlled according to the sensitivity of the documents. Persons with access to documents affecting the national security of the United States must not only be cleared to the same level as the document but must also demonstrate a "need to know" the information contained in the document.

The documents themselves are usually stored in metal file cabinets with combination locks on the doors. In general, these cabinets are easily broken into, but they are designed in such a way that the occurrence of a forced entry would be easily detected. Since a file cabinet can only contain a fairly small number of documents, a thief intent on obtaining a large number of documents would have to break into a large number of cabinets.

A manual system of paperwork to keep track of documents is itself fallible, and documents sometimes disappear or are lost. Nevertheless, only a small number of documents could ever be lost at a time. Thus a manual system for controlling sensitive documents has the properties that a single document can be lost or stolen, but large numbers of documents are extremely difficult to steal or misplace.

The combined use of locks on file cabinets, procedures, and investigations of the trustworthiness of people creates a security system in which the theft of information is not impossible but costly. Hopefully, information is secure if the cost of the theft exceeds the value of the information.

Computerized files

Unfortunately, technology often has a way of upsetting the conventional ways of doing things. One protective mechanism in the system for protecting conventional documents was that the physical theft of a document would be noticed so that the appropriate corrective measures could be initiated. However, the development of photography and xerography quickly changed all of this, since a document could be copied and placed back in the file, and the theft would never be detected. Although the original document itself was not stolen, the information contained within the document was copied and stolen. The technologies of photography and xerography thus were a great improvement over theft of the information in a document by manual transcribing with paper and pencil. Computer technology and computerized files have introduced far more complicated possibilities for the theft, destruction, and modification of information -- and on a scale previously impossible.

Information stored within a computer system is usually in the form of electromagnetic energy or electrical impulses. These impulses are internally organized within the computer system to form files of information which, at the request of the user, can be translated and printed by the computer on conventional paper. The amount of information stored within the computer system is considerably greater and requires considerably less space than a conventional manual system of files. The computer can perform analyses of the information contained within its files and also retrieve the information required to satisfy some specific request.

Computerized files are vastly superior to conventional files in terms of efficiency and they also enable file processing which would be impossible with conventional manual filing systems. A possible disadvantage to computerized files, other than their cost, is that unless adequate attention is given to the creation of an effective environment for communication by man with the computer, an estrangement between the user and the information stored within the computerized files might occur.

A computer system usually includes a variety of devices for storing data, magnetic tapes and disks are being presently the most frequently used. The computer also has its own internal memory, and capacities of five million (5×10^6) bits are not at all uncommon. (A storage capacity of one million bits is equivalent to over 200 one-thousand-word documents.) Research and development in storage technology is an extremely active area, and a variety of bulk storage devices with capacities of a million million (10^{12}) bits are already available. Many computer scientists speak very seriously of storing the entire contents of the Library of Congress in digital form accessible by computers, which would require a storage capacity on the order of a hundred million million (10^{14}) bits.

In addition to such vast storage capacity accessible to a single computer, modern data communication networks interconnect computers so that one computer has access not only to its own storage devices but also to all the storage devices of all the computers on the network.

Thus a computer user may have at his disposal access to a volume of information that would be impossible with conventional file cabinets. He can easily delete, copy, or change any part of all this information from a terminal that might be located a great distance from the computer and actual storage device containing the information.

Theft by copying information contained in a document stored in a conventional file cabinet requires physical removal of the document from the cabinet, even if only for the short time required to photograph or reproduce it. Theft of information from computerized files is also through copying, but the requirement of physical removal of the original information from the file is meaningless, since copying occurs within the computer and the file itself. The ability to detect a physical removal of information is thus meaningless with computerized files. Detection of theft from a computerized file requires an ability to detect unauthorized copying of the information within the file.

Unlike conventional files, in which the very large number of separate cabinets makes unauthorized access to all the information impossible, the methodology used to gain unauthorized access to any one computerized file can often be used to gain unauthorized access to all the files stored within the computer system.

Since many users will usually be sharing the same computer, the computer itself must be able to detect an unauthorized entry into a restricted file stored within the computer system. Authorized physical access to the computer does not usually imply authorized access to all the information stored within the computer system, as it would for all documents stored in a file cabinet.

