Chapter 3

The Vulnerabilities of Electronic Information Systems

CONTENTS

	Page
Findings	23
Introduction	23
Vulnerabilities of Communications Systems	24
Background	24
Spectrum of Adversaries' Resource Requirements	27
Networks	28
Transmission Systems	29
Other System Components	37
Commercial Availability of Interception Equipment	3$
Vulnerabilities of Computer Systems	39
Background	39
Large-Scale Computers	39
Microcomputers	41
Software	42
The Extent of Computer Misuse	44
Typical Vulnerabilities of information Systems	44

Boxes

Box	Page
A. Examples of Historical Concerns for Misuses of Telecommunications Systems	25

Figures

Figure No.	Page
l. Spectrum of Adversaries' Resource Requirements v. Technologies	28
Z. The Communications Network	30
3. Example of Antenna Directivity Pattern	32
4. Examples of Commercial Equipment for Interception of Microwave Radio Signals	33
5.Typical Fiber Optic System...	35
6. Mainframe Computers in Federal Agencies	40
7. Computer Terminals in Federal Agencies	41
8. Trends in Component Density, Silicon Production, and Gallium Arsenide Announcements, 1960 to 1990	42
9. Microcomputers in Federal Agencies	43
10. Typical Vulnerabilities of Computer Systems	45
11. Technical Safeguards for Computer Systems	47

Tables

Table No.	Page
l. Bell System Circuit Miles of Carrier Systems Using Different Transmission Media	29
2. Telephone Company Fiber Applications	34
3. Sales of Large-Scale Host Computers in the United States	40
4. Sales of Personal Computers in the United States...	42

Chapter 3

The Vulnerabilities of Electronic Information Systems

FINDINGS

- Today's public communication network is, for the most part, at least as easy to exploit as at any time in the history of telecommunications. The design of the public switched network is such that some parts of it are vulnerable to relatively easy exploitation (wiretaps on copper cable, over-the-air interception), while others (e.g., fiber optic cable) present greater inherent barriers to exploitation.
- There are, and will likely remain, opportunities for casual, generally untargeted eavesdropping of communications. However, targeted and consistently successful unauthorized access requires greater resources. For systems with sophisticated safeguards, the resource requirements may frustrate even the efforts of national intelligence agencies. However, adversaries with sufficient resources can eventually defeat all barriers except, perhaps, those based on high-quality encryption.
- Users of communications systems face a spectrum of vulnerabilities ranging from those that can be exploited by unsophisticated, low-budget adversaries to those that can be exploited only by adversaries with exceptionally large resources.
- Technological advances may increase the capabilities of adversaries to misuse computer and communications systems, but these same advances can also be used to enhance security.
- Increases in computing power and decentralization of functions have increased exposure to some threats. Two types are important: abuse by intruders who are not authorized to use or access the system, and misuse by authorized users. For many organizations, the latter problem is of most concern.

INTRODUCTION

Unauthorized disclosure, alteration, or destruction of information in computer and communications systems can result from technical failure, human error, or penetration. While each of these is important to users, this chapter focuses on malicious or deliberate unauthorized access and alteration, principally because it is in these areas that the impact of Federal policies is greatest.

Widely different levels of time, money, and technical sophistication are needed to gain unauthorized access to different parts of communications and computer networks. Some forms of covert access—placing wiretaps, intercepting mobile telephone calls, hacking into poorly safeguarded computers—require few resources. Others, such as targeted and consistently successful unauthorized access, require greater resources because of the inherent barriers posed by the complex designs of these systems. For systems with sophisticated safeguards, the resource requirements may frustrate even the efforts of national intelligence agencies.

Today's communications networks make use of diverse technology. This diversity is accompanied by an uneven ease of unauthorized access to different parts of the system. Although security has not been a consideration in network design, today's systems provide some inherent barriers to easy exploitation. However, adversaries with sufficient resources can eventually defeat all barriers, except perhaps high-quality encryption.1 Information in computers also has been vulnerable to malicious disclosure or alteration by various methods of penetration, including misuse by both authorized and unauthorized users. However, significant advances are being made in the technology available for safeguarding computer and communications systems, as discussed in chapter 4.

Many users of communications and computer systems remain unaware or unconvinced of significant threats due to such vulnerabilities. Most users are not now adding safeguards, despite the growing volume and value of information being stored in or transmitted across these systems.

Computer and communications systems are becoming increasingly closely intertwined. Consequently, information security is affected by the operation of all segments of these systems. Communication networks pose one set of vulnerabilities to misuse that centers around unauthorized disclosure of information and to modification of data. When computers are linked by communications networks and are remotely accessible, the potential for misuse increases.

This chapter focuses primarily on the vulnerabilities to misuse of communications systems and methods to safeguard against them. It is intended to raise awareness and understanding of some of the technical vulnerabilities of these systems without providing a cookbook for prospective exploiters. [2] Because communications and computer designs and applications vary widely, their vulnerabilities are described in general ways in the sections that follow.

[1] For the purposes of this report, high-quality encryption techniques, for which there are no known and significant weaknesses or deciphering shortcuts, are considered to be fully secure, in spite of the fact that trial-and-error attacks will yield the unenciphered text (plaintext) with a sufficient number of trials.

[2] Although not the subject of this report, it should be noted that simpler and often less expensive ways than electronic eavesdropping can be used to gain access to sensitive information; i.e., by bribing employees or by using spies. Thus, users considering adopting electronic security measures must weigh all sources of potential losses, including those from human and other errors, as well as from dishonest employees.

VULNERABILITIES OF COMMUNICATIONS SYSTEMS

Background

The developed world has become increasingly dependent on communications systems to operate businesses and governments at all levels. This can be seen in the revenue growth of communications services. The operating revenues from the domestic services of common carriers, for example, grew from $8.4 billion in 1960 to $166.5 billion in 1985. Similarly, revenues for domestic satellite services rose from near zero in 1975 to $17 billion in 1985. And Intelsat's revenues from international services went from near zero to $475 million in the past two decades.

The growth in revenues reflects the fact that communications networks have become vital for many purposes, ranging from making interbank and government fund transfers to running national electric power grids and the world's airlines. There is every indication that this dependence will increase with continued advances and new applications. Both the volume of information communicated and its importance will continue to grow.

There have been occasional concerns about the vulnerability of telecommunications systems to misuse. Illustrations of some historical concerns and examples of misuse during

the past century are shown in box A. Although today's systems are likewise vulnerable to misuse, commercial demand for improved security (e.g., message confidentiality and integrity) has been slow to materialize. Nevertheless, message authentication and digital signature capabilities are becoming important for a number of industries (see ch. 5).

Little has been done to improve the security of public communications systems themselves. Generally, commercial systems have been designed for efficiency and reliability rather than security. Also, their inherent barriers to misuse adequately serve most users' needs for confidentiality. Where additional safeguards are deemed necessary, "add-on" measures are taken either by the user directly (adding encryption or message authentication capabilities), through the special service options offered by some communications carriers (see chs. 4 and 5), or by a combination of administrative procedures and the use of a protected private communications network.

The regulatory climate has also influenced the confidentiality of systems. The communications industry now faces an increasingly deregulated environment created, in part, by the divestiture of the American Telephone &

Box A.—Examples of Historical Concerns for Misuses of Telecommunications Systems

- In 1845, only one year after Samuel F. B. Morse's famous telegraph message "What hath God wrought, " a commercial encryption, or encipherment, code was published as a means of ensuring secrecy. [1]
- The first voice scrambler patent application was dated within 5 years of the first demonstration of the telephone in 1881.
- During the Civil War, "the first concerted efforts at codebreaking and communications system penetration, or telegraph 1ine tapping were undertaken. "[2]
- Soon after radio communications came into use in 1895, they were used for intercepting others' messages, particularly before and during World War I.[3] In the 1920s, the British surreptitiously eavesdropped on international cable traffic.[4]
- The diversion of an undertaker's business by an eavesdropping switchboard operator resulted in a patent grant for design of the first automatic switch in 1891, eventually eliminating the need for switchboard operators. [5]
- During the 1920s, pervasive Government and criminal use of telephone wiretaps triggered congressional hearings and antiwiretap legislation.
- Interception of telecommunications signals played a key role in the course of World War 11. It continues to be a source of foreign intelligence gathering by major governments.[6]
- In recent years, there has been concern about the ease of misuse of a variety of telecommunications signals, ranging from the pirating and even malicious jamming of subscription television signals transmitted over satellite communications systems to the ease of interception of cellular radio and mobile radiotelephone signals.[7]

[1] David Kahn, *The Codebreakers: The Story of Secret Writing* (New York, NY: MacMillan, 1967), p. 189.

[2] Supplementary Reports on I ntelligence Activities, Book V 1, Final Report of the Select Committee to Study Government Operations with respect to Intelligence Activities, U. S. Senate, Apr. 23, 1976, p. 51.

[3] Kahn, op. cit., pp. 298-299.

[4] James Bamford, *7'he Puzzle Palace* (New York, NY: Penguin Books, 1983), pp. 29-30.

[5] John Brooks, *Telephone: The First Hundred Years* (New York, NY: Harper & Row, 1976).

[6] Kahn, op. cit.; Bamford, op. cit.; Peter Wright, *Spy Catcher (New* York, NY: Viking Penguin, Inc., 1987); also see Glen Zorpette (cd,), "Breaking the Enemy's Code, " *IEEE Spectrum*, September 1977, pp. 47-51.

