[redacted]

[redacted]

(U) Computers and the Internet

(U) Background

[redacted]

(U) Advances in telecommunications and in computer technology have caused an information revolution in the United States and worldwide, the impact of which may be as profound as that of the industrial revolution of the 19th century. Developments such as fiber optic cable have occurred when computer processor speeds have doubled and redoubled and computer memory has trebled and sextupled. A seemingly instantaneous evolution of telephone, cable, satellite and computer networks and software, combined with technological breakthroughs in computer processing have made this latest revolution possible.

(U) Apart from the rapid evolution of personal computers (PCs), the computing environment today allows for a sophisticated and complex interconnection of PCs, networks and hosts. Many organizations now have PCs connected to different networks with the additional capability of accessing a mainframe. Laptops and notebook computers add to the risk factor by providing the ability to easily remove sensitive information from the workplace. The loss of sensitive information, whether deliberate or inadvertent, can carry a price tag far beyond the cost of platform hardware.

(U) Since networks of computers allow users to share vast amounts of data very efficiently, networked computer environments are used every day by the majority of corporations and organizations. Corporate networks are not always designed and implemented with security in mind, merely functionality and efficiency. Although this is good from a business standpoint in the short-term, security problems arise later, which cost millions to solve in larger environments.

(U) The most obvious example of both the prevalence and power of computer networking today is the Internet. The Internet is not a single network, but a worldwide collection of loosely connected networks that are accessible by individual computer hosts in a variety of ways, including gateways, routers, dial-up connections, and Internet service providers. The Internet is easily accessible to anyone with a computer and a network connection. Individuals and organizations worldwide can reach any point on the network without regard to national or geographic boundaries or time of day.

(U) The only equipment required for Internet access is a computer with a modem and a telephone line, and even these requirements are being superseded by services that offer high-speed connection through cable TV lines or directly through a combination computer-television set. As more people get connected, the attractiveness of the Internet as a convenient, cheap, quick and intriguing way of communicating increases. With more participants, the amount of available information (news groups, program and data files, graphic and multimedia documents, and government and industry documents) increases and attracts even more users.

Corporate networks are not always designed and implemented with security in mind, merely functionality and efficiency.

(U) The Internet strives to be a seamless web of networks; therefore, it is often impossible to distinguish where one network ends and another begins. Local, state, and Federal government networks are connected to commercial networks, which in turn are connected to military networks, financial networks, utilities networks, etc.

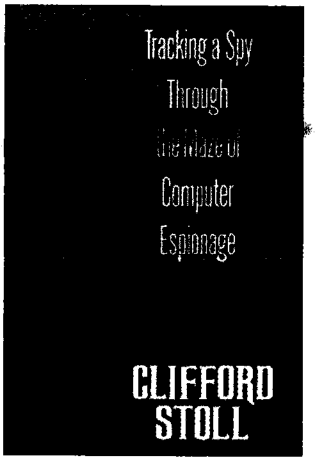
(U) History of Internet Security

(U) The Internet began in 1969 as the ARPANET, a project funded by the Advanced Research Projects Agency (ARPA) of the U.S. Department of Defense. One of the original goals of the project was to create a network that would continue to function even if major sections of the network failed or were attacked. The ARPANET was designed to reroute network traffic automatically around problems in connecting systems or in passing along the necessary information to keep the network functioning.[127]

(U) As more sites joined the ARPANET, the usefulness of the network grew. The ARPANET consisted primarily of university and government computers, and the applications supported on this network were simple: electronic mail (E-mail); electronic news groups; and remote connection to other computers. By 1971, the Internet linked about two dozen research and government sites, and researchers began to use it to exchange information not directly related to the ARPANET itself. The network was becoming an important tool for collaborative research.[128]

(U) The ARPANET protocols (the rules of syntax that enable computers to communicate on a network) were originally designed for openness and flexibility, not for security. The ARPA researchers needed to share information easily, so everyone needed to be an unrestricted "insider" on the network. During these years, researchers also played "practical jokes" on each other, using the ARPANET. These jokes usually involved humorous messages, annoying messages, and other minor security violations. It was rare that a connection from a remote system was considered an attack, however, because ARPANET users comprised a small group of people who generally knew and trusted each other.[129]