Therefore each and every user of the computer must obtain monitored and controlled access to the different computerized files only through the security mechanisms of the computer system. In this way, a computerized security mechanism is always checking and monitoring the accesses to the files by all users. This situation is again quite different from a conventional manual filing system, in which it would be physically impossible to automatically record and monitor all physical access to each and every file cabinet, and even each and every document stored in a cabinet.

A digital computer, being programmable, can exercize considerable control over the abilities of different users to access different files. However, for this control over file access to be meaningful, the software that accomplishes it must itself be protected, and an adequate level of protection requires solutions to a number of current computer software and hardware problems.

The term "computer security" is used to include the technical area dealing with the threats to the security of information contained in a computer and also the research and development of the appropriate protective procedures and methods against these threats.

COMPUTER SECURITY

The Threat to the Security of the Information Stored in Computerized Files

In the past, the computer executed a sequence of single programs, and a new program did not begin until the preceding program was completed. If sensitive information was used by a program, then the core memory might be completely erased immediately before and after the sensitive program was executed so that no sensitive information accidentally remained in the computer. Any magnetic tapes containing sensitive data might be kept under lock and key. The computer itself might also be protected physically, and perhaps even the whole facility in which the computer was located might be protected by barbed wire and armed guards. Employees themselves might be investigated periodically to make certain that they were not security risks. A computer situated in such a facility and operated in such a careful manner was essentially in a benign environment. In effect, a physical and administrative security fence had been built around the computer and the users.

Today, many programs reside simultaneously in time-shared and multiprogrammed computers. Thus, if any one of these programs deal with sensitive data, then the other programs must be denied access to this data. The solution to this security problem has been to attempt to extend a "security fence" into the computer itself so that individual programs and data would be secure from each other, and this created the need for the appropriate computer hardware and software to keep individual programs and data secure from each other. The prime reason for this early work in computer security, however, was to protect the supervisory software from errant users.

Many users may actually be located at some remote distance from the computer installation itself, which greatly complicates the security situation, since the remote users are usually located outside the physical security fence and their remote terminal gives them entry to an otherwise physically-secure computer. The threat to information stored within the computer therefore results from remotely-located multiple timesharing users who all have needs for different information of varying degrees of sensitivity, which must be protected from improper disclosure or use because of either possible injury to the privacy of an individual or possible harm to the government or some other organization.

A concentrated attack on information stored in a computerized file would be completely different from an attempt to break into a conventional file cabinet, in which brute force and crowbar would probably be the quickest method. The potential attacker, perhaps having available a computer on which all the access protection systems of the computer to be attacked are simulated, could write programs of his own to assist his efforts to "crack" the hardware and software protecting the attacked computer. The simulated attack could be conducted from a remote terminal, and the simulation on the attacker's own computer would prevent any knowledge that an attempted attack is even being planned. After the attacker has determined the appropriate procedures and written the program required to attack the actual computer, he might then commence the actual attack.

Value of Information

A basic design principle of conventional security systems is to make theft of information not impossible but very costly, relative to the value of the information. The application of this principle requires that the value of the information can be assessed reasonably, which is usually possible for the relatively small number of documents stored in a conventional file cabinet. However, the vast amounts of information stored in computerized files, coupled with the power of computers, has created a situation in which large amounts of sensitive information might be vulnerable to an undetected theft in their entirety. Also, the potential risks for changing and destroying vast amounts of information have been greatly increased by the widespread use of computers and computerized files; new ways will always be unearthed to exploit information that will defy relational assessments in advance of such exploitation.

The interconnection of computers through data communication networks will further complicate attempts at assessing threats relative to the "value" of the data stored in the computer. Once a small hole in the security system of any one of the interconnected computers is discovered, it can be enlarged and used to gain entry into many other computers. Thus the total value of all the information potentially accessible in the whole system of interconnected computers must be assessed -- probably an impossible task. Thus, with computerized files, the sheer bulk of stored information becomes a liability rather than a protective asset.

A further complication in attempting to determine the value of information stored within a computer system is that the information will undoubtedly have considerably different value to different people. For example, the operator of a computer system might give little or essentially no value to information about the health of a large number of people, but the people themselves might be quite concerned about violations of their privacy through unauthorized access to this health information. Hence, they would give very high subjective value to this information.

Thus, since values of computerized information are probably impossible to ascertain in any realistic manner, some design principle for computer security other than a comparison of the value of the information with the costs of theft must be devised.