[7] "HBO Piracy Incident Stuns other Satellite Users. " *New York Times*, Apr 29, 1986, p. Cl 7; "Look! Up in the Sky!" *Washington* Post, Apr. 29, 1986, p. ('1; "Mystery Broadcast overpowers HBO." The *INSTITUTE*, vol. 10, No. 10; October 1986, p, 1; "Uplinks and HighJinks: Satellites Are the Hackers Next Frontier, " *Newsweek*, Sept. 29, 1986, pp. .56-57,

Telegraph Co. (AT&T) in January 1984. As a result, cost competitiveness has become an important consideration for communications carriers. It discourages them from providing cost-incurring safeguards for which there is no significant demand. A 1980 survey found that, with few exceptions, the Nation's 10 largest common-carrier systems were not designed for securing messages against interception. On the other hand, at least one carrier did offer an add-on encryption service.[3] A 1986 OTA review of six carrier systems indicates that a combination of protective services are becoming available, including encrypting radio signals or routing selected calls over cable transmission facilities.[4]

Technology plays an important but uneven role in the security of communications systems. The rapid proliferation of ground-based or terrestrial microwave radio since the 1940s and satellite communications since the 1960s have made interception easier by making signals available over wide geographic areas. Other technical designs have also made interception easier. Private lines (dedicated channels) and cordless telephones, for example, can be intercepted because of the former's fixed position in the electromagnetic spectrum and the latter's complete dependence on radio waves.[5] Telephone lines can also be tapped relatively easily from wire closets on a user's premises.[6]

Local area networks (LANs), which already have wide use in the United States and abroad for linking computer-based systems, represent another area of information technology in which security has received little attention. The same technologies that make possible continued improvements in computer and communications systems can also provide the means for sorting rapidly through a multitude of signals in search of specific telephone numbers, spoken words, or even voices.[7]

At the same time, technology and engineering can complicate the interceptor's work. Fiber optics, which is rapidly being installed in the United States to carry telephone and other communications,[8] requires far more sophistication for successful interception because of the physical medium that carries the message. However, most customers will continue to have copper wires linking their offices and residences with the local telephone company's office for the long term.

AT&T's modern electronic switching network, on the other hand, encrypts signaling information (the numbers of the called and calling parties) prior to transmission, thus denying potential interceptors the opportunity to target specific users' messages. Many other engineering design features, such as signal compression, spread-spectrum techniques, channel demand assignment techniques, and packet switching also complicate any interceptor's work. They do so typically as a byproduct of other objectives. And, within the next few years, as end-to-end digital networks become more commonplace, encryption services are likely to become available if demand is adequate. Of course, adversaries with significant

[3] U S. Department of Commerce, National Telecommunications and Information Administration, "Identification of Events Impacting Future Carrier System Protections Against Vulnerabilities to Passive Interception, 1980.

[4] Information Security, Inc., "Vulnerabilities of Public Telecommunications Systems, " OTA contract report, 1986.

[5] For a description of the vulnerabilities of commercial telecommunications systems to unauthorized use, see the M ITRE Corp., *Study of Vulnerability of Electronic Communication Systems to Electronic Interception,* vols. 1 and 2, January 1977; and the MITRE Corp., *Selected Examples of Possible Approaches to Electronic Communication Interception Operations*, January 1977. Also, Ross Engineering Associates, "Telephone Taps, " OTA contract report, November 1986.

[6] Technical course material from a seminar on communication and information security, conducted regularly by Ross Engineering Associates, Adamstown, MD, and other firms. For additional information on wiretaps, surveillance, and related topics, see: "Electronic Eavesdropping Techniques and Equipment, " Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice, republished by Ross Engineering Associates. Also, Robert L. Barnard, *Intrusion Detection Systems: Principles of Operation and Application* (Stoneham, MA: Butterworth Publishers, 1981).

[7] Whitfield Diffie, "Communications Security and National Security: Business, Technology, and Politics, " *Proceedings of the National Communications Forum,* Chicago, IL, 1986, vol. 40, Book 2, pp. 733-751.

[8] Bellcore, "Evolving Technologies: Impact on Information Security, " OTA contract report, Apr. 18, 1986. Also, see U.S. Congress, Office of Technology Assessment, *Information Technology R&D: Critical Trends and Issues, Case Study 2: Fiber Optic Communications* (Springfield, VA: NTIS #PB 85-245660/AS, February 1985), pp. 67-75.

resources, such as a national intelligence organization, can be expected to readily surmount most of these obstacles.[9]

A number of recent developments may also be making it more difficult to intercept, alter, or misuse signals. These include the advent of commercial encryption services and products, the emergence of new technical standards for safeguarding communicated and stored messages, recent Federal Government policies that influence the safeguarding of sensitive information, and congressional legislation concerning unauthorized access to information in some systems (see chs. 4 through 6).

Still another barrier exists to the misuse of data obtained from passively monitoring or intercepting automated information systems—the problem of obtaining unambiguously the information of direct interest. This is readily illustrated with an example of data in the form of passively intercepted communications signals. Even if an adversary is reasonably assured that the intercepted signals contain useful data among them, the adversary must select from what may be a wealth of transmitted data in the hope of finding the target information in a timely, complete, and understandable context. Although these barriers are not likely to prove overwhelming to a determined, sophisticated adversary, they do not exist for an adversary who has the cooperation of a knowledgeable inside employee with the ability to select exactly the information of direct interest and with a full understanding of its context and limitations.

Spectrum of Adversaries' Resource Requirements

Telecommunication systems are vulnerable to unauthorized access in many ways, but the ease of such access varies widely depending on the resources available to potential adversaries. Targeted, unauthorized access to a specific user's communications over the public switched network, with a few exceptions, considerably increases the need for technical expertise, sophisticated equipment, and money. The complexity of these systems can prevent unsophisticated adversaries who lack the necessary resources from gaining access to information, but would not stop those who have adequate resources from readily surmounting the barriers.

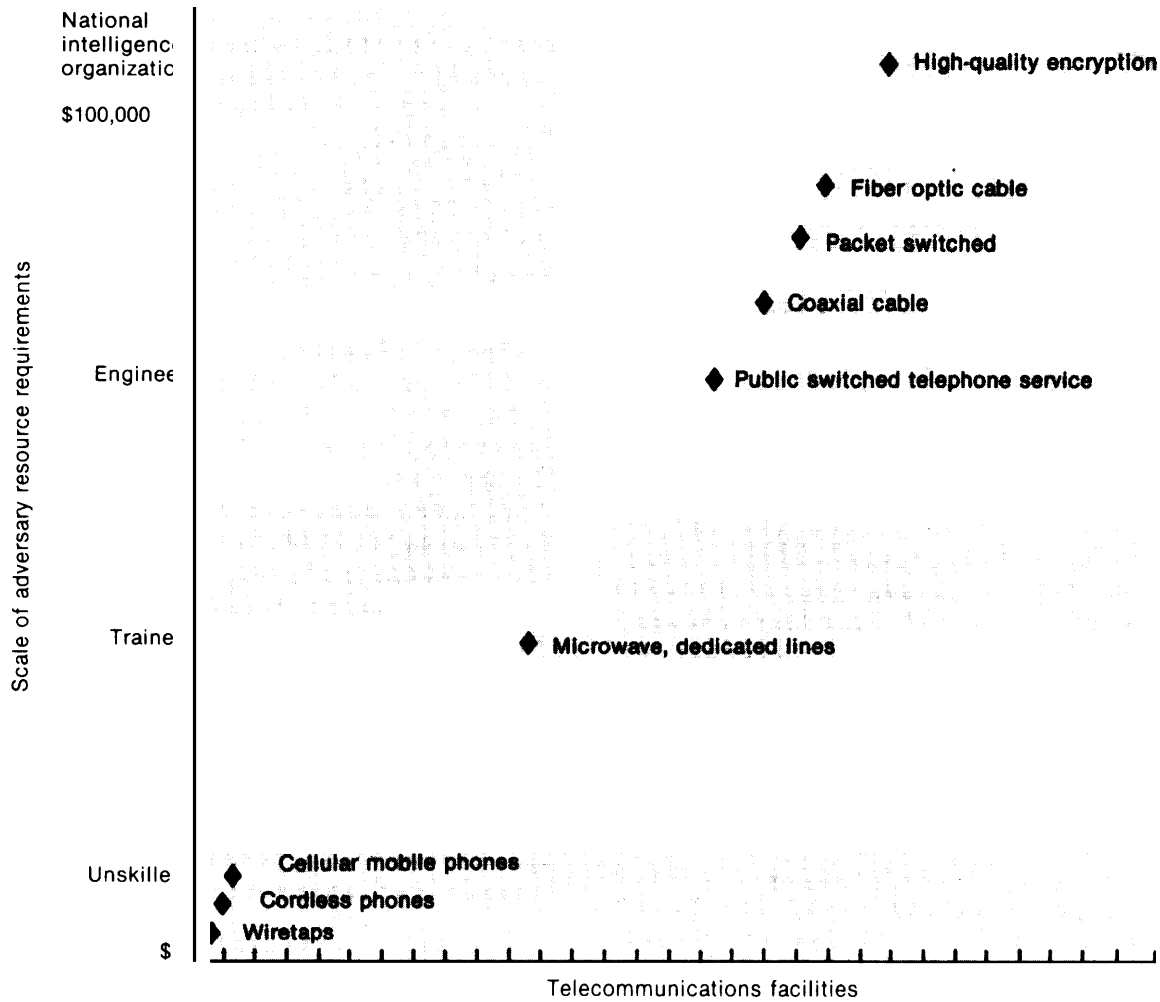
Figure 1 illustrates the spectrum of vulnerabilities and adversaries' resource requirements. On one extreme are readily exploitable *services* (cordless telephones) and facilities (copper wire in local loops and wire closets) that require very limited resources for successful, targeted exploitation. Some cordless telephone conversations can be monitored using ordinary FM radios. Cellular radiotelephone conversations can be monitored using tunable ultra high frequency (UHF) television receivers. Further, wiretapping equipment can be purchased for as little as $12. At the other end of the spectrum are applications and facilities, such as fiber optic communications and technologies, particularly those using high-quality encryption and other safeguards (see ch. 4), that make unauthorized access much more difficult.

On the other hand, technology may simplify targeted interception through such means as computer-based data matching, word recognition, and voice identification. For most users, concern about unauthorized access is more likely to focus not on potential high- or low-resource adversaries, such as wiretappers or Government intelligence agencies, but on those in between.

The situation is far from a static one. The spectrum of vulnerabilities shifts as technological advances change the nature of communications systems and the resources available to potential adversaries. Technological advances, other than those associated with information security, tend to increase the capabilities of adversaries, especially those of high- and middle-level resources. Perhaps the most

[9] David Kahn, *The Codebreakers: The Story of Secret Writing (New* York, NY: MacMillan, 1967); James Bamford, *The Puzzle Palace (New* York, NY: Penguin Books, 1983); "Soviets Take the High Ground, New Embassy on Mount Alto is a Prime Watching and Listening Post," *Washing-ton Post,* June 16, 1985, p. B 1; and *The Soviet-Cuban Connection in Central America and the Caribbean,* released by the Departments of State and Defense, March 1985, Washington, DC, pp. 3-5.

Figure 1.—Spectrum of Adversaries' Resource Requirements v. Technologies



SOURCE: Office of Technology Assessment, 1987

visible illustration of this is that of increasingly powerful personal computers, which make unauthorized access to communications and data easier.