(U) In 1986, the first well-publicized international computer-network security incident was identified. A university scientist noticed a simple accounting error in the computer records of systems connected to the ARPANET, and this discrepancy led him to uncover an international effort, using the network, to connect to computers in the United States and copy information from them. These U.S. computers were not only at universities, but at military and government sites all over the country. This incident raised awareness that the ARPANET could also be used for destructive purposes.[130]



(U) In 1988, the ARPANET had its first automated network security incident. A student at Cornell University, Robert T. Morris, wrote a program, now called a "worm," that would connect to another computer, find and use one of several vulnerabilities to copy itself to that second computer, and begin to run the copy of itself at the new location. Both the original code and the copy would then repeat these actions in an infinite loop to other computers on the ARPANET. This "self-replicating automated network attack tool" caused a geometric explosion of copies to be started at computers all around the ARPANET. The worm used so many system resources that the attacked computers could no longer function. As a result, 10% of the U.S. computers connected to the ARPANET effectively stopped at about the same time.[131]

(U) By that time, the ARPANET had grown to more than 88,000 computers and was the primary means of communication among network security experts. With the ARPANET effectively down, it was difficult to coordinate a response to the worm. Many sites removed themselves from the ARPANET altogether, further hampering communication and the transmission of the solution that would stop Morris's worm.[132]

(U) The Morris worm prompted the Defense Advanced Research Projects Agency (DARPA, the new name for ARPA) to fund a computer emergency response team, now the CERT Coordination Center at Carnegie-Mellon University, to give experts a central point for coordinating responses to network emergencies. Other teams quickly sprang up to address computer security incidents in specific organizations or geographic regions. Within a year of their formation, these incident response teams created an informal organization now known as the Forum of Incident Response and Security Teams (FIRST). These teams and the FIRST organization exist to coordinate responses to computer security incidents, assist sites in handling attacks, and educate network users about computer security threats and preventive practices.[133]

(U) In 1989, the ARPANET officially became the Internet and moved from a government research project to an operational network; by then it had grown to more than 100,000 computers. Security problems continued, with both aggressive and defensive technologies becoming more sophisticated. Among the major security incidents were the 1989 WANK/OILZ worm, an automated attack on one type of system attached to the Internet, and exploitation of vulnerabilities in widely distributed programs such as the "sendmail" program, a complicated set of instructions commonly used for sending and receiving electronic mail.[134]

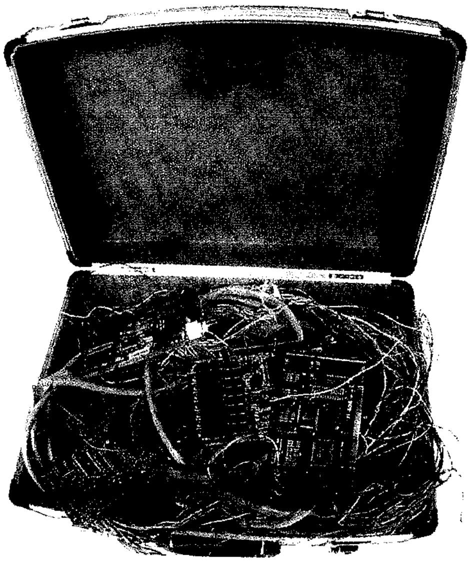
(U) In 1994, intruder tools were created to "sniff" packets from the network easily, resulting in the widespread disclosure of user names and password information. A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travels over the network in clear text.[135]

(U) In 1995, the method that Internet computers use to name and authenticate each other was exploited by a new set of attack tools that allowed widespread Internet attacks on computers that have "trust relationships" with any other computer, even one in the same room. Computers on networks often have trust relationships with one another. For example, before executing some commands, the computer checks a set of files that specify which other computers on the network are permitted to use those commands. If attackers can forge their identity, appearing to be using the trusted computer, they may be able to gain unauthorized access to other computers.[136]

(U) Although the Internet was originally conceived of and designed as a research and education network, usage patterns have radically changed. The Internet has become a home for private and commercial communication, and it is still expanding into important areas of commerce, medicine, and public service. Increased reliance on the Internet is expected over the next five years, along with increased attention to its security.[137]

(U) Threats to Computer Network Security

(U) Three basic security concepts important to information on computer networks are confidentiality, integrity, and availability. When information is read or copied by someone not authorized to do so, the result is known as loss of confidentiality.