Adequate Computer Security

Computers are ultimately used by people who will have been authorized access to particular computerized files. If from experience the cost of bribing an authorized user to divulge the information to which he has access is less than the cost of penetrating the computer in a malicious manner, then the computer system can be considered secure.

With the preceding criterion for security, the human user -- not the computer system -- is the weakest element in the theft of information and hence is the prime target. However, with the appropriate techniques for protecting computerized information, it should be possible to prevent all users, including computer operators and supervisory system programmers, from having unauthorized access to another user's file, thus limiting the bribed user to divulging only information to which he has authorized access. Thus the use of computerized files will not increase the risk of theft of information beyond the usual problems causes by dishonest people. Ultimately, with appropriate techniques, such as computerized audit trails, incorporated into the computer security system, even the people risk should become less, because an undetected theft would be virtually impossible.

The virtual impossibility of determining a value for the vast amounts of information stored in a computerized file, coupled with the nature of the threat to computer security, can lead to the conclusion that perfect security is a goal that must be achieved for computerized information containing sensitive information. However, because nothing can ever be really perfect, the obvious question arises as to whether computer security in the sense of making the human user the weakest link is adequate enough. This controversial question can only be answered through actual experience.

Levels of Computer Security

Different levels of computer security for information of different "value" is probably an unrealistic approach, in view of the impossibility of determining a "value" of the sensitive information stored in a computerized file and the sophistication of the tools available to the attacker. Hence computer security methods must ultimately afford maximum protection to information that can in any way be considered sensitive, while at the same time making this information readily accessible to authorized users. For the present, maximum security is a goal for the future, and considerations of all the costs of obtaining information through the subversion of people relative to the costs of penetrating the computer system might have to be an adequate approach to computer security.

Cost of Computer Security

Developing new hardware and software for computer security will undoubtedly involve some additional costs to protect against deliberate modifications, disclosures, and destruction of data. However, these costs will probably be more than saved by the elimination of accidental destruction, modification, and disclosure. In effect, an increased reliability and efficiency of the computer system will result.

The passage of legislation protecting the privacy of individuals could mean a ban on storing information about individuals in computerized files if the protection of this stored information were inadequate. This could mean that the efficiencies of using computers for large information processing could be denied to the government and others who have need to use information which has an impact on privacy. It can be claimed that such legislation should be based upon technological feasibility, but it can also be claimed that the potential violation of an individual's privacy is far more important than technological feasibility or government efficiency.

Until an adequate level of computer security can be developed, many installations might require two computers: one operated in an extremely secure environment including a reasonably secure software system and the other operated in a nonsecure environment. Timesharing applications might have to be forbidden for computers containing sensitive information. The machine might have to be run in a dedicated manner for sensitive problems, and this will entail clearing the machine of all past jobs, reloading the operating system, and clearing again when the sensitive job has been run. Thus, without adequate computer security, the cost of many computer installations could be almost doubled by the need for two computers in order to achieve security.

Government and Industry Involvement

The Federal government has many responsibilities to supply many different services to the people. The government must have information about the people and their needs in order to supply these many services in the most efficient and effective manner. Thus, most Federal agencies have amassed files containing information about the people and their needs.

In the past, Federal services were rather simple, and each Federal agency was able to maintain the files containing the information required to support the particular mission of the agency. However, both the demand and the breadth of services have increased greatly within the last decade or so, and both the amount and depth of information in agency files have likewise increased. For example, a Federally-financed housing allowance might be dependent upon such parameters as income, location, and health of recipient. The information needs for a housing allowance might thus involve the files of many Federal agencies. These agencies would thus, depending upon the costs involved, each amass all this information, share this information among themselves, or create a large common centralized information file.

The government's need for information will most certainly continue to increase in the future. As the amount of information increases, the risk of accidental or deliberate violations of the privacy of this information obviously will likewise increase unless some adequate protection measures are introduced. The government, as custodian of considerable amounts of information about both the people and itself, has a strong responsibility to protect adequately all this information and to develop the appropriate procedures and technology to protect both its own information and information about its citizens.

The Federal government is not the only supplier of services to the people -- State and local governments also supply considerable services to the people, and they require information about the people and their needs to supply services in the most efficient and effective manner. Also, the complexity of management of government agencies at the State and local level is ever increasing, so that these non-Federal agencies will be using computers to increase the efficiency and effectiveness of their own internal operations. Thus, State and local governments will become increasingly concerned with the protection of information stored within their own computerized files.

