Chapter 8
The Security of Computer Systems

Contents

Chapter 8
The Security of Computer Systems

Concern and Need

The security of computer systems, particularly those operated by the Federal Government, has increasingly concerned Congress. Hearings have been held, studies have been published by the General Accounting Office, and legislation has been intraduced, [1] all addressing the problem of meeting threats to Federal data installations.

Security concerns have also appeared in congressional reaction to proposals for new advanced information systems by Federal agencies, such as the proposed Social Security system, the Tax Accounting System of the Internal Revenue Service, and the upgrading of the National Crime Information Center (NCIC) system of the Federal Bureau of Investigation. All of these proposals have been scrutinized carefully by congressional committees, with particular emphasis on the security of the systems.

Similar concerns have also been expressed by the executive branch. Presidential Directive 24, published in February 1979, established policy for the security of Federal communications and assigned responsibility for the protection of nonmilitary but sensitive Government communications. This directive was motivated by a concern for national security, that is, the potential value of intercepted communications to an enemy.

In a 1978 memorandum,[2] the Office of Management and Budget directed all Federal agencies to pay attention to the security of their data processing operations. The memorandum required the agencies to conduct risk analyses of the threats and vulnerabilities of their systems and to develop appropriate security plans.

The National Bureau of Standards, under authorization by the Brooks Act,[3] is continuing to develop guidelines and standards in all areas of computer security for use by Federal agencies. The first standard to emerge from this effort is the Data Encryption* Standard for protecting data communications. Its adoption may present difficulties because of the rapidly changing technology and the extraordinarily wide range of types and uses of Federal information systems that would have to be covered.

In the domestic sector, the security problem is growing in importance due to several trends:

- The rapidly increasing quantity of computerized data stored and transmitted over communication networks.
- The increasing value of the data, both as a marketable commodity and as representative of value, for example, as in an electronic funds transfer or an automated stock exchange transaction.
- As has been pointed out, an increasing quantity of personal information is being collected, stored, and transmitted. The security needs of electronic mail or of the NCIC system are motivated, in part, by privacy concerns.

[1] See S. 240 (and H.R. 6192), 96th Cong., "Federal Computer Systems Protection Act of 1979, " to prohibit the use, for fraudulent or other illegal purposes, of any computer owned or operated in interstate commerce or by the Federal Government or any financial institution.

[2] Office of Management and Budget; circular A-71, "Responsibilities for the Administration and Management of Automatic Data Processing Activities, " transmittal memorandum No. 1, "Security of Federal Automated Information Systems, " 1978.

[3] Public Law 89-306.

*Encryption is the coding of a message so it is only understandable to a receiver who knows the secret decoding procedure.

- An organization's operations are becoming more dependent on the reliable, secure functioning of the supporting computer system. A computer failure can close down all sales registers in a department store, the air traffic control system, or all the teller stations in a bank.

The Technology of Security

There is a blend of optimism and pessimism in the computer technology community about the future of computer security problems. On the one side, experts correctly point out that the technology of securing computer systems is improving steadily (see ch. 13). They also maintain that computerized systems, even if not perfectly secure, are often far more secure than the manual systems they replaced.

On the other side two main arguments are advanced. First, since security has not been historically a high-priority goal in the design of information systems, the existence of security technology does not necessarily guarantee its proper application. Security hardware and software are often added as an afterthought rather than integrated into the system from the beginning. Most designers have not been trained to build security into the systems they assemble, since security features can increase the initial cost and operating overhead, and may be burdensome to manage.

The second objection is that advances in the technology of protection may not be adequate to deal with the complex systems now being built. In particular, the present trend towards linking computers into networks that use new communication services, which vastly increases the overall complexity of the resulting systems, presents new and difficult challenges to the designer attempting to build a secure system.

Threats and Targets

Analysts view the security problem in several parts. *Threats* are the possible actions of outside forces that may compromise a system. *Targets* are those points within the system against which an attack may be mounted. Assets are the resources of the system (information, money, goods) that may be lost.

Because of the trends cited, threats against computer systems appear to be on the increase. The transfer of funds electronically is only one case in which the information processed is assuming a significant tangible value. Electronic mail and future systems for trading commodities and securities will also tempt criminals. As the society grows more information oriented, the risk of theft will increase along with the potential payoff for its success. In response, a number of computer scientists have focused their attention on computer security.[4,5]

Computer crime analysts note a number of types of threats:

- theft;
- sabotage;
- data alteration (i.e., in a credit file);
- blackmail;
- extortion;
- corporate espionage;
- system failure;
- service interruption;

---

[4]Lance J. Hoffman, *Modern Methods for Computer Security and Privacy* (Englewood Cliffs, N. J.: Prentice Hall, 1977).