But the question remains: Should a business that communicates valuable, sensitive, personal, or proprietary information be concerned about unauthorized access to messages transmitted over the public switched network? If history serves as a guide, we can expect few immediate changes in the confidentiality of private communications over public networks except where user demand is adequate to justify investment in safeguards. However, some corporate and Government users who face considerable risk in the event of such accesses (e.g., for communications deemed sensitive for national security purposes or for electronic fund transfers) are taking steps to improve the confidentiality and integrity of their communications (see ch. 5).

Networks

Early communications networks began as relatively simple point-to-point transmission systems. At first, telegraph and later voice-

modulated electronic signals, were transmitted exclusively over copper wires, and switching was accomplished manually. Such networks were vulnerable to eavesdropping by wiretapping. Today's networks, by contrast, consist of cables (copper wire, coaxial, and fiber optic), radio links (terrestrial and satellite), and other equipment providing a complex mix of services (voice, data, graphics, text, and video) through a variety of specialized interconnected networks. Figure 2 illustrates the complexity of modern networks. In spite of the added complexity, however, vulnerabilities remain.

Communication networks have also vastly expanded the ability of users, whether from an office building or home personal computer, to gain access to computers nationwide and even worldwide. The current movement toward a worldwide digital network is aimed precisely at increasing the accessibility of network capabilities, enhancing the variety of services available, and lowering the costs of services.

Transmission Systems

Communications systems use two types of media to transmit signals: over-the-air systems, such as radio transmissions; and conductors, such as copper wire and coaxial or fiber optic cables. In general, over-the-air systems (e.g., cordless telephones) can be intercepted and systems that use conductors can be tapped. Some conductor-based transmission systems (e.g., fiber optic cable) require sophisticated resources to tap, while others require minimal resources (taps of copper wires from wire closets). Whatever the form of transmission, it is not necessarily easy to render intercepted or monitored signals intelligible.

Microwave Radio Systems

Microwave radio systems, totaling 740 million circuit miles, carry most of the long-distance communications messages transmitted within the United States (table 1).[9] Systems operating at frequencies mostly between 2 and 11 GHz (gigahertz or billion cycles per second), for example, provide high-capacity circuits that carry about two-thirds of all telephone toll calls today. They often use highly directional antennas to transmit signals between stations, typically spaced from 10 to 35 miles apart.

Microwave systems are designed for a wide range of capacities, from as few as 24 voice grade circuits to as many as 2,400 circuits per radio channel. In addition, there are multiple radio channels in each of the many frequency bands that these systems operate in. For example, in the 6 GHz common carrier band, there are eight radiofrequency channels, each capable of carrying 2,400 voice grade circuits.

Interception of point-to-point microwave transmissions is relatively easy if the interceptor has technical information about the transmitter. Most such information is made available to the public by the Federal Communications Commission (FCC). Interception of signals, however, is only part of an eavesdropper's job. The signals must be demodulated and demultiplexed, which can be done using the same type of equipment as used by common carriers. But then an eavesdropper must also be able to sort through individual messages and select those of interest.

Table 1.—Bell System Circuit Miles of Carrier Systems Using Different Transmission Media

	Circuit miles at year end (In millions)	
Media	1975	1982a
Analog:		
Paired wire	42	140
Coaxial cable	142	221
Radio	399	737
Digital:		
Paired wire	58	138
Coaxial cable	—	2
Radio	—	6 (62°/0 installed in 1982)
Fiber optic	—	4 (98°/0 installed in 1982)
Subscriber	—	8 (54°/0 Installed in 1982)

[a]This list shows major categories of transmission media Although *analog* systems were still predominant, the growth of digital systems was almost three times faster from 1975 to 1982 Almost no new analog systems were added during this period Comparable information is not available after 1982, but a significant commitment is being made to glass fiber systems especially by AT&T MCI and GTE

SOURCE Bellcore

[10]Bellcore, *Evolving Technologies: Impact on Information Security,* Apr. 18, 1986.

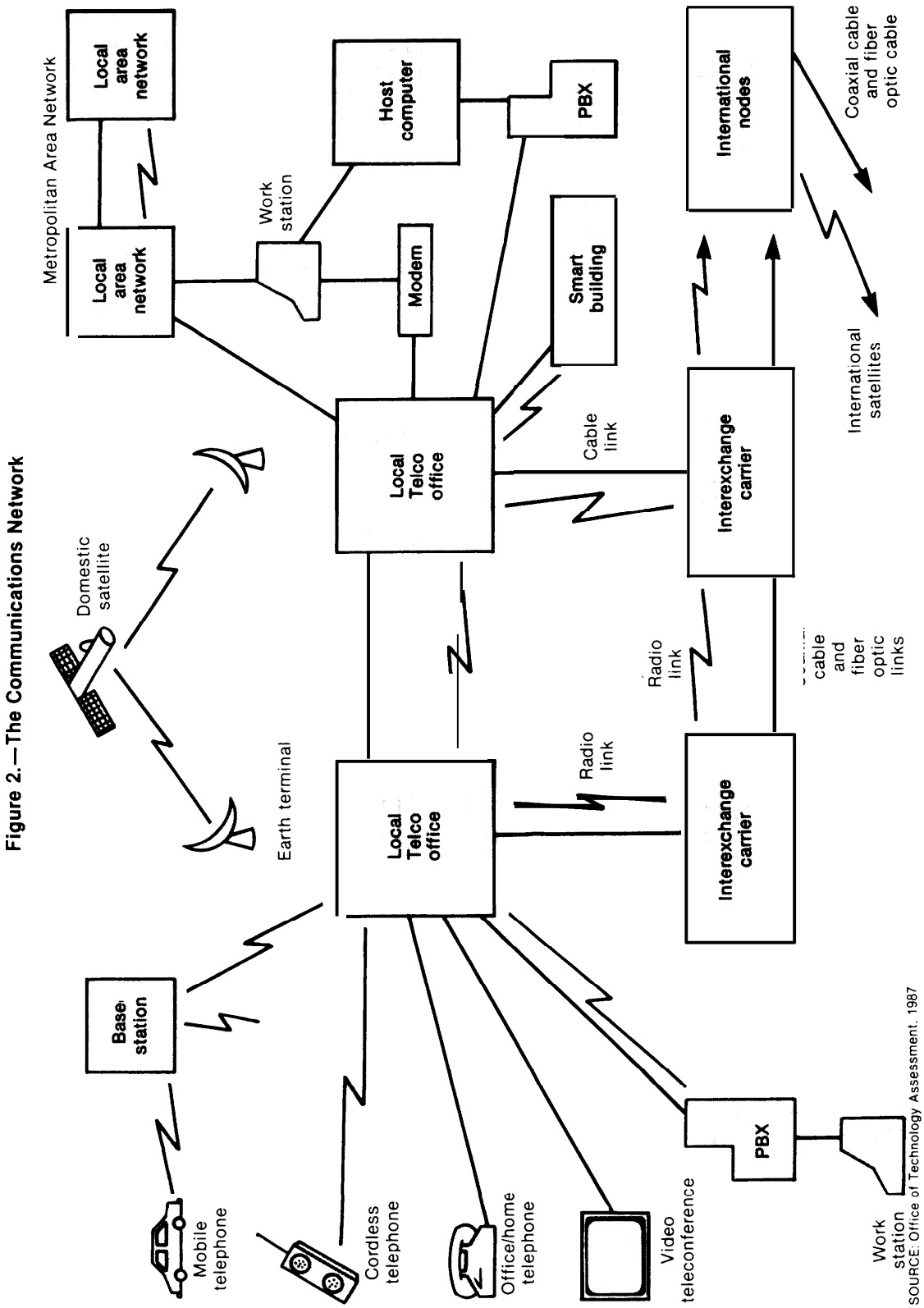


Figure 2.—The Communications Network

SOURCE: Office of Technology Assessment, 1987

Point-to-point systems are vulnerable to interception wherever there is sufficient radiated signal strength. The geographic area in which adequate signals can be received is generally very large. It can cover dozens of square miles in the paths of the antenna's radiation and in the vicinity of either the transmitter or receiver (figure 3). Custom-built receivers may be designed with greater sensitivity than those used by the common carriers in order to broaden the area of reception.

Modern digital systems complicate interception by unsophisticated adversaries, but they simplify the work of those that are more sophisticated. Signals are transmitted as virtually indistinguishable series of ones and zeroes, typically mixed together (multiplexed) with many other signals and encoded prior to transmission to reduce the total number of bits transmitted and thereby reduce bandwidth requirements. Many systems also route different segments of the same transmitted signal over different paths. For adversaries with few resources, these conditions alone would represent significant obstacles, particularly for targeted interception.[11] Other obstacles include the need to record a large volume of data and process it to extract the message content.

For adversaries with considerable resources, such as very powerful computer processing capabilities and the equivalent of the switching and transmission facilities used by common carriers, targeted interception would not represent a severe challenge. Indeed, these adversaries can sort messages to select those of interest and undo the various types of signal processing to recover the message content. To consistently intercept preselected targets in switched systems, potential adversaries must be able to carry out functions equivalent to those performed by the carriers' equipment. In addition, they need the ability to select those messages of interest and to operate covertly. This level of sophistication and investment is assumed to be beyond the means of any adversaries except those with considerable resources and motivation, principally because of the cost of such an operation.

At the other extreme, there is inexpensive commercial equipment that can be used to intercept radio signals.[12] Figure 4 illustrates the types of equipment needed and current prices, based on catalog advertisements. The equipment includes an antenna that can be pointed, low-noise amplifier, receiver, and equipment to extract audio (and video) signals (i.e., demultiplex and demodulate them). Depending on the particular equipment selected, the total price would range from $1,000 to $50,000. People skilled in the design of communications equipment could undoubtedly build their own units for less, however.

Specialized Microwave Systems

The Multipoint Distribution Service (MDS), authorized by the FCC in the early 1970s, uses broadcast microwaves to distribute video and other one-way communications locally. MDS transmitters use omnidirectional antennas to broadcast signals that are received by small parabolic (directional) antennas. MDS systems are typically used as a radio version of cable television and, infrequently, to provide one-way business or educational communications.