Information can be corrupted when it is available on an insecure network. When information is modified in unexpected ways, the result is known as loss of integrity. Information can be erased or become inaccessible, resulting in loss of availability. This means that people who are authorized to get information cannot get what they need.[138]

(U) Concepts relating to the people who use network information are authentication, authorization, and nonrepudiation. To make information available to those who need it and who can be trusted with it, organizations use authentication and authorization. Authentication is proving that a user is who he or she claims to be. That proof may involve something the user knows, such as a password; something the user has, such as an electronic passcard; or something about the user that proves his identity, such as a fingerprint. Authorization is the act of determining whether a particular user (or computer system) has the right to carry out a certain activity, such as reading a file or running a program. Authentication and authorization go hand in hand. Users must be authenticated before carrying out the activity they are authorized to perform. Security is considered to be strong when the means of authentication cannot later be refuted—the user cannot later deny that he or she performed the activity. This is known as nonrepudiation.[139]

(U) Just as with other types of threats, it is useful for OPSEC managers to conceptualize computer network security in terms of the risk of loss of critical information or other damage caused by outsiders versus the risks posed by the actions of insiders. While the potential for attack may come from a variety and potentially large number of individuals, computer attacks themselves tend, just like other areas of OPSEC concern, to use a relatively small number of methodologies to compromise the organization's security systems.[140]

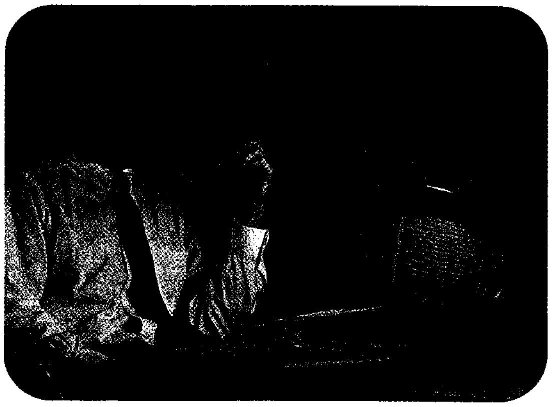
(U) Website Content and OPSEC

(U) It is not necessary for an intelligence adversary, a terrorist, an economic competitor, a mischief-maker, or any other potential security threat to an organization to devise novel and clever methods to steal the organization's critical information, if that information is already being given away on the organization's website or a series of sites. While the World Wide Web provides any organization a new and powerful tool for conveying information quickly and efficiently on a broad range of topics, it also increases the risk to the organization. The particular problem posed by today's technology is that Internet connectivity provides a single user with new levels of understanding from unclassified sources.[141]

(U) While analysts have always employed "data mining" techniques to collect small pieces of information from a number of different sources and compile them into a product which contains critical information, it was hard for them to produce a timely product. Their problem was that the sources of information they required might be very widely scattered, and gaining physical access to them imposed real constraints on the process. With today's interconnected networks, however, geography is no longer a factor in information retrieval. Time is now the most critical factor, but increasingly sophisticated computer search engines and information compilation algorithms have automated many steps in the research process and vastly reduced the time necessary to collect comprehensive amounts of information.[142]

Information posted on the organization's website may pose more risk than information about the organization available through other means.

(U) For OPSEC managers, this means that information posted on the organization's website may pose more risk than information about the organization available through other means. For example, one website might identify the officers of a given military unit, and a page on the site might provide names of immediate family members. Using this information, an analyst might be able to locate another website that provides support and advice to military families. Noting the type of support offered, in particular anything under a "what's new" banner, an analyst might be able to derive indicators that the unit will deploy in the near future or indicators of where the unit will deploy. Both of these items of intelligence might be considered critical to the unit's ability to carry out its mission. Using conventional information-gathering techniques, it might take days or even weeks to gather such information; on the Internet, it could take only hours—or even minutes.



(U) Because of the increased risk that someone will be able to make a coherent mosaic of small pieces of information, small items of information posted on a publicly available website are of increased OPSEC significance. Further, it may be possible for an intelligence adversary, or other collector, to put together a public item from one site, and an item from an unrelated site, and derive critical information from the combination. An OPSEC manager, can no longer simply review the organization's website for items that may be targets for an adversary, since there is no sure way of specifically identifying which items in conjunction with information from other sites or sources may become a critical indicator.