[5]Dorm B. Parker and Susan N. Nycum, *Computer Abuse and Con trol Study* (Menlo Park, Calif.: SRI International, March 1979).

- natural hazards (e. g., volcanic eruption, flood); and
- unauthorized disclosure.

Computer literacy is growing and with it a proportionate number of people sufficiently knowledgeable to compromise a computer system. In addition, access to low-cost personal computing systems may provide such criminals with more sophisticated tools. At least one such attack has already been made on the telephone system with the aid of a small in-home computer system. Recently, newspapers reported the alleged use of a small computer by high school students to break into the data banks of several Canadian corporations.[6]

Certain social conditions may increase the threats to computer-based systems. A period of stagnation coupled with high inflation could create economic pressures that might lead to an increase in white-collar insider crime. In addition, some social and political scientists see the possibility of an increase in domestic terrorist activit y.[7] Foreign experience has shown that such activity is often directed against computer and communication systems, which the perpetrators assume, often rightly, to be at the heart of organizational operations.

Forewarnings such as these, although based on expert opinion, are at best speculative. Nevertheless, security plans must be developed against potentialities, not just certainties. Thus, the possibility that an increase in certain social pressures could lead to economic and sabotage threats against the coming decade's complex information systems is a significant factor in any security analysis.

While threats to information systems and the potential losses from attacks are clearly increasing, the vulnerability of systems to successful attack is changing in character. In some cases it is improving, in others worsening.

The vulnerability of the system software to intrusion should decrease as operating systems are designed with security as a principal goal. They can be expected to be more immune to compromise than those currently available. Data communication will be better protected, both by its changing basic technology and by the incorporation of cryptographic protection. The language used to query the data base will be designed to more easily isolate users from data that they are not authorized to use. Thus, in the future virtually every component of an information system will have better security technology designed into it.

New vulnerability problems, however, will arise at the level of the overall system. As a system becomes larger and more complex, so do the managerial and technical problems of securing it at a system level. The trend toward linking a large number of computer systems together to be used for diverse applications by many persons, scattered geographically, poses system design and management problems that are orders of magnitude larger than those faced in the design of previous generations of information systems. It will be difficult to assess the vulnerability of such complicated systems to accidental or deliberate misuse or failure. Detecting that an untoward incident has occurred would be even more difficult in such systems because of the high volume of work that flows through them and the lack in many systems of full transaction logs.

Although the individual communication links may be more secure (say through encryption), data communication adds its own problems when integrated into information systems. A network of computers that links together individual computer systems over telecommunication lines has numerous points that need to be protected in an environment where failure or penetration at any point compromises the entire system. In addition, such systems are deliberately designed to distribute access, to make it easier

[6] "The Great Dalton School Computer Tie-In Mystery," *New York Times*, July 7, 1980, p. 2, col. 1.

[7] Donn B. Parker, "The Potential Effects of Electronic Funds Transfer on National Security," *Proceedings of the Fifth International Conference on Computer Communication*, October 1980, pp. 470-476.

for users to get at the system, and to decentralize administrative control of the data processing. Consequently, security management—setting up and overseeing administrative and personnel controls—becomes more difficult, both because of the increased number of persons with direct access to the system and because of the geographical dispersion of the organizations involved.

Problems of overlapping or inadequate authority can complicate attempts to control a system's security. This would be the case, for example, with a Federal system that links with State systems, because different nodes in the system would have different rules, practices, and assignments for system security. Yet to be most effective, controls over data access, usage, and security must be applied uniformly over an entire system. A private industry information system that linked together data processing nodes under different authorities would face similar problems.

The problems of controlling access in a widely distributed data network are exemplified by NCIC. (They are discussed in detail in OTA's NCIC assessment, in progress.)

Future Security Issues

Among the several difficult issues involving computer security that are likely to confront Congress over the next decade, the following appear to be the most significant.

Protection of Federal Systems

Federal information systems control the disbursement of an enormous amount of money. The Social Security system itself disburses over $1.5 billion per week. Other Federal systems contain information that could be used directly or indirectly to make profitable financial decisions, e.g., information concerning Federal monetary policy, commodity markets, energy resource estimates, and the like. Still others contain sensitive information relating to personal privacy or national security. All would be highly attractive to theft, manipulation, or eavesdropping.

