PART 1

Digital Espionage, Warfare, and Information Security (INFOSEC)

In Chapter 1, the interesting concepts of *Digital Espionage* and *Digital Warfare* are introduced. The family of computer security countermeasures known as INFOSEC is discussed. All computer information is vulnerable to a variety of attacks. A primary theme of this book is that information security (INFOSEC) countermeasures are reasonable and prudent technologies to thwart *Digital Espionage* and *Infocrimes* perpetuated by a host of bad guys we encounter: *Hackers, Crackers, Spies,* and *Thieves.* As a corollary, poorly implemented INFOSEC technologies provide fertile ground for the practice of *Digital Espionage* in corporate and military theaters. We attempt to profile the computer criminal and present some primary tools that investigators have at their disposal to prosecute them. Since encryption is a primary weapon in the INFOSEC arsenal, it is introduced at this junction.

In Chapter 2, traditional INFOSEC goals are persented. We review some of the serious consequences that occur when INFOSEC technologies are inappropriately applied. Finally, Donn Parker's brilliant extensions to the traditional INFOSEC theory are reviewed.

CHAPTER 1

Introduction to Digital Espionage

Digital Espionage (DE)—What It Is and What It Represents

Infocrime refers to any crime where the criminal target is *information. Digital espionage* (DE) is the *specific-intent infocrime* of attacking, by computer means, personal, commercial, or government information systems and assets for the purpose of theft, misappropriation, destruction, and disinformation for personal or political gain. This crime has become an enormous problem with the growth of the Internet. The authors' definition of digital espionage represents a compendium of activities. DE is really a *family* of specific-intent infocrimes. The logical questions are as follows: how big is the family, what really is a computer crime, why and how does it occur, and most importantly, how does one prevent a computer crime from occurring? How important is it that the main thrust of the attack is against information assets?

The advent and growth of the Internet has made digital espionage a real and potential danger of enormous magnitude. The average computer user is still blissfully unaware of this danger, but digital espionage has already begun to affect the general public, as well as corporations and government agencies. Corporate management has also been slow to recognize and react to the specter of digital espionage. Most existing security systems reflect a concern for short-term profit or reaction to a specific breach of security in the past. The need to educate employees about the protection of intellectual property is rarely seen as a high-priority item. Many security initiatives are delayed until the manager is dealing with crisis rather than appropriate planning and security policies. Each new security crisis usually induces a similar limited reaction, without any consideration of the more general problem within which any one incident is only an immediate example.

Scope of Computer Crime (Infocrime)

The scope of computer crime is difficult to quantify. Public reports have estimated that computer crime costs us between $500 million and $10 billion per year.[1] A survey performed jointly by the Computer Security Institute (CSI) and the Federal Bureau of Investigation's Computer

Crime Division found that nearly half of the 5000 companies, federal institutions, and universities polled experienced computer security breaches within the past 12 months. These attacks ranged from unauthorized access by employees to break-ins by unknown intruders. The study found that:[2]

- The problem is growing.
- The greatest problem is insider attacks.
- Identified computer crime accounted for over $100 million in losses in 1996.

In addition, a WarRoom Research, Inc. survey of 236 respondents showed major underreporting of security incidences related to computers:[3]

- 6.8 percent always reported intrusion
- 30.2 percent only report if anonymous
- 21.7 percent only report if everyone else did
- 37.4 percent only report if required by law
- 3.9 percent only report for "other reasons, including protect self"

According to a recent U.S. Department of Justice presentation,[4] some examples of systems and facilities that were seriously hit are as follows:

- U.S. Marshals system—Alaska
- U.S. District Court system—Seattle
- NASA attack—Houston
- Military systems—Gulf War
- Organ Transplant Hospital—Italy
- Power companies
- 911 systems

Furthermore, in 1996 the National Security Agency (NSA) reported over 250 intrusions into DoD systems. The consequences from these computer attacks were labeled as *devastating*.

Research by Barbara D. Ritchey at the University of Houston presents another view: computer crimes account for losses of more than $1 billion annually and those computer criminals manifest themselves in many forms, including coworkers, competitors, and "crackers."[5] The Computer Security Institute of San Francisco also surveyed 242 separate Fortune 500 companies concerning Internet security and found that in 1995 only 12 percent of the companies reported losses as a result of system pene-

tration totaling losses of $50 million. In terms of dollar value, the average theft costs a company $450,000 for each incident.

In 1996, *Information Week* magazine conducted its third annual survey in conjunction with Ernst and Young. The survey queried 1290 respondents, almost one-half of which said they suffered a financial loss related to information security in the last two years. At least 20 percent of the 1290 respondents stated their information security losses came to more than $1 million each. Additional loss information acquired from the Ernst and Young survey is that one in four U.S. companies has been a victim of computer crime, with losses ranging from $1 billion to $15 billion.[6]

From 1990 through 1995, the number of computers in the world increased tenfold, from 10 million to 100 million. In 1990, 15 percent of the computers were networked, and by 1995, 50 percent, or almost 50 million computers, were hooked together. From 1995 to 1999 the number of connected computers is estimated to have grown to over 250 million.

Theft of trade secrets is one of the most serious threats facing business today. The latest CSI/FBI Computer Crime and Security Study, released in March 1999, found that of the 12 types of computer crime and misuse, theft of proprietary information had the greatest reported financial losses for the period 1997 to 1999. According to the survey, more than $42 million worth of trade secrets were stolen from 64 organizations that were able to quantify their losses from this type of breach.[7] Reported losses in 1998 ranged from $500 to $500,000. Penetration attacks by "outside" sources were 18 percent of the organizations reporting in 1997 and 21 percent of those reporting in 1998.[8]

The Federal Computer Incident Response Center reported 244 incidents involving government sites from October 1996 through October 1997. Of those, 92 (38 percent) were intrusion incidents, 83 (34 percent) were probes, 37 (15 percent) were computer viruses, 22 (9 percent) were e-mail incidents, 4 (2 percent) were denial of service incidents, 2 (1 percent) were malicious code incidents, 2 were misuse incidents, and 2 were scams. One particularly sensitive intrusion ran over several months and involved more than 10,000 hosts. Hackers gained root access in several of the incidents.[9]

The National Police Agency of Japan received reports of 946 cases involving hacking during the first six months of 1997. This was a 25 percent increase over the first six months in 1996. The Australian Computer Emergency Response Team reported a 220 percent increase in hacker attacks from 1996 to 1997.[10]