The use of computers and computerized files is essential for the efficient and effective operation of nearly all industrial firms. Many industries require information not only about their own internal operations but also about their customers, and much of this information is stored in computerized files. Thus, private industry is also becoming increasingly concerned about the protection of information stored within its own computerized files.

TECHNOLOGICAL ASPECTS OF COMPUTER SECURITY

Although the purpose of this paper is not to give a thorough review of the technical details of computer security, some technologies of computer security will nevertheless be discussed in order to give a better understanding of the hardware and software aspects of computer security and also to evaluate the prospects for achieving adequate computer security. Although it is readily admitted that adequate computer security for all computer installations is a goal to be achieved, it is nevertheless firmly hoped that a realistic application of computer hardware and software techniques already available will enable this goal to be achieved in a reasonably short time for some computer installations without waiting for lengthy solutions to some of the research aspects of computer security.

Adequate computer security, at a minimum, will require solutions to the following, treated in the next subsections:

- Physical security of the computer installation, including the computer and all files.
- Identification and positive authentication of all users.,
- Secure communications between the computer and any remote terminals.
- Secure supervisory programs to control user access and such other functions as continuous auditing of user access.

Physical Security of the Computer Installation

Computer security includes the development of the appropriate techniques, methods, and procedures for protecting information from accidental or deliberate modification, disclosure, or destruction. The physical security of the computer installation itself must also be considered along with appropriate hardware and software protections for the data stored within the computer.

Although the physical security aspects of a computer installation seem simple and mundane, they nevertheless cannot be ignored. Such careless practices as storing magnetic tapes on an unguarded loading dock prior to shipment is an open invitation to theft of the tapes and the information contained on them. Most electronic devices emit electromagnetic radiation, and computer terminals and devices are no exception. Adequate protection of computers must therefore consider appropriate shielding of electromagnetic emissions. There are a large number of such potential sources of information leaks from a computer installation, and none of them can be neglected.

Computer security is really not much different from conventional security in its physical aspects. Armed guards, barbed wire, locked doors, administrative procedures, and many more safeguards form a collection of techniques that can be applied to reduce risks to an acceptable value.

The protection of the physical security of the computer is an essential portion of the overall security of a computer installation. However, the computer hardware itself does not introduce any unique problems into implementing the appropriate physical-security safeguards for the computer installation, and the amount of information exposed by threats to the physical security of the computer itself can probably be kept quite small. Hence the major thrust in computer security research and development is on those special aspects of computer security which are unique to a computer system. These aspects include primarily: the identification, and authentication by the computer of the identification, of the user at the remote terminal, the communication of information between the remote terminal and the computer, and the computer hardware and software for controlling user access to the information contained within the computer.

User Identification and Authentication

If a physical security fence is built around a computer installation, then security guards can verify that users are authorized to have access to it. When remote terminals are connected to the computer, the physical security fence would have to be extended to include the terminals, which would mean that a human guard would have to be stationed at each terminal to verify that the user is authorized to use the terminal. This could be costly and still would not restrict authorized and authenticated users from accessing the other users' information within the computer. The only solution is for the computer itself to verify the identification of the user.

A user of the computer must identify himself so that the computer can determine the files to which he has access. However, the claimed identification of a user is not sufficient -- the computer, just like a guard at a gate, must authenticate or verify the identification of the user. This authentication can be accomplished only by something the user possesses either physically (such as an identification card or an attribute like a fingerprint) or mentally (such as a password or some fact known only to the user).

The user identification and authentication problem has stimulated considerable interest in the use of the physical attributes of a person for identifying and authenticating a user, such as fingerprints and speech verification. This is an extremely challenging area of research and development, and new techniques are actively being investigated. Computers are for people, and hence these techniques must not be so cumbersome as to make potential users reluctant to use the computer.

The computer must be totally untrusting of all users -- not only *human* users -- and therefore must identify and authenticate even other computers when they seek access through networks. Individual processors in a multiprocessor computer might even be required to identify themselves. The human user will probably require some form of identification and verification from the computer he is using, to be certain that another computer is not masquerading as the legitimate machine for the purpose of obtaining information from the user. The intricacies of identification and authentication can thus become quite involved and complicated.