(U) The OPSEC solution to this apparent security dilemma is to adopt a zero-based approach to website content. Decide which items, combined with other information, would be critical to an outside collector. Use OPSEC procedures to determine what information is necessary to post on websites to fulfill the mission. These are the most important considerations in zero-based website security:

- (U) **Assess the benefits to be gained by posting specific types of information on a website.** Identify a target audience for each type of information and why their need for the information is important to the organization's mission. A careful examination of the potential consequences of placing information on the website is necessary.[143]

- (U) **Post only information for which the organization is responsible.** Since any organization knows its own critical information best, it can reduce the vulnerability of other organizations by letting them post their own information.[144]

- (U) **Do not post public links to more sensitive sites.** These links identify the existence and location of potential targets for a collector who may previously been unaware of them. If it is necessary to link to other sites, the link should pass through an intermediate site, which can screen visitors through passwords or other criteria.[145]

(U) Roots of Network Vulnerability

(U) Many early network protocols that now form part of the Internet infrastructure were not designed with security in mind. Without a fundamentally secure infrastructure, network defense becomes more difficult. Furthermore, the Internet is an extremely dynamic environment. Its software changes constantly, and this makes it difficult for security systems to catch up with current and newly discovered security holes.[146]

(U) Because of the inherent openness of the Internet, and the original design of its protocols, Internet attacks are quick, easy, inexpensive, and may be hard to detect or trace. An attacker does not have to be physically present to carry out the attack. Many attacks can be launched readily from anywhere in the world—and the location of the attacker can easily be hidden. It is not always necessary to "break in" to a site (i.e., gain privileges on it) to compromise the confidentiality, integrity, or availability of its information or service.[147]

(U) Many sites place unwarranted trust in the Internet. It is common for operators of sites to be unaware of the risks or unconcerned about the amount of trust they place in the Internet. They may not be aware of what can happen to their information and systems. They may believe that their site will not be a target or that precautions they have taken are sufficient. The technology is constantly changing and intruders are constantly developing new tools and techniques, therefore solutions do not remain effective indefinitely.[148]

(U) Since much of the traffic on the Internet is not encrypted, confidentiality and integrity are difficult to achieve. This situation undermines not only applications (such as financial applications that are network-based) but also more fundamental mechanisms such as authentication and nonrepudiation. As a result, sites may be affected by a security compromise at another site over which they have no control. An example of this is a packet sniffer that is installed at one site but allows the intruder to gather information about other sites, possibly in other countries.[149]

(U) Another factor that contributes to the vulnerability of the Internet is the rapid growth and use of the network, accompanied by rapid deployment of network services involving complex applications. Often, these services are not designed, configured, or maintained securely. In the rush to get new products to market, developers do not adequately ensure that they do not repeat previous mistakes or introduce new vulnerabilities.[150]

Operating system security is rarely a purchase criterion.

(U) Compounding the problem is that operating system security is rarely a purchase criterion. Commercial operating system vendors often report that sales are driven by customer demand for performance, price, ease of use, maintenance, and support. As a result, off-the-shelf operating systems are shipped in an easy-to-use but insecure configuration that allows sites to use the system soon after installation. These hosts/sites are often not fully configured from a security perspective before connecting. This lack of secure configuration makes them vulnerable to attacks, which sometimes occur within minutes of connection.[151]

(U) Finally, the explosive growth of the Internet has expanded the need for well-trained and experienced people to engineer and manage the network in a secure manner. Because the need for network security experts far exceeds the supply, inexperienced people are called upon to secure systems, opening still more windows of opportunity for the intruder community.[152]

(U) Outsider Attack Techniques

(U) The typical outsider threatening the computer security of an organization with critical information in its network is a computer "hacker." Once used as a slang term for a computer enthusiast, "hacker" is now largely used to refer to individuals who gain unauthorized access to computer systems for the purpose of stealing or corrupting data. A typical hacker is male, between 16 and 25 years old. Hackers usually become interested in breaking into machines and networks in order to improve their computer skills, or to use network resources for their own purposes. Most hackers are quite persistent in their attacks, possibly because of the amount of spare time the average hacker has.[153]

(U) In addition, there are as many as 1,000 professional hackers worldwide. According to the managing director of the Centre for Infrastructural Warfare Studies, "These are people with hard-core skills. They know exactly what they're doing .... these are highly trained professionals and are way out of the age bracket of the teenage hacker. These people are very difficult to stop. They'll come at you in 10 different ways, not just trying to get through a firewall. They'll steal a password, they'll put 'honey pots' [i.e., very attractive sub-sites] out there to trap passwords, they'll do anything."[154]