Networking has helped technology increase exponentially. With these cultural changes, the need for heightened security has also increased. A computer criminal formerly was able to attack systems at only one loca-

tion, giving administrators the advantage of protecting one site. In today's client/server environment, network administrators are fighting a very different battle. They are subject to attacks at every access point on their network, from a modem port to a laptop on an airplane headed for Paris. The Internet poses its own share of unique problems in that never before have so many computers been hooked together.[11]

The Criminal Playground

Computer crimes take several forms including sabotage, revenge, vandalism, theft, eavesdropping, and even "data diddling," or the unauthorized altering of data before, during, or after it is input into a computer system. Computers can be used to commit such crimes as credit card fraud, counterfeiting, bank embezzlement, and theft of secret documents. The physical theft of a disk storing 2.8 MB of intellectual data is considered data theft. Logging into a computer account with restricted access and being caught there or purposely leaving evidence in the form of a message with an explanation of what has been done are examples of data diddling. A traveling employee who leaves his or her computer unattended while on an airplane, only to discover an empty drive slot to the tune of lost billing information, marketing plans, and/or customer data, can be considered inattentive, but this type of incident is steadily increasing.

Another type of computer crime involves electronic funds transfer or embezzlement. The first person convicted under the Computer Fraud and Abuse Act was Robert T. Morris Jr., who, as a Cornell graduate student, introduced a "worm" into the Internet. These "worms" float freely through the computer environment, attacking programs in a manner similar to viruses. Some would consider this an act of vandalism. By multiplying, the worm interfered with approximately 6200 computers. Morris was sentenced to three years' probation, ordered to pay a $10,000 fine, required to perform 40 hours of community service, and required to pay $91 per month to cover his probation supervision.

Computers can play three different roles in criminal activity. First, computers can be *targets* of an offense; for example, a hacker tries to steal information from or damage a computer or computer network. Other examples of this behavior include vandalism of Web sites and the introduction of viruses into computers.

Second, computers can be *tools* in the commission of a traditional offense, for instance, to create and transmit child pornography. COMSEC

Solutions composed an interesting list wherein the computer was used as a tool to facilitate the following crimes:[12]

- Drug trade
- Illegal telemarketing
- Fraud, especially false invoices
- Intellectual property theft
- "True face" or ID theft and misrepresentation
- Espionage, both industrial and national
- Conventional terrorism and crimes
- Electronic terrorism and crime
- Electronic stalking
- Electronic harassment of ex-spouses
- Inventory of child pornography
- Bookmaking
- Contract repudiation on the Internet
- Cannabis smuggling
- Date rape
- Gang crimes, especially weapons violations
- Organized crime
- Armed robbery simulation
- Copycat crimes
- Pyramid schemes
- DoS (denial of service) attacks
- Exposure or blackmail schemes
- Revenge and solicitation to murder of spouses
- Hate crimes
- Web site defacement (automated)

Third, computers can be *incidental* to the offense, but still significant for law enforcement purposes. For example, many drug dealers now store their records on computers, which raises difficult forensic and evidentiary issues that are different from paper records.

In addition, a single computer could be used in all three ways. For example, a hacker might use his or her computer to gain unauthorized access to an Internet service provider ("target") such as America Online,

and then use that access to illegally distribute ("tool") copyrighted software stored on the ISP's computer-server hard drive ("incidental"). COMSEC Solutions composed another interesting list where the computer was an incidental part of computer crime. These included hacking, data theft, diddling, alteration and destruction, especially involving financial or medical records, spreading viruses or malicious code, misuse of credit and business information, theft of services, and finally, denial of service.

Internet service providers (ISPs) and large financial institutions are not the only organizations that should be concerned about computer crime. Hackers can affect individual citizens directly or through the person's ISP by compromising the confidentiality and integrity of personal and financial information. In one case, a hacker from Germany gained complete control of an ISP server in Miami and captured all the credit card information maintained about the service's subscribers. The hacker then threatened to destroy the system and distribute all the credit card numbers unless the ISP paid a ransom. German authorities arrested the hacker when he tried to collect the money. Had he been quiet, he could have used the stolen credit card numbers to defraud thousands of consumers.[13]

Government records, like any other records, can be susceptible to a network attack if they are stored on a networked computer system without proper protections. In Seattle, two hackers pleaded guilty to penetrating the U.S. District Court system, an intrusion that gave them access to confidential and even sealed information. In carrying out their attack, they used supercomputers at the Seattle-based Boeing Computer Center to crack the courthouse system's password file. If Boeing had not reported the intrusion to law enforcement, the district court system administrator would not have known the system was compromised.[14]

The computer can also be a powerful tool for consumer fraud. The Internet can provide a con artist with an unprecedented ability to reach millions of potential victims. As far back as December 1994, the Justice Department indicted two individuals for fraud on the Internet. Among other things, these persons had placed advertisements on the Internet promising victims valuable goods upon payment of money. But the defendants never had access to the goods and never intended to deliver them to their victims. Both pleaded guilty to wire fraud.[15]

Personal computers can be used to engage in new and unique kinds of consumer fraud never before possible. In one interesting case, two hackers in Los Angeles pleaded guilty to computer crimes committed to ensure they would win prizes given away by local radio stations. When the stations announced that they would award prizes to a particular caller—for example, the ninth caller—the hackers manipulated the local

telephone switching network to ensure that the winning call was their own. Their prizes included two Porsche automobiles and $30,000 in cash. Both miscreants received substantial jail terms.[16]

In another interesting case that raises novel issues, a federal court in New York granted the Federal Trade Commission's request for a temporary restraining order to shut down an alleged scam on the World Wide Web. According to the FTC's complaint, people who visited pornographic Web sites were told they had to download a special computer program to view the sites. Unknown to them, the program secretly rerouted their phone calls from their own local Internet provider to a phone number in Moldova, a former Soviet republic, for which a charge of more than $2 a minute could be billed. According to the FTC, more than 800,000 minutes of calling time were billed to U.S. customers.[17]

Internet crimes can be addressed proactively and reactively. Fraudulent activity over the Internet, like other kinds of crimes, can be prevented to some extent by increased consumer education. People must bring the same common sense to bear on their decisions in cyberspace as they do in the physical world. They should realize that a World Wide Web site can be created at relatively low cost and can look completely reputable even if it is not. The user should invest time and energy to investigate the legitimacy of parties with whom they interact over the Web. Just as with other consumer transactions, we should be careful about where and to whom we provide our credit card numbers. The legal maxim *caveat emptor* ("let the buyer beware"), which dates back to the early sixteenth century, applies with full force in the computer age.