Because the amount of information transmitted to a remote user will usually be extremely small compared to the amount of information contained within the computer, the loss of information to an unauthorized user might not be so disastrous. The effect of this loss might even be minimized if the authorized user had some way of knowing that his information had been violated. The computer could accomplish this by supplying the user with lists of past access to his files, for comparison with his own records. It could also be programmed to place severe user-specified restrictions upon the type and amount of information transmitted to the remote terminal. Thus, through appropriate procedures, the type and amount of information available to an unauthorized user could be severely restricted, and the probability of detecting an unauthorized access could be increased, thereby increasing the risk of being caught.

Communications Security

The security of the information transmitted from the computer to a remote user is an important aspect of the total security of a computer system. Communications security includes the use of appropriate cryptographic techniques to protect the information communicated between the computer and the remote terminal over networks. This will require cryptographic devices and techniques both at the computer and at the remote terminal, although the computer could be programmed to perform the appropriate cryptographic transformations.

Cryptographic devices are usually rated in the amount of effort someone would require to break down the coding techniques used to encipher the information being transmitted. The sensitivity of the information being transmitted over the communications link between the computer and the terminal will determine the elaborateness of the cryptographic techniques used to protect the information.

The general philosophy of making the theft of information costly relative to the value of the information is indeed applicable to communications security, since the amount of transmitted information is usually small enough for its value to be deterministic. Quite obviously, the passwords or other methods used to authenticate a remote user would have to be highly protected through encryption when transmitted to the computer for other than "one-time" users.

Encryption can also be a very useful technique for protecting a considerable amount of the information stored within the computer. The information stored on tapes and disks could also be encrypted and thus safeguarded against any physical theft of the tape or disk itself. However, to read back this information, the computer must obviously decipher what has been written before in encrypted form. This might be costly in terms of accessibility by the computer to this information. Perhaps the computer itself will have to be designed with dedicated hardware for performing encipherment and decipherment of information, both within the machine itself and in its communications with peripherals.

Computer Hardware and Software for Controlled Access

A very weak link in the overall security of present computer systems is the computer's supervisory program, which includes the appropriate software for protecting the security of the information stored within the computer. Supervisory programs for modern computers can be as large as many hundred thousand computer instructions. The sheer size alone of the supervisory program creates many possibilities for software errors which would defeat any security provisions built into the supervisory system. However, no supervisory system has yet to be designed with adequate protection from a malicious penetrator as an initial primary design requirement.

Unfortunately the present development of secure supervisory programs has become a countermeasure game of almost endless extent, in which each new threat has a procedure to counter it, which then could create a new threat -- ad infinitum. The real challenge to the development of a secure supervisory system is to break this infinite loop. This will occur only when a supervisory system is written with computer security as an initial design requirement and not as an afterthought to be patched in. As a direct result of a philosophy of haphazard patching and repairs for computer security, no supervisory system presently exists which could not be quickly penetrated in a few weeks by a remote user. Most computer installations that handle sensitive information therefore rely upon conventional physical-security fences and perhaps restrict the uses to information storage and retrieval only, with no programming capabilities.

The supervisory system includes appropriate software for protecting the information stored within the computer, and hence adequate computer security in the context used in this paper really means an adequately secure supervisory system.

The supervisory system has access to the passwords and names of the users, along with the identification of the files to which each user has access. This extremely sensitive information must be given maximum protection.

The data stored within the computer system must be protected not only against reading but also against writing and possibly even execution. In this way, some users might be allowed to read a program but not to execute or change it. Bounds for segments of storage can be specified for each user along with an access specification. Such peripheral storage media as disks, drums, and tapes can all be made to appear to the users as an extension of memory by appropriate techniques, and memory bounds can then be applied to this one extremely large virtual memory.

Many supervisory system security features will probably be implemented in software, which is a reasonable procedure until the security design has been finalized. However, as this security software resides in storage, it is itself a target for any security threats. Also, security software will slow down somewhat the data processing speed of the computer. For these reasons, some of the security software should probably be implemented in hardware, with provisions to ensure that any failures of this security hardware are not undetected.

Certification

Conventional security file cabinets and cryptographic devices have specifications in terms of the amount of time and effort required to penetrate the cabinet or cryptogram. A similar type of specification, if required for a computer system, would probably be in terms of the time and degree of effort required by the penetrator to perform a successful entry into the computer system. The problem, of course, is that a file cabinet is a physical device, and only a finite number of mechanical means might be used to force entry into the cabinet. A computer system is an extremely complex affair, and the number of entry points through the operating system, for example, might be infinite or, at best, indeterminate.