A Digital Termination System (DTS) is another specialized microwave radio service that is similar to MDS in terms of its broadcast of microwave signals. However, unlike MDS, DTS is designed for full two-way communications between stations. The mechanics of intercepting DTS transmissions are similar to those involved with MDS or point-to-point microwave systems. Interception might be considered easier with DTS because of the clearer identification of the user's dedicated communications channel.

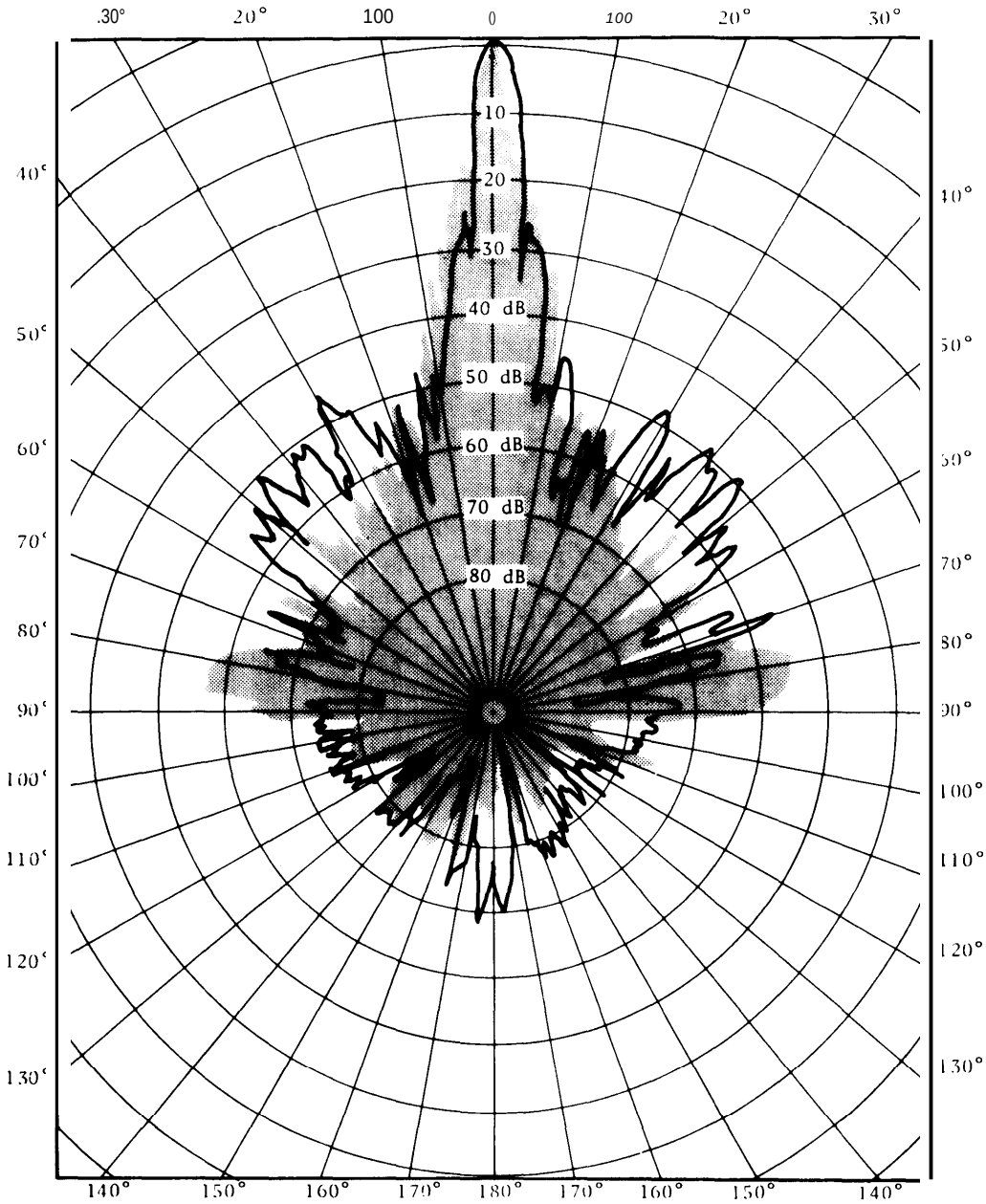
Dedicated Lines

Users who need to communicate extensively between two points often use dedicated *or* pri-

[11] *The* MITRE Corp., *Study of Vulnerability of Electronic Communication Systems to Electronic Interception, vol.* 1, January 1977, p. 96.

[12] Information Security, Inc., "Vulnerabilities of Public Telecommunications Systems, " OTA contractor report, 1986.

Figure 3.—Example of Antenna Directivity Pattern



SOURCE: MITRE Corp., *Study of Vulnerability of Electronic Communication Systems to Electronic Interception,* VOl 1, January 1977

Figure 4.— Examples of Commercial Equipment for Interception of Microwave Radio Signals

Antenna, low noise amplifier, motor drive

Receiver

Type of multiplexing and modulation	FDM/FM	TDM	FDM/AM	SCPC
	Demodulation/down conversion			
Type of demodulation equipment needed	HF AM/SSB	Digital TESTSETS	Scanner VHF/UHF	Scanner VHF/UHF

	Commercial equipment	Approximate price
Examples of Receiving equipment, Low noise amp.. Motor drive ‘	RAYDX 10.5 antenna, LUX or 990C receiver	$2,200 Good quality reception
	ALCOA 6.0 antenna, Uniden 2000 receiver	$695 Minimum quality reception
Examples of Demodulation Equipment	HF-AM/SSB ICOM R7000	$969
	HF-AM/SSB BEARCAT DX1OOC	$285
	VHF-UHF Scanner Regency MX5000	$330

Total system cost: Between $1,000 and $3,200

SOURCE Information Security Inc using catalog prices from SATCOM, and SCANNER WORLD USA magazines, 1986

vate line services. These are fixed circuit paths through some combination of terrestrial or satellite microwave radio or wire transmission facilities. Dedicated lines are commonly used to link corporations' main switching centers with one another, to link interactive computer systems, and to link computer systems with remote terminals. Whereas ordinary dial-up calls might be routed along any of a number of paths depending on traffic loading conditions, dedicated circuits remain in place on the same transmission path. This simplifies the interceptor's burden considerably, since the location of the user's dedicated line need be found just once. As an example of a part of a dedicated circuit, the local loop connecting the subscriber's premise with the local telephone company's nearest office also provides a fixed path that is relatively easy to identify.

Fiber Optic Communications

Fiber optic cable is being installed rapidly by communications carriers in the United States, primarily for heavy traffic, long-distance routes, but also for many local uses. Local telephone companies installed more than 62,500 miles of fiber in 1984 and 100,000 miles in 1985 for their local loops (connecting telephone offices with subscriber's premises). Another 285,000 miles of fiber were installed by the same companies during those years for interoffice trunking (table 2).

Fiber optics is attractive, in part, because much higher data rates can be transmitted—about 1 gigabit per second currently—than using copper wire. One small cable containing two glass fibers can carry more than 15,000 two-way voice telephone conversations, or the

Table 2.—Telephone Company Fiber Applications
(fiber miles in thousands)

	1984		1985	
Companv	Long distance	Loop	Long distance	Loop
NYNEX	25	15	50	25
Bell Atlantic	20	15	30	25
BellSouth	20	35	60	30
Ameritech	25	15	40	35
SW Bell	10	5	50	15
U.S. West	15	5	30	10
Pacific Telephone	20	15	40	25
Independents	10	—	10	5
Total	145	105	310	170

SOURCE: Annual Reports/Internal Siecor Estimates.

equivalent in data signals, for up to 25 miles without requiring repeaters (amplifiers). Conventional telephone cables composed of 24 gauge copper wires, in contrast, would require 1,250 pairs of wires and repeaters spaced about 1 mile apart in order to carry the same traffic. Further advances in fiber technology are widely expected. Fiber optics also is less expensive than conventional cable, does not radiate energy under normal operating conditions, and is not as readily subject to passive or active interception as are radio signals or signals on copper wire. Figure 5 illustrates a typical fiber optic system.

Satellite Communications Systems

Satellites were first used for commercial telecommunications in the mid-1970s. Today, there are more than 100 satellites worldwide, with some two dozen providing domestic services for the United States. Still, satellites account for only a small portion of domestic transmission capacity. In terms of domestic nonbroadcast channel capacity, they are being outpaced rapidly by fiber optic cable. International communications services have, for the past decade, been provided about equally by satellite and cable facilities. This balance is likely to shift sharply with the planned use of fiber optic cable for trans-Atlantic service beginning in 1988 and for trans-Pacific service in 1989.

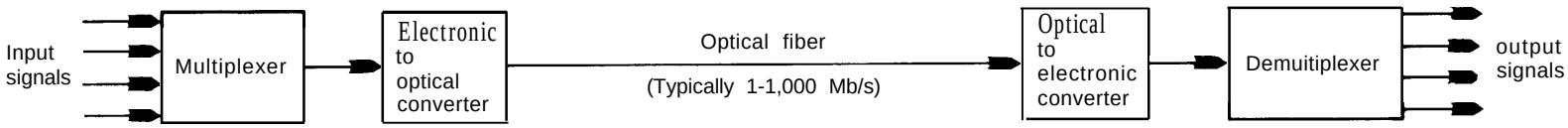
Satellite communications systems operate in much the same manner as microwave relay systems, except that the repeater or amplifier is in geostationary orbit 22,300 miles above the equator. Satellites accept signals from transmitting earth stations (the uplink), translate the signal to a different frequency band, and retransmit it at suitable power levels to receiving earth stations (the downlink).

Some satellite networks are widely used for one-way distribution services, including cable and network television, and a variety of data services, such as financial information and weather reports. Two-way distribution services include point-of-sale transactions, database inquiries, and inventory control. Most of these applications use digital transmission and various techniques to share the satellite bandwidth among the users.

The satellite “footprint,” defined by the beamwidth of the spacecraft antenna, maybe contoured to the shape of the intended coverage area, but is nevertheless likely to be thousands of miles across. The satellite channel is “visible’ to all points within the coverage area and, therefore, readily interceptable within that area. The signals from many satellites may be received from locations beyond the borders of the contiguous United States. The key to targeted interception, consequently, is determining which satellite and transponder channel frequencies are of interest.