The public can also be protected by vigorous law enforcement. Many consumer-oriented Internet crimes, such as fraud or harassment, can be prosecuted using traditional statutory tools, such as wire fraud. Congress substantially strengthened the laws against computer crime in the National Information Infrastructure Protection Act of 1996. The law contains 11 separate provisions designed to protect the confidentiality, integrity, and availability of data and systems.

Novel Challenges: Jurisdiction and Identity

The Internet presents novel challenges for law enforcement. Two particularly difficult issues for law enforcement are *identification* and *jurisdiction*.

One of the benefits of the global Internet is its ability to bring people

together, regardless of where in the world they are located. Boundaries are virtual, not real. This can sometimes have a subtle impact for law enforcement. For example, to buy a book, you used to drive to the local bookstore and have a face-to-face transaction; if the bookseller cheated you, you went to the local police. But the Internet can make it easier and cheaper for a consumer to make purchases, without even leaving his or her home, from a distributor based in a different state or even a different country. And if the consumer pays by credit card or, in the future, electronic cash, and then the book never arrives, this simple transaction may become a matter for the federal or even international law enforcement community, rather than a local matter. There are issues of *trust* that concern both the merchant and the customer.

The Internet makes interstate and international crime significantly easier in a number of respects. For example, a fraudulent telemarketing scheme might be extremely difficult to execute on a global basis because of the cost of international telephone calls, the difficulty of identifying suitable international victims, and the more mundane problem of planning calls across numerous time zones.[18] But the Internet enables scam artists to victimize consumers all over the world in simple and inexpensive ways. An offshore World Wide Web site offering the sale of fictitious goods may attract U.S. consumers who can "shop" at the site without incurring international phone charges, who can be contacted through e-mail messages, and who may not even know that the supposed merchant is overseas. The Moldova phone scam demonstrates the relative ease with which more-complex international crimes may be perpetrated. In such a global environment, not only are international crimes more likely, but some consumer fraud cases traditionally handled by state and local authorities may require federal action.

Another fundamental issue facing law enforcement involves proving a criminal's identity in a networked environment. In all crimes—especially information-based infocrimes—the defendant's guilt must be proved beyond a reasonable doubt, but global networks lack effective identification mechanisms. Individuals on the Internet can be anonymous, and even those individuals who identify themselves can adopt false identities by providing inaccurate biographical information and misleading screen names. Even if a criminal does not intentionally use anonymity as a shield, it is easy to see how difficult it could be for law enforcement to prove who was actually sitting at the keyboard and committing the illegal act. This is particularly true because identifiable physical attributes such as fingerprints, voices, or faces are absent from cyberspace, and there are few mechanisms for proving identity in an electronic environment.

A related problem arises with the identity of the victim. With increasing frequency, policymakers are appropriately seeking to protect certain classes of citizens, most notably minors, from unsuitable materials. But if individuals requesting information can remain anonymous or identify themselves as adults, how can the flow of materials be restricted? Similarly, if adults can self-identify as children and lure real children into dangerous situations, how can these victims be protected? In 1999, Congress, in response to this problem, enacted the Communications Decency Act. The act did not pass its first federal court challenge. The federal court found the act to be exceedingly vague.

One area that raises both identification and jurisdictional issues is Internet gambling. The Internet offers several advantages for gambling businesses. First, electronic communications, such as electronic mail, allow for simple record keeping. Second, the Internet is far cheaper than long-distance and international telephone service. Third, many software packages make it easy to operate consumer businesses over the Internet. Use of the Internet for gambling—as well as for other illegal activities such as money laundering—could increase substantially as the use of "electronic cash" becomes more commonplace.[19]

Existing federal law governs gambling on the Internet. Interstate gambling by the use of any wire communication facility, including the Internet, is illegal unless the gambling activity is legal in both states. Even where gambling is legal, it is legal only for adults. Therefore, the legality of gambling depends critically on both the location and the age of the participants, neither of which can be verified reliably through current network mechanisms, especially when the participants are not willing to cooperate. Congress has already established the National Gambling Impact Study Commission to study a variety of issues, including "the interstate and international effects of gambling by electronic means, including the use of interactive technologies and the Internet."[20]

Digital Warfare

Certain futurists predict that the next U.S. war will involve the injection of malicious code into Pentagon computers and the blitzing of telecommunication and financial networks through use of a modem. This information war can be conducted by attacks on software in lieu of hardware, such as targeting the Federal Reserve software versus the Federal Reserve headquarters building, taking power grids off-line in Kosovo rather than bomb-

ing a hydroelectric plant, crashing the air traffic control computers instead of hijacking a plane, activating a virus within SPADOC (Space Defense Operations Center) computers or NORAD/USSPACECOM I & W (the Integrated Warning Division at the U.S. Space Command Headquarters in Cheyenne Mountain, Colorado, responsible for alert, warning, and verification of potential hostile space-related events), and blinding satellite communications versus theft of a nuclear weapon.

Approximately 33 countries are perfecting information war attack strategies, and the U.S. Department of Defense is developing combat viruses, logic bombs, electromagnetic pulse weapons, and other classified technology designed to "fry" circuit boards, crash networks, and alter an enemy's weapons control software so that bombs miss their intended targets. The outlay in the Department of Defense's information security budget is approximately one-twentieth the cost of a B-2 bomber.[21]

Of several possibilities, Dr. Dorothy Denning describes a future warfare scenario in which military operations take place almost exclusively in cyberspace. Under this scenario, wars will be fought without armed forces. Instead, trained military hackers will break into the enemy's critical infrastructures, remotely disabling communications, command, and control systems that support governmental and military operations. Operations might also target key civilian and commercial systems, such as banking and finance, telecommunications, air traffic control, and power supply. At present, however, there is no evidence to support the notion that a country's infrastructures could be so disabled by hacking that a government would surrender to a foreign power or alter its policies. The fallout from such an attack and how it would affect the decision-making systems of the enemy are unknown. Launching it would require considerable knowledge about target systems and interconnectivities.[22] (Recognize that this is a primary motive for digital espionage activities. Note the interesting line between the criminal aspect of DE and the military offensive, hence sanctioned, use of DE. In the first case you go to jail. In the second case, you are decorated or if you are on the opposing side, you go to jail.) As a counterpoint, DE activities against U.S. national security information are a serious crime.