(U) A typical hacker attack pattern consists of gaining access to a network user's account, gaining privileged access, and using the victim's system as a launch platform for attacks on other sites or areas of the network. It is possible to accomplish all these steps manually in as little as 45 seconds; with automated software hacking tools, the time can decrease further.[155] Hackers tend to use the following ways to penetrate or damage an organization's computer network:

- (U) **Probing:** A probe is a search initiated at a remote site with the intent of determining potential weaknesses in systems for later exploitation. They are characterized by unusual attempts to gain access to a system or to discover information about the system. One example is an attempt to log in to an unused account. Probing is the electronic equivalent of testing doorknobs to find an unlocked door for easy entry.[156]

- (U) **Scanning:** A scan is simply a large number of probes done using an automated tool. Such tools are available for download at hacker websites on the Internet. Scanning is often a prelude to a more directed attack on systems that the intruder has found to be vulnerable.[157]

[redacted]

- (U) **Compromising an account:** An account compromise is the unauthorized use of a computer account by someone other than the account owner, without involving privileges a system administrator or network manager has. An account compromise might expose the victim to serious data loss, data theft, or theft of services. The damage can usually be contained, but a user-level account is often an entry point for greater access to the system.[158]

- (U) **Compromising a root directory:** A root compromise is similar to an account compromise, except a compromised account has special privileges on the system. Intruders who succeed in a root compromise can do just about anything on the victim's system, including run their own programs, change how the system works, and hide traces of their intrusion.[159]

- (U) **Packet sniffing:** A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travels over the network in clear text. With perhaps thousands of passwords captured by the sniffer, intruders can launch widespread attacks on systems. Installing a packet sniffer does not necessarily require privileged access. For most multi-user systems, however, the presence of a packet sniffer implies there has been a root compromise.[160]

- (U) **Launching a denial-of-service attack:** The goal of denial-of-service attacks is not to gain unauthorized access to machines or data, but to prevent legitimate users of a service from using it. A denial-of-service attack can come in many forms. Attackers may "flood" a network with large volumes of data or deliberately consume all of the channels used to connect with the targeted site. Sometimes an attack is used in conjunction with an intrusion attempt. For example, a denial-of-service attack may be launched against a website, effectively shutting it down or keeping it too busy to communicate with other sites. While the first site is busy defending itself, the hacker sends a message to another site, misrepresenting it as a communication from the disabled site, which may be fully trusted by the other site. The hacker uses this trust to penetrate the targeted site.[161]

The cost of security measures to protect against network weaknesses is normally a small fraction of the cost of having to handle a successful outside attack against an organization.

- (U) **Exploiting Trust:** Computers on networks often have "trust relationships" with one another. For example, before executing some commands, the computer checks a set of files that specify which other computers on the network are permitted to use those commands. If attackers can forge their identity, appearing to be using the trusted computer, they may be able to gain unauthorized access to other computers.[162]

- (U) **Malicious Code:** Malicious code is a general term for programs that, when executed, would cause undesired results on a system. Users of the system usually are not aware of the program until they discover the damage. Malicious code includes Trojan horses, viruses, and worms. Trojan horses and viruses are usually hidden in legitimate programs or files that attackers have altered to do more than what is expected. Trojan horses are programs that hide inside other programs and then execute commands, like ordering a copy of all passwords typed in by the user to be copied stored in a new directory. Viruses are self-replicating programs usually designed to become a nuisance by replicating themselves endlessly until they crowd all available memory out. They usually require action on the part of the user to spread inadvertently to other programs or systems, normally inserting an "infected" diskette into an uninfected machine. Worms are self-replicating programs that are constructed with a built-in strategy to spread themselves to other computers with no human intervention after they are started. These programs can lead to serious data loss, downtime, denial of service, and other security incidents.[163]

(U)The Outsider Target: Network Weaknesses

(U) Most network security incidents exploited by attackers from the outside are made possible by a relatively small number of problems. Most problems can be prevented if adequate defenses are established against these weaknesses. The cost of security measures to protect against network weaknesses is normally a small fraction of the cost of having to handle a successful outside attack against an organization. The following weaknesses are the perennial targets of outside attack:

- (U) **Easy network passwords.** Passwords are the single most important weakness in computer network security. Doing everything else correctly is almost of no value if password security is low. The biggest such problem is an account where the username is the same as the password. This makes the password both easy to remember and easy to guess. The most common occurrences of this problem is the initial password that the system administrators set for an account, with the expectation the user will change it promptly. Often enough, the user doesn't know how to change it or never logs in at all.[164]

- (U) **Duplicate passwords on different machines.** Many years ago, it was reasonable to request that a person to use a different password on each machine or set of machines. With a modern workstation environment, however, it is no longer practical to expect this from a user, and a user is unlikely to comply if asked. At a minimum, users with computer access at another facility should use a different password for their accounts on machines at those facilities. Otherwise, a compromise of a computer at a remote facility could compromise all the computer systems the user has access to. The worst offenders of the "shared password problem" are network maintenance people and teams. Often they want an account on every local area net that they service, each with the same password. That way they can examine network problems and such without having to look up hundreds of passwords.[165]

- (U) **Readable password files.** A readable password file is an accident waiting to happen. It is vital to prevent any user from making and removing a copy of the organization's password file, and it is important to make it as difficult as possible for a user to see the encrypted version of his individual password. A related password problem can arise if there is a game or other lower-level computer application on the network that identifies and stores the records for individual users by allowing them to choose their own passwords. Usually applications do not encrypt the user's password, and there will always be some people who choose their network password as their game password.[166]

- (U) **Old password files.** When a system is backed up or upgraded, several copies of the password file may be created and left in a completely readable state in a forgotten corner of the storage system. Looking for these files is a favorite technique of any hacker who manages to get past the outermost layer of system security.[167]

- (U) **Managers.** Managers, center directors, and other respected people are often given privileged accounts on a variety of machines. They are given these privileges as a sign of respect. Unfortunately, they often are not as familiar with the systems as the programmers and system maintainers themselves. As a result, they often are the targets of attack. Often they are so busy, they do not take the security precautions that others would, and do not have the same level of technical knowledge. They often ignore instructions to change passwords or file protections. Managers should have separate privileged accounts and normal user accounts, with a different password for each.[168]

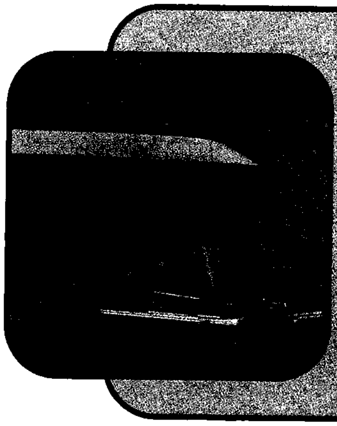
- (U) **Secretaries to managers.** Managers are often so busy or out of the office so frequently that they reveal their passwords to their secretaries, who may make an electronic note of it and inadvertently leave it within easy electronic reach of a hacker. The risk involved can escalate when the manager has a single password that gives him special user privileges.[169]

- (U) **System administrators.** System programmers often add their own security problems. They sometimes create privileged programs that are needed and then forgotten about without being disabled. To make the situation worse, their files and user accounts sometimes are excluded from security audits because they are thought to know better than to create computer security vulnerabilities.[170]
- (U) **Demonstrators.** The one case where it is especially important to have separate accounts or passwords for a single individual is for an employee who travels to give demonstrations. Such an employee may inadvertently reveal his password if he experiences equipment failure while on the road.[171]
- (U) **Well-known security holes.** There are a very small number of security holes in most large systems that are exploited by hackers over and over. Hacker websites publish information about such entry points, and security manager websites in turn post patches and upgrades that patch the holes.[172]

(U) Examples of Attacks by Hackers

(U) In September 1996, Russian hackers apparently succeeded in siphoning about $10 million into foreign bank accounts, but bungled their attempts to extract cash from these electronic, fraudulent deposits. All but $400,000 of the stolen funds was recovered.[173]

(U) In February 2000, the FBI reportedly was investigating a total of 17 distributed denial of service intrusions. The number of reported attacks had quadrupled from the beginning of the month. Four investigations centered on the placing of denial of service tools, known as daemons, on ambushed computers that were later remotely ordered to attack a victim site. Planting daemons on unwitting host computers is a



(U) In March 1997, a juvenile computer hacker disabled a Worcester, Massachusetts, airport control tower and other airport facilities for six hours and disrupted phone service in a neighboring town. The juvenile also hacked into a Worcester pharmacy computer and stole prescription details from a local pharmacist. Both attacks occurred after computer systems were made accessible through the Internet so that system administrators could work remotely.[244]

key step in mounting such an attack. The tools to accomplish these attacks can be downloaded free from Internet websites.[174]

(U) Insider Attack Techniques

(U) For most organizations, the major threat to computers remains internal. Not only is there the possibility that a disgruntled employee will attempt to disrupt the organization's computer files for malice or steal information for personal gain, there is also the possibility that a skilled outsider employed by a competitor may gain employment with the organization and thus become an insider. Inside access, even if as a temporary employee, puts such a person in position to supplement his computer network hacking with HUMINT operations, called "social engineering" by some.