One of the simplest methods for intercepting subscription satellite signals was advertised until recently in an amateur radio publication and sold for less than $100. The device used a short piece of wire, cut to the proper

Figure 5.—Typical Fiber Optic System



SOURCE Off Ice of Technology Assessment. 1987

length for reception at the selected broadcasting frequency, and mounted in an ordinary metal coffee can. This apparatus was connected, through the printed circuit card provided, to the lead-in wires of a television set. All that remained was to point the coffee can at the desired satellite, adjusting by trial and error until an adequate signal was received.

These characteristics make communications satellites vulnerable to several different types of misuse. The uplinks can be overpowered by unauthorized users, whether intentionally or not, who transmit stronger signals than those used on the authorized uplink. This was the case in both of the April 1986 takeovers of the Home Box Office (HBO) channel in which a part-time satellite uplink operator and retailer of home receiving dishes overpowered the HBO uplink transmitter signal with an unauthorized one and put his own message on the screens of some 8 million viewers.[13] In addition, the downlinks can be jammed by bogus earth transmitters.

Other vulnerable parts of communications satellites include the transponders, whose lifetimes can be severely shortened by excessive received signal strength and unprotected telemetry systems, which might be manipulated to move the satellite out of its intended orbit.[14] Broadcasters and communications carriers are especially concerned about jamming since the former could lose millions of dollars if advertisements are interfered with and the latter could lose many tens of millions of dollars if a satellite's lifetime is prematurely shortened. Both groups, therefore, want to shift to a less vulnerable transmission system, such as fiber optic cable, if capacity expands sufficiently. [15] There are also concerns about the survivability of satellite communications systems in times of national emergency.[16]

Mobile Radio and Cordless Telephone Systems

Land mobile telephone service typically provides two-way, voice-grade communications between abase station and mobile units or between two mobile units. The mobile unit is most commonly a car phone, although some "briefcase phones" have recently appeared on the market. The use of these systems is growing by about 20 percent annually. In addition, one-way paging services have become very popular recently.

The antennas for these units transmit omnidirectionally. Cellular mobile systems use a base station in each cell to communicate with all mobile units within that cell. A relatively small number of frequencies are needed for each cell. Inexpensive scanners can be used to monitor for mobile call signals and to tune in to the next call made. Each call transmitted from the base station is addressed to a particular mobile unit within the cell, making targeted, passive eavesdropping simple as long as the eavesdropper knows the telephone number of interest and the cell the target is in.

Cordless telephones substitute a duplex (two-way), low-power radio link for what otherwise would be a very long extension cord. Their growing popularity and the relatively small number of channels available have created problems for some users. A cordless phone always uses the same channel in the same small area; thus, these phones are much easier to target by eavesdroppers. Nearby users with the same frequency channel pair can listen to their neighbors' calls simply by listening with their own cordless units. In addition, some people

[13] For a detailed review, see Donald Goldberg, "Captain Midnight, HBO, and World War 3," *Mother Jones*, October 1986, p. 26.

[14] The range of vulnerabilities of commercial communications satellites were discussed in some detail by representatives from HBO, CBS Technology Center, and MA-COM, Inc., at a seminar at the Massachusetts Institute of Technology on Oct. 16, 1986. Also discussed were a number of safeguards that are being considered for current and, especially, future satellites.

[15] Ibid.

[16] See "Commercial Satellite Communications Survivability Report, " prepared for the National Security Telecommunication Advisory Committee (NSTAC), May 20, 1983. This report notes that:

> . . . commercial satellite communications systems are vulnerable to hostile actions which would deny service in emergency situations, particularly actions by a relatively unsophisticated antagonist—the so called "cheap shot" attack. For example, today's satellite command links provide only modest protection against electronic intrusion. Also, in nuclear war, some of the control facilities of satellite systems would become unusable.

have intentionally used their remote units to initiate calls by triggering other parties' base units, thus avoiding having to pay for the call since the related bill (usually for along-distance call) is sent to the base unit owner. This "theft of dial tone" is possible when the base unit does not have appropriate security features.[17]

Mobile and cordless radio have much in common, but two main differences involve signal range and the ease with which an adversary may target on particular users. Although cordless phones are easy to target, their range is typically no more than 1,000 feet, while conventional mobile radio signals may be received at a distance of 20 to 30 miles. Newer cellular mobile phones have a smaller range and use a variety of channels and base stations as they move from cell to cell, making them slightly harder to pinpoint.

Other System Components

Switching Systems

In addition to the transmission paths that connect end users and network nodes, and the network nodes to each other, switching systems located at the network nodes provide opportunities for misuse. Thousands of communications lines are concentrated at these nodes. With the use of telephone company records, individual circuits assigned to particular customers can be identified. In order to reduce opportunities for potential misuse of these records, the operating companies must carefully limit both physical and remote access to these nodes. The necessary precautions are the same as those described below in connection with the security of computer systems.

Most electromechanical switching systems require frequent maintenance, particularly those that serve large numbers of customers. On the other hand, stored, program-controlled switching systems of comparable size require less frequent onsite maintenance since many of their functions can be controlled electronically from remote, centrally located maintenance sites. From these sites, however, access can be gained to an even greater number of communications channels. This is an important reason for controlling both physical and remote access to these nodes. A special concern is electronic access to the processor used to control these switching systems: A knowledgeable individual, for example, could sabotage or manipulate the switching system (e.g., by rerouting calls destined for one person to another) without physical access to the switching systems.

Switching systems are equipped with circuitry designed to permit operators to verify that busy lines are actually in use and, in an emergency, to interrupt ongoing conversations. By the very nature of the circuitry's design, it would permit monitoring of conversations if protections were not incorporated. In fact, current versions of this circuitry have scramblers built in and, if interruption is required, periodic audible tone bursts are used to alert the users that a third party has joined their conversation.

Signaling Elements

Signaling is another element of communications systems that may provide opportunities for abuse. Signaling is normally used to send the destination address data between switching network nodes. There are signaling methods that use either slowly pulsed direct current or voice band tones that are in predominant use between customers' premises and the local telephone office.[18] These are used for voice and a substantial number of data communications. Both of these signaling methods can be monitored, using methods described above for monitoring communications, allowing an eavesdropper to intercept not only message content but also its destination.

Carriers use pen registers and modern dialed number recorders to monitor destination address signals. A new type of digitally coded

[17] See Federal Communications Commission, "Further Notice of Proposed Rulemaking, " Docket 83-325, released May 23, 1984.

[18] Some data communications only use these signaling methods to direct a call through the telephone network to a packet switched network and thus information about the destination address is of limited value to an adversary.

address signaling is now used in connection with some data communications networks, such as packet networks. This type of signaling is also used for internode signaling in AT&T's common channel interoffice signaling system (CCIS) and some other networks. Separation of signaling information from message content increases the confidentiality of messages provided the eavesdropper does not have access to the signaling data. The CCIS encrypts the signaling information sent between nodes.

Operational Support Systems

In addition to the transmission, switching, and signaling components, communications systems include supporting equipment for testing, repairing, and maintaining customer records. The information stored in these systems could be valuable to a person seeking to intercept communications. Access to this information can be limited by time of day, terminal location or function, physical access, logon identification passwords, authorization verification, and audit trail records.

A testing system is another type of operational support system. Testing systems can gain access to specific trunk and line circuits, and thus provide an opportunity to either monitor communications or obtain information regarding communication links. These systems are often protected by many of the same techniques described above.

Commercial Availability of Interception Equipment

The very technologies that make possible continued improvements in communications and computer processing also lend themselves to illicit purposes. The successful disruption of the HBO satellite broadcast in April 1986 shows that some of these systems are no better protected against such attacks than against passive interception. This may be changing as a result of the HBO experience. The satellite transponder cannot distinguish between the legitimate signal and a bogus one—it simply selects the stronger signal.[19] In the HBO case noted earlier, the "adversary' or hacker was sophisticated technically and had access to commercially available and relatively inexpensive transmitter equipment, as well as information in the public domain concerning the satellite's location and transponder frequency.

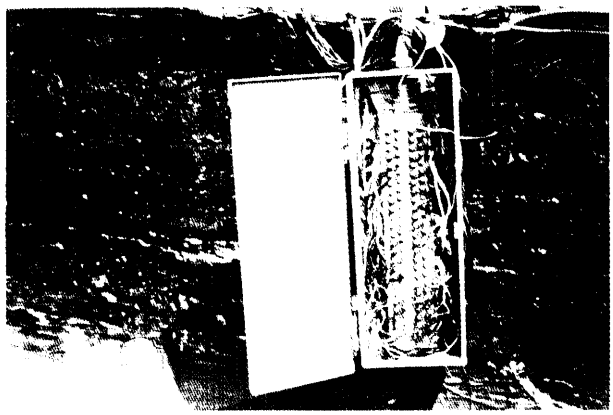
In a completely different part of the network, wiretapping of telephone lines remains one of the simplest forms of eavesdropping, as long as physical access to wire closets and other interconnection points are generally accessible.[20] Certain types of wiretaps cannot be detected by electronic means, and some wiretaps can be performed using equipment costing as little as $12.[21] A wiretap is sufficiently easy to install that even a 9-year-old can do it." Rooftop terminal junction boxes and residential junction boxes are often readily accessible to potential wiretappers. In contrast, when fiber optic cable is used to connect the user's premises to the carrier's facility (the local loop), tapping the fiber cable requires more sophisticated and expensive equipment and skill.

'("'Mystery Broadcast Overpowers HBO," Institute for Electrical and Electronics Engineers, *THE INSTITUTE*, vol. 10, No. 10, October 1986, p. 1.

[20]In one of the relatively few examples in which telephone taps are uncovered, a tap and electronic bugging equipment were recently reported discovered in the office of the governor of New Mexico. "Capitol Bug Found," *Washington Post*, Jan. 10, 1987, p. A8.

[21]Ross Engineering Associates, "Telephone Taps," OTA contractor report, November 1986.

[22]Ibid.



Rooftop Terminal Junction Box

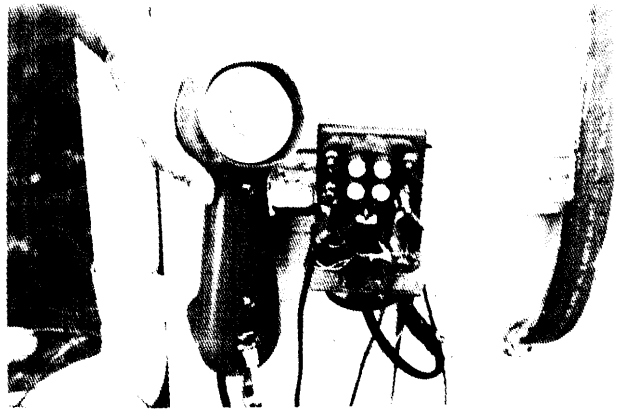


Photo credits Courtesy of Ross Engineering Adams/own MD

Residential Junction Box

VULNERABILITIES OF COMPUTER SYSTEMS[23]

Background

In a simplified form, computer security is the ability of ensuring that people use information systems only as they are supposed to. This involves protecting:

- the system itself against failures, whether caused by deliberate misuse, human error, or technical problems; and
- the information in the system to ensure that it is seen and used only by those who are authorized to do so and that it is not accidentally or maliciously disclosed or modified.