The Digital Espionage Family

Focusing on computer-related and computer-facilitated crime issues in the following, we have slightly amended the U.S. Department of Justice

(USDOJ) Criminal Division's view; the digital espionage family has been broadly divided into:

Computer-Related Crime

- Intrusion or malicious hacking
- Theft of service
- Denial of service (DoS)

Computer-Facilitated Crime

- Espionage: theft of national security information
- Economic espionage: theft of trade secrets
- Worldwide distribution of pornography and its associated kidnapping and/or physical molestation
- Fraud, including pyramid schemes and bait and switch schemes
- Theft and embezzlement

The rationale behind this familial ordering is the potential for financial loss. The potential is enormous. The USDOJ recorded at least two cases that incurred multimillion dollar losses.[23] Computer-related crimes catch the public with their eyes closed—for example, the California radio contest mentioned previously.[24] Banks and securities firms will tell you that information about money or the movement of money is more valuable than money itself. It is also the measure that allows for successful prosecution of computer-related crimes.[25] The value and movement of money is used to comply with evidentiary requirements of the various federal statutes.

Portrait of the Computer Criminal—Targets of Opportunity

Computer criminals manifest themselves in many forms. Many company security officers believe that the weakest element in the computer cycle is the disgruntled or simply lazy employee. Conversely, the preeminent danger to a company's intellectual property (trade secrets, R & D plans, pricing lists, customer information) is other companies. "Competitors are the single greatest threat in computer crime," according to Richard Power of Computer Security Institute in San Francisco. Insiders steal corporate data to boost their income. Competitors may be the primary threat, but the insiders perform the dirty work.

A CSI/FBI survey found that insiders were involved in 46 percent of

electronic espionage cases. When trying to identify the insider who has perpetrated a fraud, look for the disgruntled employee who is making points for himself or herself with a future employer. The American Society for Industrial Security (ASIS) estimates the loss from theft of intellectual property to the U.S. industry to be approximately $2 billion per month.[26]

Numbers like the previous example may leave the manager cold. They are not personal enough. During the writing of this book, one interviewee at a large company, who required anonymity, gave a different point of view:

> If someone steals our manager's personalized pen set, given to him by the president for success of our division in sales, every employee hears about it and security for the area is substantially upgraded. But when someone steals from our computer [network] key documents for marketing of [a new toy], which may or may not be successful via a campaign with a fast food chain, and *valued by accounting at five million,* based on labor costs and equipment depreciation, et cetera, you will be lucky if you get to talk to the manager's secretary. You will be even luckier if he springs for some intrusion detection software, and luckier still if he approves the *ten thousand* needed to install VPN [virtual private network] secure gateways between our trading partners and customer sites. And, bringing the security solution to him makes me the prime suspect.[27]

As long as there have been computers, there have been *hackers.* Until recently being a hacker was not considered a dirty word. Now hackers are mild peppers compared to *crackers.* The difference is that hackers are performing break-ins for the thrill of it, and crackers are breaking in for the financial rewards involved.

This is not the only way in which computer crimes occur. Some *thieves,* on the other hand, do not bother to break into the computer via the hacker method; they just steal the entire hardware ensemble, server and all. Organized gangs are known to steal chips and components. Traditionally, computer chips have been stolen from suppliers and assemblers that would have the chips on hand. Criminals are now stealing computer chips by dismantling the computer to get them or carrying off the entire computer.

And then we have the traditional *spies.* Their targets may be any of a variety of treasures: SIOPS (Single Integrated Operational Plans—used to tie together military nuclear weapons and regional plans from the Atlantic, the Pacific, and Europe), commercial marketing plans, military or diplomatic ESI (Extremely Sensitive Information), or personal data on political or sports figures, and so on. No matter what we call them—hackers, crackers, spies, or thieves—they are breaking the law and vio-

lating your property and rights. It is your responsibility and duty to stop them. It is your right to protect your personal data, your computers, your company's data, or your organization's information. We trust this book will provide some tools to assist you to achieve these security goals.

Another type of "computer criminal" are *T*iger *T*eams. These are teams assembled by the U.S. Army to perform *legal* and *permitted* surprise attacks on computer systems to test the security of the systems and support structures. One researcher reports that in one year tiger teams attacked 8932 systems and penetrated 7860 of them. Only 390 of these attacks were detected and 19 reported.

Tiger teams are also hired by private industries to break into their computers to test their security programs. The main problem in computer crimes is not the crime itself but the detection of the break-in because there are few tools to trace the criminal's path through the network. Tiger teams have been around since the 1960s when the NSA used them to check the security of its own computer systems. NSA's judgment of the results was mixed because the problem was a moving target and solutions found were temporary.[28]

The perceived anonymity of the act of computer crime and the huge financial gain involved lead individuals to do things that they would not normally do. The belief that they will not be detected is the basis for many crimes. An otherwise upstanding executive would not dream of looking into the briefcase of a competitor but has no problem perusing their computer files. As more and more global businesses join the World Wide Web, the motive to commit computer crimes increases. Companies that spend billions on research and development, which if performed successfully by a competitor would allow the competitor to catapult ahead in technology, are especially susceptible.

Network administrators are another source for the rise in computer crimes. Many individuals blame the Internet and new connections that create back doors for crackers, but professional hackers who test networks say that security is too lax due to the network administrator's complacency.

Failure to monitor security programs that are implemented allow crackers to infiltrate and often remain undetected. The former coworker, now referred to as an ex-employee, poses a unique threat. The termination of an employee, disgruntled or otherwise, is too often handled by a manager who fails to notify the network administrator. This oversight creates a huge hole through which that ex-employee could breach security.

Social engineering—that is, contacting company employees and acquiring sensitive information by posing as a friendly—is often

employed by computer criminals to gain important information such as passwords. Annual reports for companies are a wealth of information when looking for connections. Much like a burglar guesses the combination to a safe by viewing how long it takes to open between turns or numbers, a computer cracker can read the cryptographic key by timing the computer as it decrypts a message.

Other threats to networks include firewall and system probing, network file systems application attacks, vendor default password attacks, spoofing attacks, sniffing attacks, easy-to-guess password compromise, destructive computer viruses, prefix scanning, and Trojan horses. Programs that were initially built for the network security specialists are now being used by crackers to break into networks. "Crack," a brute-force program, was designed for network security officers to test for easy-to-guess passwords. This program attacks the computer by trying every dictionary word as a possible password.

The network file, which is used to share files between systems, is exploited through well-known vulnerabilities. Crackers use vendor-installed passwords to infiltrate systems. "Spoofing" involves faking the Internet Protocol (IP) address to appear as if a friendly computer is involved. "Sniffing" is literally a program that sniffs all traffic on a network to collect authorized passwords. "Prefix scanning" involves scanning telephone company phone lines for modem lines. This detection is especially damaging because most modem lines bypass firewalls and security. Trojan horse programs are also aptly named. This is a program that will install "backdoor" programs, allowing unrestricted access into the internal systems by bypassing the monitoring and auditing process. Crackers inform other crackers of the existence of these programs via Web sites.