There are many potential victims of security failures. Taxpayers would suffer the losses from a fraudulent drain on the Federal Treasury. Other types of attacks, for example on social service systems, could create severe hardship for individuals dependent on those programs. In an extreme case, the national security could be threatened, not only by attacks on military and diplomatic computers but also by assaults on such major domestic activities as the air traffic control system or the computer-controlled national electric power distribution grid, whose disruption could create significant social turmoil. Electronic mail service or an electronic funds transfer network would be similarly vulnerable.

Theft, eavesdropping, and sabotage are not the only threats to Federal computer systems that Congress will need to consider. A more subtle threat is a system's potential diversion by the bureaucracy from its intended use. This issue is raised in OTA's NCIC assessment. Expressing similar concern in a different area, Congress has imposed criminal sanctions for bureaucratic violations of the Privacy Act of 1974.[8]

The technology currently available is not very useful for securing a system against this type of bureaucratic abuse, although the researchers in the field of electronic data processing auditing are looking at related problems. Many abuses do not involve violations of the computational procedures within the computer system, but rather represent misuse of the data once it is out of the system. Thus, the most effective controls

[8] Public Law 93-579.

against bureaucratic abuse for now will likely be in the areas of policy, personnel, and management, rather than technical. Strong criminal sanctions for misusing a system may also have a deterrent effect.

As the Government continues to automate, problems of bureaucratic accountability and the responsibility for oversight will confront Congress with the need to better understand and more closely monitor the use of large Federal information systems.

Protection of Vital Domestic Information Systems

There are a number of national interests that will cause Congress to become concerned about the security of major nonfederal national information systems.

Regulations regarding the flow of personal information are proliferating in nations around the world. To date, most laws concern the transfer of personal information and stem from national privacy laws. However, there seems to be a distinct trend toward the extension of these laws to organizations, which are designated as "legal persons "[8] and thus included under privacy laws designed to protect personal data. There is also a growing concern expressed by some nations, particularly those in the Third World, that information originating within their borders is a national resource over which they want to maintain control. [10]

These trends may create additional fears about the security of networked systems that communicate beyond their boundaries. The relatively mild wording about security in current privacy legislation could reappear in much more stringent form in new legislation.

There is also a Federal responsibility for certain information systems that although privately operated, are fundamental to social well-being. The security and reliability of automated systems for nationwide bank check clearing, for a national stock exchange, and for computer-based commodity trading, for example, would all be under the purview of Congress. The vulnerability of such systems is of governmental concern because of the harm that a major system failure could cause to the Nation's economy and to its citizens.

The continuing evaluation of the privacy issue will undoubtedly lead to more stringent security provisions consistent with the evolution toward more communication-based computer systems.

If there is in fact a growing commercial market in personal data, an illicit traffic in stolen information could develop, thus increasing the threat of piracy of personal data from these systems. This would call for tougher and more specific standards for their security.

The Federal Government, due to its traditional concern for the protection of military and diplomatic communications, has a high degree of expertise in the field of data security. A good deal of this expertise is either classified or in the hands of highly sensitive organizations such as the National Security Agency. The appropriate role of the Federal Government has not been defined in transferring this knowledge, for supporting computer security in both the public and private sectors, for setting standards, and for certifying security technology.

The lack of such policy definition is visible in the current debate over Government control of cryptographic technology. *l In this debate, the needs of the private sector for increased communication security, and hence for the existence of a civilian commercial cryptographic capability, are set against the

[8]H. P. Gassman, "Privacy Implications of Transborder Data Flows: Outlook for the 1980s," *Computers and Privacy in the Next Decade*, L. J. Hoffman, (ed.) (New York: Academic Press, 1980).

[10]American Federation of Information Processing Societies, Panel on Transborder Data Flow, *Transborder Data Flows*, Washington, D.C., 1979.

[11]David Kahn, "Cryptography Goes Public," *Foreign Affairs*, vol. 58, No. 1, fall 1979, pp. 141-159.

perceptions of the defense community that such development threatens national security concerns by putting sensitive information in the public domain. " A related issue is the desire in the academic community for the freedom to conduct research on the mathematics underlying cryptography.

[124]" Study Group Agrees to Voluntary Restraints, " *Science*, vol. 210, Oct. 31,1980, pp. 511-,512 and " MIT Committee Seeks Cryptography Policy, " *Science*, vol. 211, Mar. 18, 1981, pp. 1, 139-1,140.