Computer "hackers" aside, it is even more important to recognize that information security is much broader than just protection against those who would penetrate information systems from the outside. People within organizations are perhaps even more likely to misuse information systems, including unauthorized actions by those who are authorized to use the system. In addition, technical failures can be caused by natural disasters.

The rapid evolution of computer technology, and society's growing dependence on it, have important implications for information security. Three distinct kinds of technical trends can be identified that have security implications—the growth of large-scale computers, the evolution of microcomputers, and changes in computer software.

Large-Scale Computers

Advances in large-scale computing have dramatically lowered the cost of computation. [vi] The power of machines relative to their cost and size has been increasing during the last 30 years by more than a factor of 10 per decade and is likely to continue increasing for the foreseeable future. These changes have been complemented by magnetic (and more recently

[23]Because this report emphasizes telecommunications security, the treatment of computer security is brief. For more information on computer security, see U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Management, Security, and Government Oversight,* OTA-CIT-297 (Washington, DC: U.S. Government Printing Office, February 1986).

[24]In this analysis, a "large-scale" computer generally means a machine that is intended to serve multiple users performing different tasks at the same time, that is generally not considered to be a "desk-top' or "personal' computer, and that stores data on large-scale magnetic (or optical) disks rather than floppy disks or small. hard disk drives.

optical) disks that can hold greater and greater amounts of information on each disk. Communication between computers has also become considerably more pervasive and efficient—line speeds are higher, protocols and technical standards have been established, and communications systems are generally evolving from analog links to digital technology.

These increasingly powerful machines have also become much more pervasive in society. Figure 6 shows that the number of mainframe computers operated by the Federal Government has increased from about 11,000 in 1980 to 27,000 in 1985, with most of the increase coming in the Department of Defense. Perhaps more important, figure 7 shows that the points of access to Federal computers have increased geometrically in recent years, from roughly 36,000 terminals in 1980 to 173,000 terminals in 1985. Table 3 indicates similar trends in sales of large-scale host computers in the United States from 36 units in 1965 to more than 1,600 in 1985.

These trends–increased power and use of large-scale computers—have strong implications for security. First of all, the changes have resulted in increased dependence on information technology generally. That means that virtually all Government agencies and private organizations are more susceptible to technical sabotage or failure of their computers. But it also means that there is more information stored in computers, that this information is often accessible to more people, and that this information is accessible at a distance via telecommunications linkages.

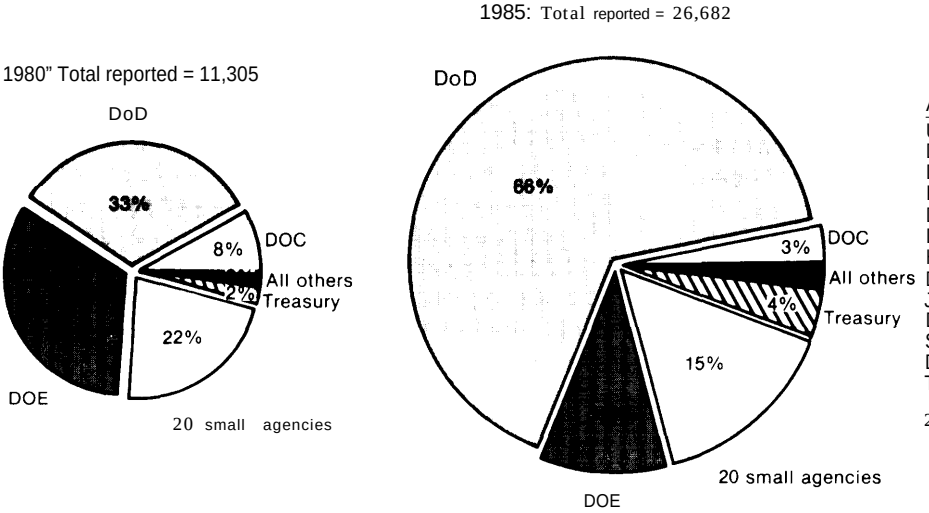
Table 3.—Sales of Large-Scale Host Computers in the United States

Year	Units	Value
1965	36	$200 million
1976	514	$ 2.2 billion
1977	611	$ 2.4 billion
1978	1,009	$ 3.9 billion
1979	1,461	$ 5.3 billion
1980	1,328	$ 4.8 billion
1981	887	$ 3.9 billion
1982	1,448	$ 6.8 billion
1983	1,836	$ 8.1 billion
1984	2,420	$ 9.0 billion
1985	1,617	$ 9.3 billion
1986 (estimated)	1,800	$ 9.7 billion
1987 (estimated)	2,090	$10.2 billion
1988 (estimated)	2,070	$10.6 billion
1989 (estimated)	2,200	$11.5 billion
1990 (estimated)	2,300	$12.1 billion

NOTE: Large. scale host computers are those machines serving more than 128 users in a normal commercial environment This is definition is not necessarily the same as that used in figure 6

SOURCE International Data Corp

Figure 6.— Mainframe Computers in Federal Agencies



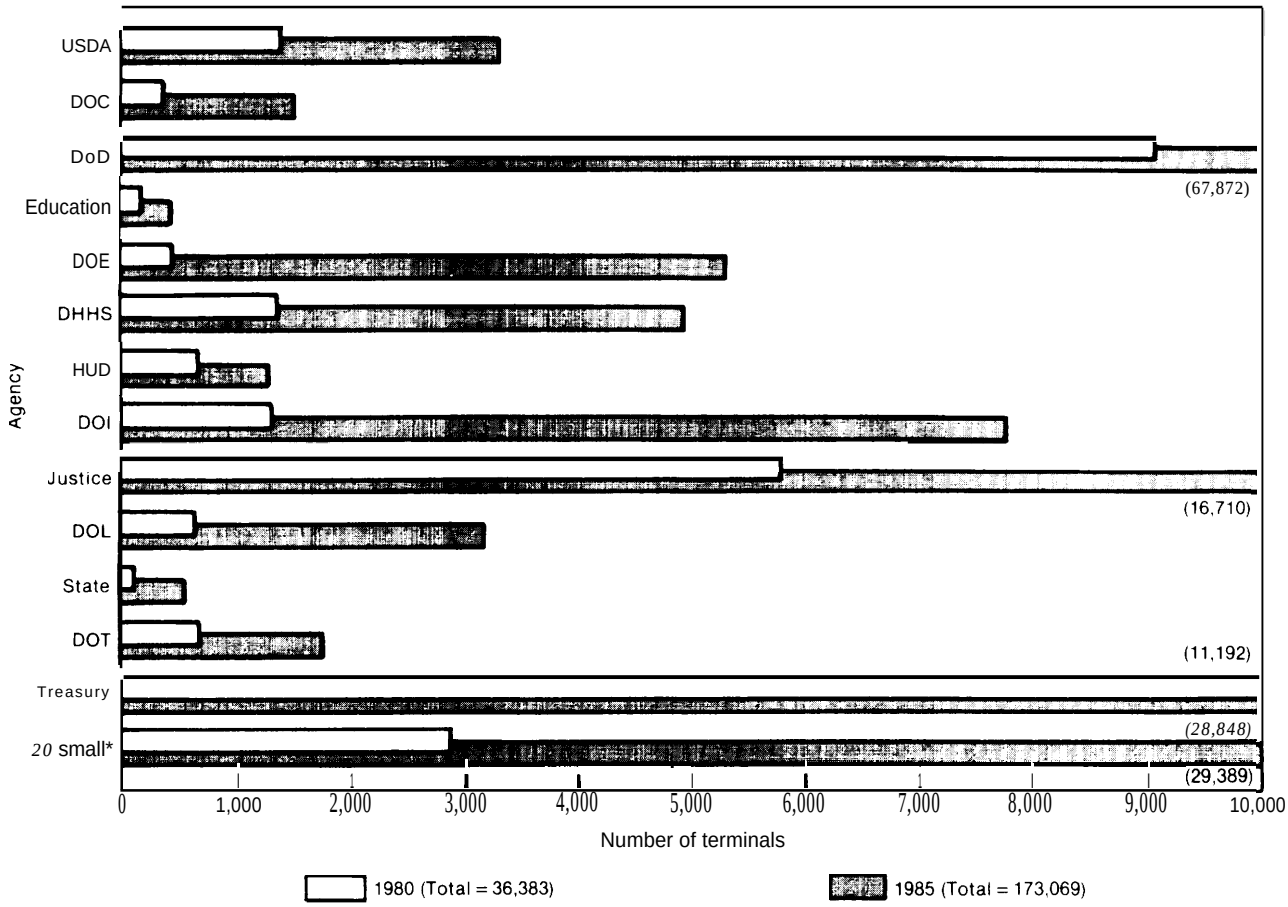
Reported numbers of mainframe computers in Federal agencies

Agency	1980	1985
USDA	13	23
DOC	967	915
DoD	3,765	17,565
Education	3	6
DOE	3,718	2,781
DHHS	48	106
HUD	3	7
DOI	81	250
Just Ice	28	75
DOL	11	15
State	5	6
DOT	16	15
Treasury	205	1,030
20 small agencies	2,443	3,888
Total	11,305	26,682

NOTE' Consistency in definitions of "mainframe" central processing units cannot be assured because of different Interpretations of the term Definitions may not agree with definition of large host computers in table 3

SOURCE" OTA Federal Agency Data Request

Figure 7.—Computer Terminals in Federal Agencies



*20 selected independent agencies that received OTA's data request.

SOURCE: OTA Federal Agency Data Request.