Mainframe computer security was relatively simple in that the physically large disk drives were secured behind locked doors and direct access could be denied to the attackers. In the current client/server environment, physical and information security is complex. More individuals than before have access to the server where programs and data are stored. Laptop computers, which in some cases are more powerful than old mainframes, fly around the world with businesspeople. Internet connections, if connected to the company's main server, pose an original challenge in that literally millions of people are able to access the computer. Computer systems that cannot provide adequate information security to protect data from intruders are not acceptable. Surveys produce huge estimates of dollar losses resulting from system penetration, but the truth of the matter is that these figures represent only a small portion of the actual losses,

because the average business usually is not aware of the penetration and therefore has no idea the store is being robbed.

The USDOJ Criminal Division suggests that computer criminals intrude because of their curiosity or pride in their ability to use the computer as a gateway or launching pad for more-advanced attacks; their ability to destroy things, such as rerouting calls (including 911) and shutting down power systems in order to cause mayhem in a hospital; their desire to eliminate or destroy personnel data (in one case, convincing the VA that a soldier was dead when in fact he was very much alive—and, we suspect, pretty angry); and finally, their ability to commit digital espionage against industrial, national, or personal targets.[29]

Portrait of the Computer Criminal—Who Are They?

It would be nice if we could identify the computer criminal by traits. In general terms we can. Let's start with the hacker. According to J.P. Barlow, "When a hacker perceives a computer or an automated information system (AIS) is poorly protected, he sees a challenge. Hacking to him is an art. He perceives himself as having an obligation to break into any system that can be broken into."[30] Peter Pitorri, an expert in counterespionage, presents this portrait of a typical hacker, based on Barlow's original work:[31]

Portrait of a Hacker, Circa 1991

- Lacking in moral values
- Well educated
- Male
- Between 15 and 37 years of age
- Lacking in self-esteem
- Passively resistant to authority
- Disdainful of the law
- Disdainful of the rights of others
- Disdainful of loyalty
- Devious
- Narrow minded, finely focused
- Introverted

- Highly intelligent
- Patient
- Social deviate, in that he seems incapable of empathy, genuineness, warmth, defined personal goals, and respect for societal norms
- Usually an authorized user of the system he has attacked.

Pitorri concludes that persons fitting this profile represent a clear and present threat to the firm that employs them.

In May 1999, COMSEC Solutions, a cryptographic, anti-virus, and biometrics countermeasures firm, presented its own research at the FBI National Academy at Quantico, Virginia:[32]

Typical Profile of the Corporate Computer Criminal

- Male, white, young (19 to 30 years of age)
- Has no prior record
- Identifies with technology, not his employer
- Employed in information systems or accounting
- Bright, clever, self-confident, adventurous
- Accepts challenges and is motivated by them
- Feels exploited by his employer and wants to get even
- Does not intend to hurt people, just feels cold indifference to his employer
- Believes that deceiving the establishment is fair game
- Uses drugs or alcohol
- Feels resentment for having been passed over for promotion
- Feels resentment due to pay inequality with peers and friends
- Believes the challenge is to beat the system, although not necessarily for monetary reward
- Has a proclivity for high living
- Has financial pressures
- Is divorced (sometimes multiple)
- Has a desire to impress a new boyfriend or girlfriend (especially for homosexual relationships)
- Is chronically late—especially with reports

These profiles are based on known cases, and the traits represent an

analysis of identified repeating factors. Lest we encourage the idea that this is an exact science, we refer the reader to several additional sources: *Fighting Computer Crime* by Donn B. Parker, *Information Warfare and Security* by Dorothy E. Dennings, *Corporate Espionage* by Ira Winkler, and *Corporate Intelligence and Espionage* by Richard Eells and Peter Nehemkis.[33,34,35,36] The interested reader will soon find that the profiles are not straightforward; human interactions and motivations are very complex. It is also interesting that as of this writing, no females have been charged with the commission of a newsworthy computer crime.

Motive, Opportunity, Means, and Method (MOMM)

In the twenty-first century almost all crime against property will be perpetrated within computer systems—hence, the name *computer crime* or, more descriptively, *infocrime*. Many other crimes, even violent ones, will be controlled or directed by computers, because computers play the central role in storing and processing the assets of individuals and organizations and in directing the activities of enterprises. Exactly what the term "computer crime" encompasses can be hard to pin down. There are 50 states, as many different laws, and at least as many definitions. And there are federal laws that do not coincide with the state laws, and international laws that do not address the virtual boundaries that exist with computer crimes. Along with confusing politics and legal definitions, organizational victims generally do not want to prosecute the perpetrator because of adverse public relations. Some companies, stinging from a theft or break-in of their computer systems, actually pay the bad guy to keep his mouth shut and to show them how he did it. Computer crime is difficult to prosecute because the offenders generally know a great deal more about computer technology than do prosecutors and judges. However, this is changing.

In 1996 the USDOJ formed the Computer Crime and Intellectual Property Section (CCIPS) to neutralize the problem. The section works with a coordinator for computer and telecommunications in each U.S. attorney general's office. The FBI created the Computer Investigations and Infrastructure Threat Assessment Center (CIITAC), in 1996, adding six computer crime squads in New York, Washington, DC, Seattle, San Francisco, Los Angeles, and Boston, and a seventh in Dallas in 1998.

Every FBI field office now employs a CIITAC agent. They also have forensic computer examination personnel in most field offices and a special team at Quantico, Virginia.

Investigators who will prosecute a computer crime normally look for motive, opportunity, means, and method (MOMM). *Motive* includes personal causation, such as economic, ideological, egocentric, or psychotic. *Opportunity* usually refers to a lapse in system controls (such as internal or access controls) or management controls (such as rewards, ethics, or trust) that permits penetration of the system. *Means* refers to the ability to compromise controls, personnel, and technology. *Methods* may include falsifying or destroying input, throughput, and output, as well as time and access logs.