Another possible procedure to be used for the certification of a computer system might consist of a team of penetrators attempting to force entry into a computer installation. These penetrators would have a listing of the operating system and a computer at their disposal to help them in their attempts at forced entry. Some forms of financial inducement might be used to stimulate these penetrators to perform more diligently. As a computer-age procedure, certification by attempts at penetration seems very sloppy, and failure to penetrate the system provides no basis for assuming that the system is secure. Unfortunately, many computers users and manufacturers do not accept the inherent weaknesses of their supervisory systems which were not initially designed for security, and as a result, teams of programmers are continuing the wasteful -- but exceptionally easy -- chore of penetrating computer systems.

It would be far easier if computer security systems were written in high-level languages so that these languages could be easily understood and analyzed by other people. In this way, these people could ascertain whether important features were incorporated in the supervisory system and in the computer hardware in order to produce a certain degree of security. However, the development of high-level languages for supervisory systems is a research problem with solutions still in the future. Therefore the only practical solution might be to design the security portion of the operating system as a small program that can be easily understood and verified by other programmers. It seems reasonably obvious that definite answers to the certification problems are not known and will entail a fair amount of careful thought and development before definite procedures can be ascertained.

Future Research

The integration of hardware and software for computer security implies new design procedures and the research and development of new computer design methodologies. These design procedures will themselves be computerized and, in addition to being applicable to computer security, will enable the efficient and inexpensive design of many special-purpose computer systems.

The somewhat pessimistic aspects of computer security hinge on the development of the techniques for ensuring that software and hardware are reliable and verifiable. In other words, both the hardware and software must be free of errors and must do exactly what they are supposed to do. An undetected and unpredictable bug in the hardware or software could easily do irreparable damage to an otherwise secure computer.

It is difficult enough to determine if a computer program is free from errors and bugs, but it is even more difficult to ascertain that the program does exactly and only what it is specified to do. These problems in software and hardware reliability and verifiability are further complicated by the sheer size of the very large hardware configurations and supervisory systems that are so prevalent today. Somehow, high-level programming languages must be developed so that supervisory systems can be small enough to be comprehended by a single human mind. Research in automatic programming is thus particularly applicable to computer security.

Administrative Aspects of Computer Security

A fair amount of technical competence will be required of the people who are responsible for designing the computer security system for a particular computer and supervisory system. It is critical that these people be technically competent in computer programming and knowledgeable of computer hardware.

For a computer system to be adequately secure, the system's programmers and computer operators must be extremely trustworthy, which means that their risks to security must be minimized by background investigations and by other personnel security techniques. The system's programmers and computer operators will have to be authorized to have access to the highest level of sensitive information contained within the computer.

Ultimately, most computerized security systems must rely upon a security officer or security administrator to watch over the system. Quite obviously these security officers and administrators for computer systems will have to be a new breed of person, since most present security officers and administrators feel that the present complexity of a computer in and of itself affords protection to the information stored within the computer, which is not so. This present lack of knowledge and understanding of computers will have to be corrected in this new breed of security officer who will require knowledge of computers and the computer security system to be able to plan and develop realistic administrative procedures for determining user access to the computer and to the sensitive information.

LEGISLATIVE AND POLICY ASPECTS OF COMPUTER SECURITY AND PRIVACY

There is some feeling that technical solutions alone will never be adequate for computer security because no computerized security system will ever be completely foolproof. Therefore, appropriate legislation might be required to create an atmosphere in which the "threat of being caught" will be the ultimate deterrent. However, these laws should be technically feasible in terms of what the science and technology of computer security can actually deliver. Conversely, new developments in the level of protection which can be granted by computer security might result in a strengthening of these laws.

In the same way that agencies are now required to consider environmental issues for all of their programs, agencies might also be required to consider the privacy issues involved in their use of computers and data banks -- in effect, a privacy impact statement. The process of accumulation of information about individuals might be prohibited unless the strictest security requirements can be and are met by the computer installation in question. Stiff penalties might be required to prevent some systems programmer, computer operator, or computer user from violating an otherwise secure system.

Although stiff penalties can provide a reasonable degree of deterrence in preventing the deliberate theft, modification, or destruction of information stored within a computer, an adequate computer security system with an elaborate trail of audits will be the best deterrent. Cooperation between legislators and computer technologists is the only way to produce legislation which is both legally effective and technologically reasonable.