(U) It is axiomatic that in technical systems humans usually are the weakest link. From an OPSEC standpoint, employees will at times take some actions or fail to take others and will make an otherwise secure system suddenly completely vulnerable. For example, sometimes employees will unwittingly facilitate a hacker's efforts by using their organization's Internet portal to visit freeware sites and download games or screen savers. Some of these programs contain Trojan-horse programs that will become active every time the infected machine is booted up and will perform actions to facilitate the covert entry of the hacker. A Trojan-horse program hidden inside a game downloaded from a user's favorite newsgroup might contain instructions to E-mail all the user's files anywhere in the world.[175]

Employees will at times take some actions or fail to take others and will make an otherwise secure system suddenly completely vulnerable.

(U) Countermeasures

(U) A high percentage of computer hackers are opportunists. They tend to operate on either the Internet or on telephone networks. Because they do not have many resources, they tend to bypass organizations that have even a low level of rigorously-enforced security in favor of attacking targets that are "softer."[176]

(U) Web servers are not usually attacked by hackers who want to break through into corporate records systems, unless the "firewall,"—the collection of hardware and software designed to examine a stream of network traffic and service requests—between the systems has been improperly configured. Hackers instead prefer to attack corporate mail servers, which must have access to Internet mail servers in order to deliver mail properly to the corporate clients. Instead of looking for a possible hole in the firewall, they try to widen and exploit existing paths in the mail servers.[177]

(U) Most hacker probes and scans occur during evening hours, when the outsider is more certain to be able to operate without worrying about the presence of systems administrators. Hackers tend to have most of their spare time on the weekends, and their intrusion attacks are usually made then.[178]

(U) While there is not much that the OPSEC manager can do on her own to protect her computer system from extremely technical attacks, there are many things that she can do to protect her network from an attack that is based on HUMINT security lapses or on a combination of computer hacking and "social engineering."

(U) OPSEC managers and personnel can take the following steps to help reduce the risk of damage to their organizations through computer security incidents:

- (U) **Secure all access points between an internal network and the outside world.** Hackers will find and attack the weakest and most easily exploitable point of a network. Usually this is the initial point of contact within the company, its computer network. One way to prevent corporate information from "leaking out" is to ensure that Internet terminals are completely separated from the company's other computer systems. Without a direct link to the company's operating systems, a potential hacker will only get into the company's Internet computer and not its core computer system. When risk is assessed as too high, the only safe connection to the Internet is none at all.[179]

- (U) **Develop a security policy for each system.** Users must know what is allowed and what is not, which applications may be run and which not, and who is allowed access and who is not. The basis for this should be an OPSEC risk analysis that identifies the organization's assets, the threats that exist against those assets, and the costs of asset loss. This policy should also cover contingencies such as guidelines for reacting to a site compromise (e.g., how to deal with the media and law enforcement, and whether to trace the intruder or shutdown and rebuild the system).[180]

Hackers will find and attack the weakest and most easily exploitable point of a network.

- (U) **Ensure all user accounts have a password.** Also, the passwords should not be easy to guess. There is software available to analyze the security of a network's passwords.[181]

- (U) **Regularly check the integrity of system software.** There are a number of software tools available at Internet computer security websites with the latest version of system-integrity analysis programs. OPSEC managers should also check security archives periodically for security alerts and technical advice.[182]

- (U) **Keep network systems up to date with upgrades and patches.** Each major operating system has its own characteristic security weaknesses. Hackers regularly confer to trade information on these as they are identified. System programmers also issue upgrades to fix problems as they are identified.[183]

- (U) **Audit systems and networks, and regularly check user logs.** Information resources should be as comprehensive as practicable. Many organizations victimized by hackers or insiders later find that they have kept insufficient track of the activities of their users and are unable to completely understand how they were victimized.[184]