Let's elaborate upon the material behind COMSEC Solutions' Typical Profile of the Corporate Computer Criminal. The following list presents several factors that invite or encourage computer crime in established corporations:

Factors that Encourage Computer Crime—Motivations

- Inadequate rewards: pay, fringe benefits, bonuses, incentives, perquisites, job security, enrichment, promotional opportunities
- Inadequate management controls: failure to communicate minimum standards of performance or on-the-job personal behavior
- Ambiguity in job roles, relationships, responsibilities, authority, and accountability
- Inadequate reinforcement or performance feedback
- Lack of recognition for service, good work, longevity, and effort
- Lack of recognition for truly outstanding performance
- Delayed or no performance feedback
- Delayed discussions about performance inadequacies or behaviors
- Failure to counsel or mentor when performance is below expectations
- Lack of job challenge or rotation
- Inadequate management support
- Lack of adequate resources meeting minimum requirements
- Failure to audit, inspect, or follow through to ensure compliance with company goals and norms
- Tolerance of antisocial behavior such as alcohol or drugs

- Fostering hostility, interdepartmental competitiveness, or bias in selection, promotion, or pay

The following lists add the dimensions of personal inducement and prevention:

Factors that Enhance the Probability of Computer Crime—Personal Inducements

- Inadequate standards of recruitment and vetting [British term that means to subject a person to an appraisal via a background investigation]
- Inadequate orientation and training on security matters
- Unresolved financial or social problems
- Failure to, for sensitive positions, screen and verify past employment, education, financial reliability, and character
- Job-related stress or anxiety

Factors that Discourage Computer Crime—Prevention

- Separation or rotation of duties
- Periodic audit and surprise inspections
- Clear written statements of policy and procedures
- Encryption hash totals and digital signatures (discussed in Chapters 7 and 9)
- Internal accounting controls: dual signature authorities, dollar budget limits, renewable check authority
- Offline entry controls and limits

The following lists add the dimensions of access controls and detection systems:

Factors that Discourage Computer Crime—Access Controls

- Identification defenses: key or card inserts, passwords, code phrases, challenge-response; exclusion and lock-out; time activator,
- Forced password length rather than user choice and frequent changes
- Authentication defenses: random personal data, biometrics, including voice, palm, iris, and/or fingerprint recognition
- Level of authority access permissions
- Need to know by using Special Compartmented Information (SCI)

Factors that Discourage Computer Crime—Detection

Exception Logging Systems

- Out-of-sequence runs and entries
- Improper order of priority of runs and entries
- Aborted runs and entries
- Out-of-pattern transactions: too high/low/many/often/few unusual file accesses
- Wrong password, entry code parity, and redundancy checks against repeated attempts to gain access improperly

Management Info Systems

- Monitoring operational performance levels for variations from plans and standards, deviations from accepted or mandated policy and procedures, and deviations from past quantitative relationships or performance norms

Intelligence Gathering

- Monitoring employee attitudes, values, and job satisfaction levels
- Soliciting random feedback from customers, vendors, and suppliers for evidence of dissatisfaction, inefficiency, and inconsistency with policies, corruption, or dishonesty by employees.

Computer criminals commit their crimes when opportunity equates to knowledge and access. Hackers have a surprising level of knowledge of communications protocols, applications programs, operating systems, database and file management systems, and accounting procedures. Access can be either physical or electronic and is the most important element in the equation. The following lists explain technical and malicious code attacks that may be used to gain access and then extend the access into the system. A good description of each of these attacks can be found in Diane E. Levine's seminal paper, "Virus and Related Threats to Computer Security," in *Computer Security Handbook*.[37]

Methodology—Obtain Access

- Masquerading as a user or being falsely identified and authenticated as a network hardware device
- Forging of credentials and passwords
- Port scanning
- War dialing

- Wiretapping
- Optical spying
- Installing bugs
- Reading electromagnetic emanations
- Scavenging outputs
- Simulating targets
- Keystroke stealing
- Deception
- Corruption of programs or database
- Guessing and dictionary attacks
- Object reuse
- Exploiting insecure terminal
- Piggybacking a valid job
- Tailgating
- Between-the-lines entry
- Exploiting bugs and getting user identification

Once the intruder has access, he or she exploits it to gain privileges. Then the intruder uses the access to destroy data. The following lists explain the process in more detail:

Extending Access

- Browsing
- Covert channeling
- Trap-door entries
- Back doors—using bypass programs
- Superzapping with utility programs to violate controls
- Becoming a "superuser" and attacking the network "root" structure
- Synchronous attacks in privileged mode
- Brute-force password attack
- Social engineering

The following list focuses on the data or internal systems destruction:

Scrutinizing, Changing, and Destroying Data

- Trojan horse

- Viruses such as Melissa, Chernobal, and Papa
- Flash2 and CIH viruses wich attack computer hardware, not just its software
- Macro and variant with encrypted signatures
- Worms and logic bombs
- Stealth programs
- IP spoofing and TCP sequencing

The criminal needs to erase his or her steps. The following list points to a few well-known approaches to destroying evidence of one's presence:

Erasing the Evidence

- Changing the clock(s)
- Using superuser privileges
- Erasing the audit trail
- Redirecting the audit data (tactical delay)
- Archiving the change-data sets (tactical delay)
- Altering the logs to frame a legitimate user

In general, security countermeasures to computer crime fall into three areas: (1) computer and terminal access controls, (2) data communications controls, and (3) improvements to environment and policy. The following lists show some of the popular countermeasures and security maxims for these three control areas:

Security Countermeasures to Computer Crime Computer and Terminal Access Controls

- Passwords (alpha and numeric)
- Compartmentalization
- Error lockout
- Voiceprint recognition
- Fingerprint recognition
- Palm geometry
- Magnetic card accesses
- Automatic shutoff
- Time lock
- Modem callback

- Random personal information
- Challenge and response
- PIN numbers with magnetic card as proof of identity
- Personal signature recognition—light pen

Security Countermeasures to Computer Crime Data Communication Controls

- Cryptographic transmission and storage of data
- Scramblers
- Dial-back devices—access after terminal ID or user ID
- Passwords and authority verification
- Logs kept and monitored.
- Aborts and alarm mode monitoring
- Online monitoring by security personnel

Security Countermeasures to Computer Crime Environment and Policy

Environment

- Requirement: Clear and explicit policies with respect to proper and authorized use of computers and sanctions for abuses thereof
- Accounting controls
- Defensive countermeasures to ward off attacks and intrusions by outsiders
- Internal controls
- Supervision of employees with computer responsibilities
- Laws against criminal acts committed by computer and against computers
- Stabilization of the current laws
- Education of computer users about security and privacy of information
- Computer auditing methods
- Hardware and software protection
- Telecommunications systems protection
- Physical security of computer centers
- Proprietary information protection methods
- Personnel policies; rewards, standards, confidentiality agreements, nondisclosure agreements

- Teamwork
- Have in place a set of security related maintenance procedures to keep the network running smoothly such as backups and ISO Security Standards