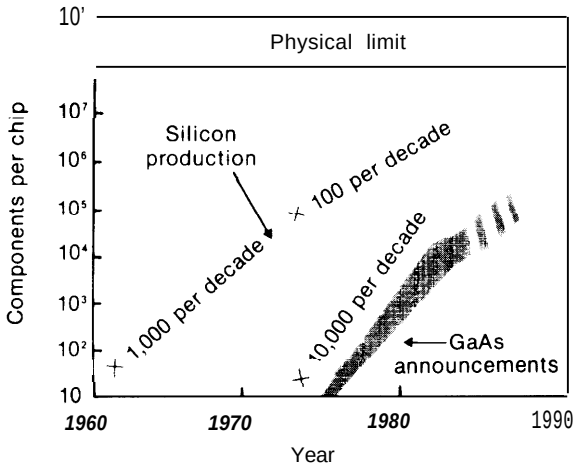
On the other hand, the increased power and sophistication of large-scale computers also means that more sophisticated safeguards are more practical than they were with smaller computers. These safeguards include "audit programs that log the actions of each user and more powerful access controls. These and other safeguards are discussed in chapter 4.

Microcomputers

Changes in smaller desk-top or personal computers have been even more striking and rapid than those in large-scale machines. Since the first microcomputer was commercially produced in the mid- 1970s, these devices have progressed to a point where their speed and power nearly equal that of mainframe computers a decade ago. These improvements are largely due to the increasing number of circuits that manufacturers can put on a single microprocessor chip. Figure 8 shows the geometric increases in the complexity of these chips, which has led to a declining cost per unit of computing power.

Microcomputers have also changed from an obscure hobbyist item to a standard and necessary piece of equipment in many homes, businesses, and Government offices. Figure 9 shows that the number of microcomputers in the Federal Government rose from only a few thousand in 1980 to about 100,000 in 1985. Ta-

Figure 8.—Trends in Component Density, Silicon Production. and Gallium Arsenide Announcements, 1960 to 1990



SOURCE: AT&T Bell Telephone Laboratories

Table 4.—Sales of Personal Computers in the United States

Year	Units	Value (thousands)	Value (billions of dollars)
1980		379	1.1
1981		644	1.9
1982		2,884	4.2
1983		5,872	8.7
1984		6,586	13.0
1985		5,689	13.3
1986 (estimated)		6,633	14.6
1987 (estimated)		7,414	15.9
1988 (estimated)		8,262	17,7
1989 (estimated)		9,317	19.8
1990 (estimated)		10,120	21.6

SOURCE: International Data Corp

ble 4 shows comparable trends in the Nation as a whole, with sales of personal computers rising from 380,000 in 1980 to almost 6 million in 1985.

Microcomputers are computers in their own right and thus require appropriate administrative and technical security measures to safe guard the information they process. Also, microcomputers can be networked and/or function as "smart" terminals to larger computer systems. Thus, the rapid proliferation of microcomputers cannot only place computing power in the hands of an increasing number of computer-literate individuals, but also can decentralize data processing capabilities. For example, employees of many firms or Government agencies are able to collect and manipulate information on their own desk-top microcomputers. Additionally, they are to able use these microcomputers to copy or "download" large amounts of information from the organization's central computer and also to "upload" information they have collected or manipulated into the central computer files.

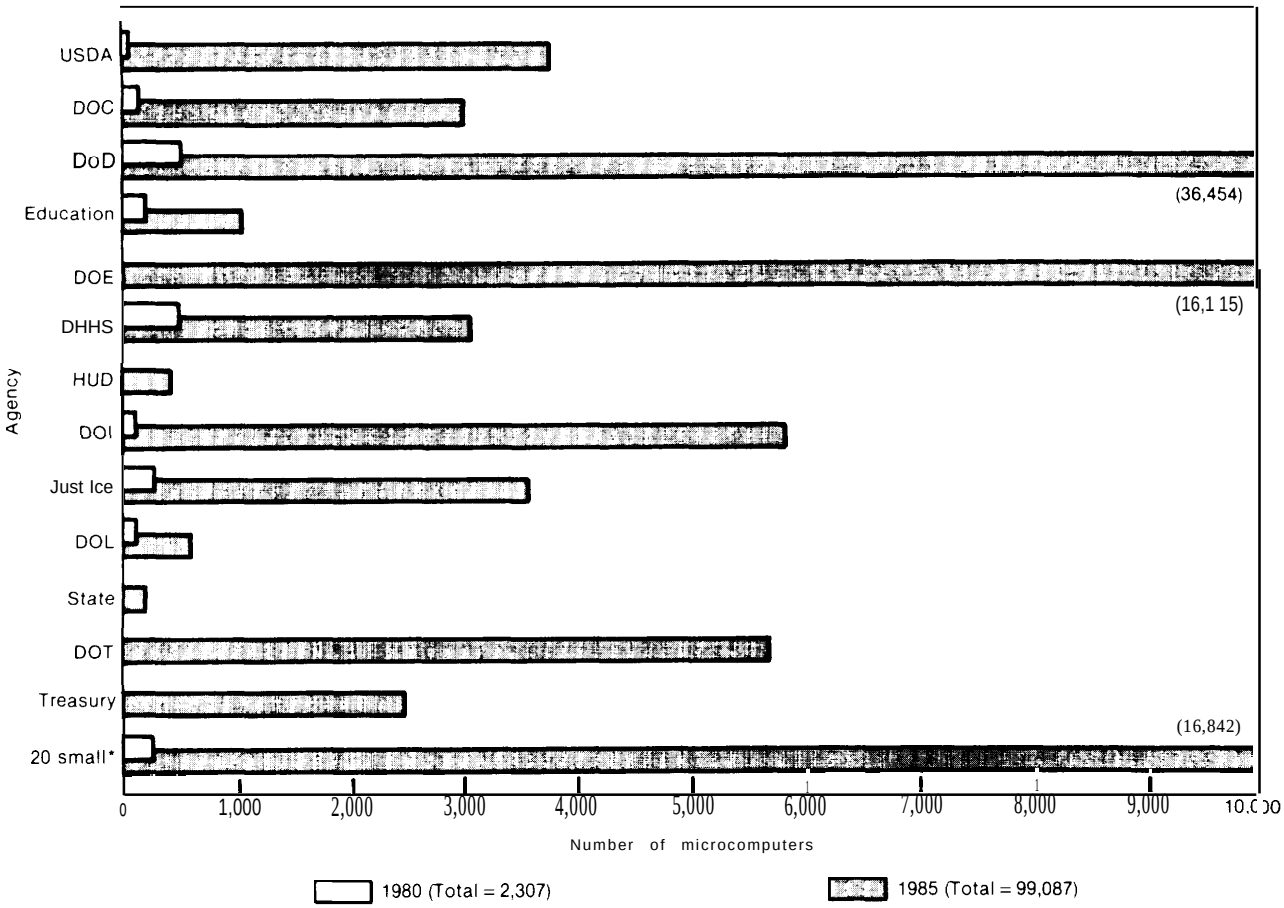
The expanding use of microcomputers can have an adverse effect on security if the appropriate security policies, procedures, and practices are not in effect. For instance, in a computer system that is not organized so as to control and monitor users' access to data files and constrain the data transactions that authorized users are permitted to perform, users can copy or manipulate data in an essentially uncontrolled fashion. There is a growing array of add-on microcomputer security products that address security problems of this sort, as well as an increasing awareness of the importance of using these safeguards. Also, the capability (at the mainframe computer) to control the downloading/uploading of data files is well within current technology. However, actual practice often falls short of the ideal, particularly in firms that do not recognize the value of electronic information in microcomputers and the importance of safeguarding it.

Using microcomputers instead of "dumb" terminals, on the other hand, can help if good security practices control the downloading and uploading of data files and if the system is configured properly. For example, data integrity can be improved by procedures requiring authorized users to make additions, corrections, or other modifications to large data files on a microcomputer. If the modified data are checked, and only then uploaded to the main computer files, then the probability of accidental or malicious deletions of main files, for instance, can be reduced.

Software

Technical sophistication in software and in databases has progressed more slowly than hardware advances. In fact, many people now

Figure 9. —Microcomputers in Federal Agencies



"20 Independent agencies selected by OTA to receive the data request

NOTE: The data request used GSA's definition of microcomputer, slightly adapted: "Any microprocessor-based workstation capable of independent use — including stand-alone and networked personal computers, professional computers, intelligent terminals, word processors, and other similar devices — costing less than $10,000 per unit, but excluding peripherals and separately purchased software."

SOURCE: OTA Federal Agency Data Request.

recognize that software is the bottleneck for many prospective applications of information technology. Nevertheless, the past two decades have seen significant increases in the size of databases that can be reasonably accommodated by software and in the sophistication of the software itself. This means, for example, that software can link disparate pieces of information in a database more readily and that users can make inquiries of databases using more natural commands.

These changes give more people direct access to computerized data and the databases contain far more information that is subject to both authorized and unauthorized use. Further, although not a subject of significant concern to many users, some security experts consider that the inferential ability to link pieces of information in a database or from different databases can have subtle but important implications for security. To date, most attention to this type of problem has been on the part of the defense and intelligence communities, but the problem can be more general. Even when the most sensitive information is unavailable, an adversary can infer critical data by combining pieces of apparently innocuous in-

formation (e.g., determining information about the design of a company's product from its orders for raw materials).

The Extent of Computer Misuse

A variety of recent studies have indicated substantial increases in computer misuse. However, information available about the extent of computer misuse is spotty. Moreover, these studies suffer from serious shortcomings that make generalizations difficult (large successful frauds are often not reported, let alone prosecuted).

The most significant studies and findings include:

- The American Bar Association's 1984 "Report on Computer Crime." In a survey of 283 public and private sector organizations, ABA found that 25 percent of the respondents reported "known and verifiable losses due to computer crime during the last 12 months."
- The American Institute of Certified Public Accountants 1984 "Report on the Study of EDP-Related Fraud in the Banking and Insurance Industries." AICPA surveyed 5,127 banks and 1,232 insurance companies. Two percent of the banks and 3 percent of the insurance companies said they had experienced at least one case of fraud related to electronic data processing. Sixteen percent of the frauds were reported to involve more than $10,000, although that figure does not reflect funds that were recovered.
- The President's Council on Integrity and Efficiency issued "Computer-Related Fraud in Government Agencies: Perpetrator Interviews," in May 1985. The Council surveyed Federal agencies and found a total of 172 relevant cases of computer fraud or abuse. The losses in fraud cases ranged from zero to $177,383, with the highest proportion in the $10,000 to $100,000 range.
- The Department of Justice's Bureau of Justice Statistics 1986 report "Electronic Fund Transfer System Fraud." This reported a study of fraud related to the transfer of electronic funds in key banks. The study estimated that banks nationwide lost $70 million to $100 million annually from automatic teller fraud. It also examined losses from wire transfers, although there were insufficient data to estimate national loss levels. Twelve banks reported 139 wire transfer fraud incidents within the preceding 5 years, with an average net loss (after recovery efforts) per incident of $18,861. However, the loss exposure or the potential loss per wire transfer incident averaged nearly $1 million.
- Security magazine and the Information Systems Security Association surveyed their subscribers and members in 1985 and 1986. Eighteen percent of the 1986 respondents reported that their company had detected a computer crime in the last 5 years, compared with 13 percent reported by the 1985 respondents. The respondents rated the threats to computers, in descending order: unauthorized use by employees, routine errors and omissions, carelessness with printouts, theft of computers, fire damage, use/misuse by outsiders, and vandalism.