Unfortunately, simply writing laws to forbid the theft of computerized information does not solve the extremely difficult policy questions of what information should be denied to whom. A determination of which information is to be considered sensitive, and hence to be protected when stored in computer systems, is a policy issue involving such considerations as national security and social concerns about the privacy of individuals.

For example, should the Federal Bureau of Investigation be allowed to examine welfare information about individual citizens under the justification that apprehending criminals is in the greater good of all the people? Or would this be a far greater harm in terms of the injuries to the privacy of a few people?

To a considerable extent, the "privacy" issue really does not concern computers, data banks, and technology, but rather reflects the concern of many people about the non-uniform policies of government agencies and other institutions for the disclosure of information about individuals. Although the technology of computer security can protect information from malicious threats, it cannot protect information which is knowingly exchanged between different government agencies and other institutions, each of which has different information handling and disclosure policies. Similarly, computer security technology cannot prevent authorized access and unauthorized disclosure of private information.

The relevant technological conclusion is that computer technology will be able to create the appropriate computer security to protect the privacy of individuals. Whether this technology is used is a nontechnical policy decision. These policy aspects will probably have to be determined by the individual agencies and institutions themselves, with policy guidance from appropriate higher-level authorities.

CONCLUDING REMARKS

Information is essential for the effective and efficient operation of government and industry and the supplying of services to the people. Digital computers are requisite for effective and efficient information handling and processing, and the government and industry must therefore continue to make use of computers.

However, the use of computers for the effective and efficient handling and processing of information is only a portion of the advantages to be obtained from computer technology. For example, only through the use of computer technology will it be possible for people to know for themselves the information stored about them in computerized data files. If this information is incorrect, then through the use of computer technology the people will have an opportunity to make corrections of this information, thereby increasing its credibility and value. Individuals could themselves specify who would have access to specific information.

It is even possible to envision computer systems which will enable one agency to perform statistical analyses of another agency's files without in any way risking disclosure of the individual information contained in the files. All of this will result in increased flow of information between agencies which will, hopefully, result in an increased efficiency of government and industry and improved services to the people. None of this would be possible using conventional file cabinets to store information. Unless adequate computer security is obtained, the application of computer technology will probably not achieve its fullest potential.

Adequate computer security has not yet been achieved, but the research and development that is presently underway to design hardware and software for computer security would imply that unauthorized access to the information stored within a computer system will ultimately become virtually impossible. Not only will agencies and individuals be prevented from obtaining unauthorized access to computerized data bases, but the programmers who wrote the supervisory system and the designers of the hardware will also be prevented from subjugating the computer and obtaining unauthorized information from the files contained within the computer.

SUGGESTED FURTHER READING

Privacy

A.R.Miller, *The Assault on Privacy,* Ann Arbor: The University of Michigan Press (1971).

J.M.Rosenberg, *The Death of Privacy,* New York: Random House (1969).

M.Warner and M.Stone, *The Data Bank Society,* London: George Allen & Unwin Ltd. (1970).

A.F.Westin, *Privacy and Freedom,* New York: Atheneum (1970).

A.F. Westin and M.A. Baker, *Databanks in a Free Society,* New York: Quadrangle Books, Inc. (1972).

Records, Computers, and the Right of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, US Dept. of Health, Education & Welfare (1973 July).

Computer Security

J.P.Anderson, "Information Security in a Multi-User Computer Environment", *Advances in Computers,* **12,** New York: Academic Press, Inc. (1972).

J.P.Anderson, "Computer Security Technology Planning Study", prepared for Air Force Systems Command, USAF, ESD-TR-73-51, Vol. 1 (1972 Oct).

L.J.Hoffman, "Computers and Privacy: A Survey", *Comput. Surveys,* **1,** No. 2, 85-103, (1969 June).

W.H.Ware (Editor), "Security Controls for Computer Systems", The Rand Corp., Santa Monica, CA, R-609 (1970 Feb) CONFIDENTIAL.

Bibliographies

R.E.Anderson and E.Fagerlund, "Privacy and the Computer: An Annotated Bibliography", *Computing Reviews* **13,** No. 11, 551-559, (1972 Nov).

J.G.Bergart, M.Denicoff and D.K.Hsiao, "An Annotated and Cross-Referenced Bibliography on Computer Security and Access Control in Computer Systems", The Ohio State University, Columbus, OH, OSU-CISRC-TR-72-12 (1972 Nov).