Security Policy Maxims

- No security is 100 percent effective—anything can be overcome
- Those responsible for security policy should have a basic understanding of networks; password and authentication mechanisms; remote access
- Use balanced approach to risk management
- Use products that are based on industry standards
- Use countermeasures in depth
- Look for the weakest link in your armor.
- Improve employee awareness

Like many businesses, the intelligence community consists of a number of discrete organizations that perform distinct missions for overlapping sets of customers. Under the Intelligence Systems Board (ISB), headed in 1994 by Director Steven T. Schanzer, a team of CIA experts developed INTELINK. INTELINK is a secure, private collection of networks implemented on existing government and commercial communications networks. These networks employ Web-based technology, use established protocols, and are protected by firewalls to prevent external use. INTELINK captures the essence of current advanced network technology and applies it to the production, use, and dissemination of classified and unclassified multimedia data among the nation's intelligence resources. INTELINK is patterned after the global Internet. The following list presents some of the key elements of the INTELINK security strategy:[38]

INTELINK Security Strategy

- Strong authentication (two-way challenge/response)
- End-to-end confidentiality (integrity of data during transmission)
- Enhanced access control
- Community of interest (COI) for most sensitive materials
- Network auditing and monitoring: logging, analysis, and reporting
- Single sign-on
- Transparent security to user

- Secure collaboration
- Security management infrastructure
- Encryption, key management, certificate management, COIs, CRLs (certificate revocation list)
- SSL (Secure Sockets Layer protocol) with initial authentication, message privacy, and ensured data integrity

Prosecution Tools

The authors apologize for being a little informal with defining terminology. We have intertwined *digital* and *computer* and have given a broad definition to *espionage*, mapping it to a family of crimes. We have suggested that the main target is information—hence, the term *infocrime*. In addition, we have presented DE as a specific intent crime—one has to specifically intend to do this crime; negligence does not fall into our initial definition. We have little respect for hackers, crackers, spies, or thieves or for the damage they do in society. We support making their profession less profitable by prosecuting them. Computer crime falls under the jurisdiction of the U.S. Department of Justice (USDOJ).

Fortunately, Congress has provided USDOJ prosecutors with six serious tools to slow the tide. The following list sets forth the six main U.S. statutes used in the prosecution of computer crimes.[39,40,41,42,43,44]

- Computer Fraud and Abuse Act, 18 U.S.C. 1030
- Economic Espionage Act, 18 U.S.C. 1831, to 1839
- Trafficking in Fraudulent Access Devices, 18 U.S.C 1029
- Wire Fraud, 18 U.S.C. 1343
- Wiretap Act, 18 U.S.C. 2511
- Access to Stored Electronic Communications, 18 U.S.C. 2701

Computer Fraud and Abuse Act, 18 U.S.C. 1030

The strongest prosecutorial tool is the Computer Fraud and Abuse Act. Section 1030 covers fraud and related activity in connection with computers. The act was extensively amended in October 1996. It protects

confidentiality, integrity, and availability of data and computer systems. It prohibits using unauthorized access to computers to commit seven crimes: espionage, access to unauthorized information, access to nonpublic government computers, fraud by computer, damage to computer, trafficking in stolen passwords, and threats to damage a computer. The act covers "protected computers," which are exclusively or shared by a financial institution or the U.S. government or used in interstate or foreign commerce or communications.

Two key terms in this act are *exceeding authorized access*, which applies to any authorized user—also called "insiders" on the system—who accesses or alters information that he is not permitted to alter, and *without access*—an "outsider" who breaks in and uses the computer for any purpose. In parts of statute, the penalty may depend on whether you are an insider or outsider to the system. *Damage* is defined as any impairment to the integrity or availability of data, a program, system, or information, causing a loss of $5000 or more in a 12-month period; or impairment of medical records or data; or causing personal physical injury; or threatening public health or safety.

The act protects national security information and specifically prohibits accessing computer without or in excess of authority, obtaining national security information that could be used to injure the U.S., and communicating or attempting to communicate that information to someone not entitled to receive it. Maximum penalties specified under this act are 10 years in prison (20 years for second violation) and a $250,000 fine. This act is similar to 18 U.S.C. 793(e), which prohibits obtaining national defense information from any source and communicating or attempting to communicate it in any manner.

The act protects information from anyone intentionally accessing a computer without permission in excess of authorization and thereby obtaining information from a financial record or a credit report, a federal agency, or a "protected computer" if conduct involves an interstate or foreign communication. It protects confidentiality of computer data from *being read, even if not downloaded* (e.g., browsing National Crime Investigation Computer data).

The act prohibits intentional trespass in a U.S. government computer. It prohibits accessing any nonpublic computer of a department or agency if not authorized to access any computer of that department or agency. In addition, the act prohibits knowingly causing the transmission of a "program, information, code, or command" and as a result of such conduct, intentionally causing damage (without authorization) to a protected computer. It applies to insiders or outsiders. It further prohibits intentionally

accessing a protected computer without authorization and causing any damage negligently or otherwise.

Economic Espionage Act, 18 U.S.C. 1831 to 1839

The Economic Espionage Act became effective as of October 11, 1996. It was originally aimed at stopping foreign theft of U.S. information. It criminalizes on a federal level the theft of trade secrets. It has two main provisions that cover state-sponsored (1831) and commercial (1832) thefts.

A Section 1831 violation occurs if a defendant stole—or without authorization of owner, obtained, destroyed, or conveyed—information; that the defendant knew was proprietary or a trade secret, and that the defendant knew would benefit, or was intended to benefit, a foreign government, instrumentality, or agent.

A Section 1832 violation applies the same elements of Section 1831 and adds that the defendant intended to convert the trade secret to the economic benefit of someone besides the owner, the defendant knew or intended that the owner of the trade secret would be injured, and the trade secret was related to a product that was produced or placed in interstate or foreign commerce.

Trafficking in Fraudulent Access Devices, 18 U.S.C 1029

Section 1029 of the Trafficking in Fraudulent Access Devices applies to fraud and related activities in connection with access devices. A person is in violation of this title if he or she, with intent to defraud, produces, uses, or traffics in one or more counterfeit access devices, in order to effect transactions aggregating $1000 or more in a year; or knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services; or knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses the following:

- A scanning receiver,
- Hardware or software used for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services, or
- Without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, one or more evidences or records of transactions made by an access device; shall, if the offense affects interstate or foreign commerce be in violation of this title.

A fine under this title is twice the value obtained by the offense, or imprisonment for not more than 15 years.