While these studies are far from conclusive, it is apparent that deliberate misuse of computers is a significant and growing problem.

TYPICAL VULNERABILITIES OF INFORMATION SYSTEMS

The combined advances in communications and computer technologies have resulted in information systems that are an order of magnitude more complex than those of 10 or 20 years ago. Not only is computing power greatly increased, but it is also more decentralized—and communication between computers and interconnected devices has become far more

pervasive. In some ways, this has improved security in that, for example, information is no longer stored in just one large computer, which could result in chaos if it failed. On the other hand, information systems are much more extensively linked and interdependent, and the number of points from which technical failure, deliberate misuse, or accidental errors could cause serious problems has increased geometrically.

To illustrate the numerous vulnerabilities of computer systems, figure 10 presents a schematic diagram of a typical information system. The circled letters in the figure correspond to certain types of vulnerabilities (discussed below) that encompass the vast majority of potential problems caused by deliberate misuse of computer systems. Some problems are more important in some systems than in others and potential adversaries may be more or less sophisticated. As will be seen in chapter 4, good security practices would require security officials to perform an analysis of each system to determine which vulnerabilities and threats are most significant and what protective measures would be most appropriate and cost-effective.

The first two kinds of vulnerabilities do not require direct on-line access to data and, generally, an adversary needs relatively few resources to exploit them. The first (a) is theft of storage media that contains valuable data. Theft (or copying) of personal computer diskettes, for example, can be particularly easy because personal computer users often do not lock up their diskettes. Similarly, theft of printouts (b), especially discarded ones, is typically quite easy and has been the source of a significant amount of computer abuse. The printouts may contain valuable competitive information or account and password information that allows an unauthorized person to later gain electronic access to the system.

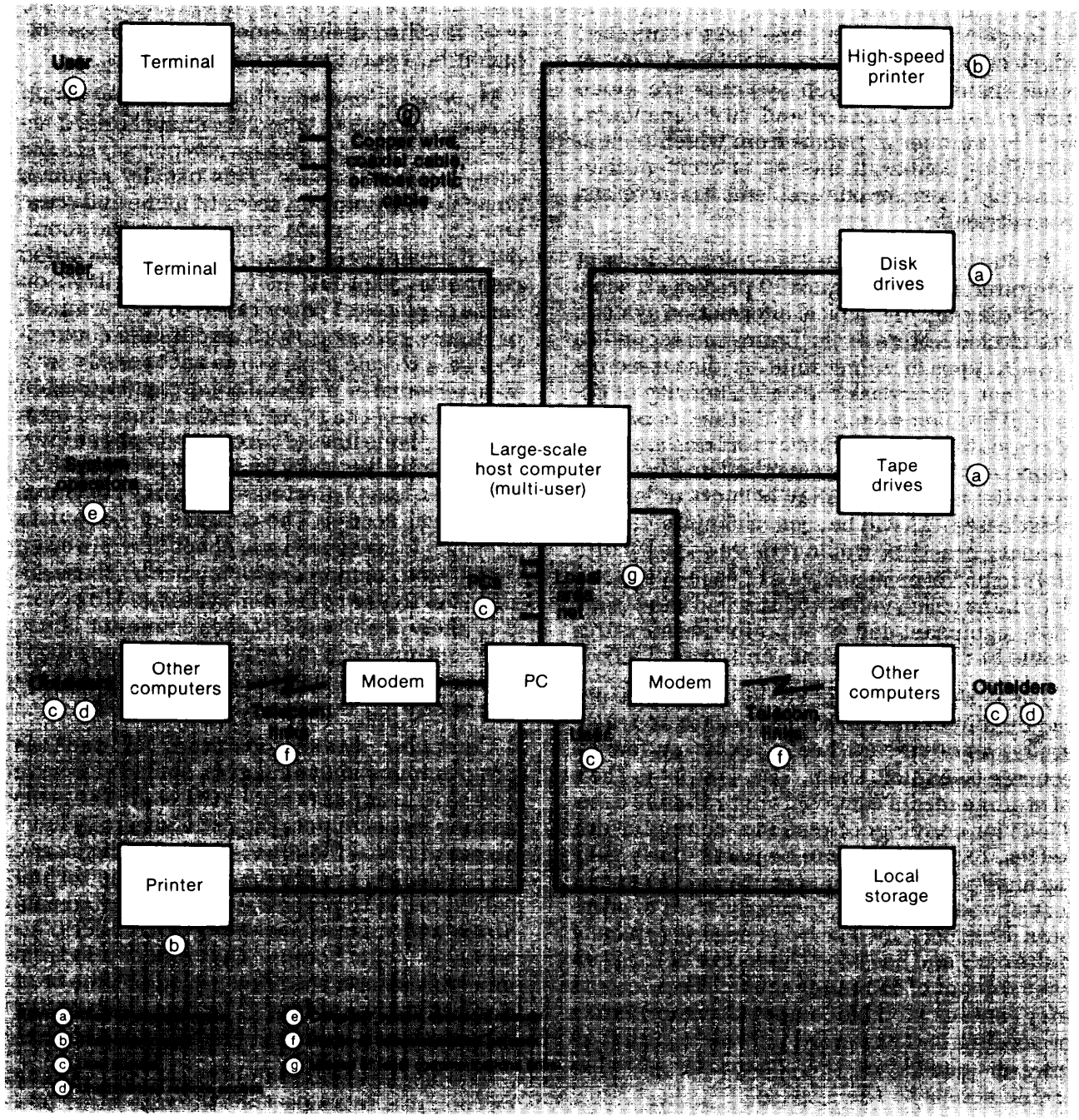
The next type of vulnerability is misuse of computer systems by those who are authorized to use them (c). The misuse can consist, for example, of stealing corporate secrets, changing personnel information, causing falsified checks to be written, or damaging databases. This type of misuse typically requires only a moderate level of sophistication on the part of the perpetrator, although in some cases (e.g., falsified disbursements) it requires collusion between two or more workers.

Moving up one step further in level of adversary, outsiders who gain unauthorized access to a computer system can perpetrate the same kinds of misuse. This usually requires covertly obtaining an account name and password by, for example, looking over the shoulder of an authorized user, finding a discarded computer printout, using codes written on cards or pieces of paper taped to the terminal, or simply guessing. Such an outsider could either seek to gain access to an authorized user's local terminal or personal computer (c)or could try to access the system from a remote location via phone lines (d). Access via phone lines *is* inherently less risky for the perpetrator since it is often less protected by security measures than local access. The dangers of hobbyists prowling in computers via phone lines are often overstated compared with misuse by those authorized to use computer systems. However, it is likely that long-distance computer abuse will continue to grow and more serious adversaries (e.g., technically adept criminals, including organized crime) will be involved.

Computer system operators (e), such as programmers and managers, sometimes have access to user passwords. Although this is becoming less common, they still generally have access to stored files unavailable to other users. In particular, programmers have the technical expertise to perpetrate sophisticated sabotage and misuse, including such exotic attacks as “logic bombs” that render a system unusable after a specified period of time or at a specific time (often after the disgruntled programmer is no longer employed at the site).

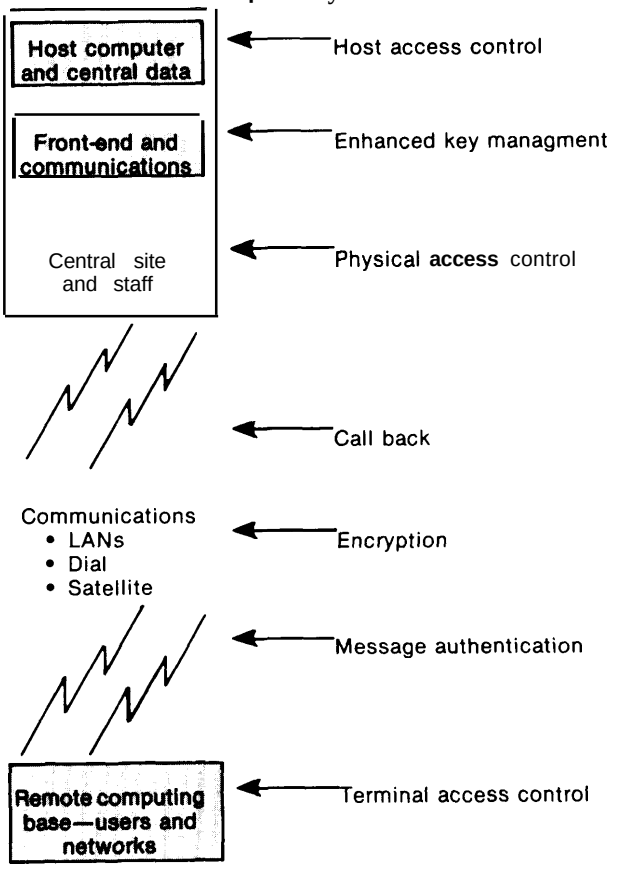
The last two vulnerabilities, eavesdropping on computer transmissions through either tele communications links (f) or local connections (g), are discussed in previous sections of this chapter. Chapter 4 describes some of the safeguards that have been developed to address these vulnerabilities and prevent such crimes in the future. Figure 11 shows how these safeguards can be used in computer networks.

Figure 10.—Typical Vulnerabilities of Computer Systems



SOURCE: Office of Technology Assessment, 1987.

Figure 11 .—Technical Safeguards for Computer Systems



SOURCE: *Personal Identification News* (Washington, DC: Warfel & Miller, Inc., 1986).