Wire Fraud, 18 U.S.C. 1343

Section 1343 covers fraud perpetrated by means of wire, radio, or television. It states that anyone who devises any scheme to defraud for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, or who transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined, imprisoned not more than five years, or both. If the violation affects a financial institution, that person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

Wiretap Act, 18 U.S.C. 2511

Section 2511 of the Wiretap Act prohibits interception and disclosure of wire, oral, or electronic communications. Complex elements of a 2511 violation include the intentional interception of any wire, oral, or electronic communication or the use of any electronic, mechanical, or other device to intercept any oral communication when the device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication, or when the device transmits communications by radio or interferes with the transmission of wire communication, and intentionally discloses contents of any wire, oral, or electronic communication. It also covers the knowledge that the information was

obtained through the interception of a wire, oral, or electronic communication.

It is further unlawful to use a pen register or a trap and trace device (without authority). It is unlawful to intercept wire or electronic communication that is scrambled, encrypted, or transmitted using modulation techniques, the essential parameters of which have been withheld from the public with the intention of preserving the privacy of communication, such as:

- Radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a public land mobile radio service communication, or a paging service communication
- Interception of a satellite transmission (encrypted or scrambled)

Punishment specified under this act includes a minimum of $500 for each violation and jail terms dependent on circumstances and damages.

Access to Stored Electronic Communications, 18 U.S.C. 2701

Section 2701 of the Access to Stored Electronic Communications Act makes it unlawful to access stored communications where one intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in the system. The punishment for an offense committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain is up to two years in jail.

Investigation

Given the legal tools in the preceding lists, investigators would be concerned with several questions. How did they get in? What did they do? How do we identify them? How do we catch them?

In this chapter we've specified some of the methods of intrusion.

Additionally, we have defined the profile for the typical attacker. Attackers generally are skilled (capable of writing the automated attack tools) or nonskilled (tool users). Both have ties to the underground. The professional attacker is hard to detect and is not tied to the underground. The outside attacker uses techniques as indicated earlier in this chapter. After the attack, the nonprofessional might access e-mail, or files, use the system as an attack platform, share information with buddies, and create back doors, install Trojans horses, and sniffers. The professional gets in, gets the data, gets out, and leaves no tracks.

Detecting an intrusion can be done by: (1) user notices (rare), (2) system administrator notices, (3) anomaly in system log, (4) system crashes, (5) receiving a call from another system admin, or (6) reading about it in the daily news or Usenet (definitely not good).

The bad guy can conceal his or her identity on the Internet in many ways: (1) screen name can be changed each session, (2) IP address can be spoofed so header information is wrong, (3) an anonymizer can be used, (4) anonymous remailers can be used, and (5) compromised accounts can be used.

Investigators obtain evidence in several ways using real-time interception through monitoring the ISP, keystrokes, and e-mail; by court order (a.k.a. "T3"); by subpoena of the subscriber; by review of log files, transactional data, usage history, and cell phone calls; by "Reasonable and Articulable Facts Order" (18 U.S.C. 2703 (d); and by search warrant on unopened mail on the ISP server.[45]

A Word about Encryption

Software or hardware may use a mathematical algorithm to scramble (encrypt) bits of data sent or stored on computer networks. The key to the cipher is a string of numbers or characters. The stronger the algorithm and the longer and more chaotic or random makeup of the string, the more difficult it is to break.

The length of the key is measured in bits, the number of digits in the key. For most encryption techniques in use today, the bit length combined with the rendomness of the key can be used as an approximation of the strength of an encryption program. Longer bit length does not guarantee greater security; a poorly designed security program could be invaded without the invader's making a brute force attack on the key (a *brute-force attack* consists of trying all the possible keys in hopes of finding the

one that works). But longer bit length usually (assuming true randomness of the bits) means stronger encryption.

Two types of encryption systems are employed. The symmetric or private key cipher uses a secret key for both encipherment and decipherment. Sender and receiver both have the same encrypting/decrypting transformation and use the identical secret key. Drawbacks of this method include: (1) the secret key must be transmitted in a separate medium between recipients, (2) the secret key might be revealed and affect full system compromise, and (3) the key may be used to forge a document in the sender's name.

The development of public key encryption from 1974 to 1975 solved this problem. There are two keys: a public key and a private key that are mathematically related. The relationship between the two keys is a nearly insoluble mathematical problem. The public key is available to everyone who desires to communicate; the private key is never given to anyone and is held very confidentially by its owner. The sender of a message uses the recipient's public key to encrypt the message. The recipient uses his or her private key to decipher the message. Only the user's private key can decrypt the message.

Public key cryptography permits the use of digital signatures of a message to uniquely identify the message sender. The sender encrypts a small portion of the message called the *hash* or *MAC* (message authentication code) with his or her private key and the message with the public key of the recipient. The recipient uses his private key to decrypt the message and the user's public key to decrypt and verify the sender's signature. Public key cryptography allows for rigorous authentication. Authentication is as important as confidentiality as a security goal when either financial and/or Internet transactions are considered. Public key cryptography can be used to secure public infrastructure communications, because authentication of users can be performed without revealing users' secret keys.

Pressure to regulate the use of strong encryption comes from law enforcement interests.[46] Encryption represents one of the biggest challenges to law enforcement because of its use by criminals. Law enforcement is able to crack the weak and older encryption (publicly announced as about 56 bits) but without key recovery (an entrenched battle with academic, industry, and public interests is ongoing). Law enforcement loses the ability to solve crime in a timely fashion. To law enforcement, basically encryption is a double-edged sword: If law enforcement *can't* crack it, the criminal may escape punishment. If law enforcement *can* crack it, the criminal is uniquely tied to the evidence.

What almost all law enforcement interests want is key escrow or key-recovery mandates. Under this system, people who use encryption must file their secret keys with the government or a third party, or include decoding information along with the message without their knowledge. Law enforcement interests want access to the stored messages and their real-time transmission.

A national debate has ensued over the use and export of strong encryption. Law enforcement interests support legislation that would force U.S. citizens and residents to give the government access to their keys. However, export controls and government-prescribed key recovery has not kept strong encryption out of the hands of criminals and terrorists, because technology is available worldwide without key-recovery features. Efforts under the Clinton administration have failed to convince either the U.S. Congress or other countries of the requirement. In March 1999, even France, who had an oppressive lock on encryption technologies for their citizens, removed restrictions from 128-bit encryption use.

A June 10, 1999 study by Lance Hoffman at George Washington University found 805 hardware and software products incorporating cryptography manufactured in 35 countries outside the United States. In addition, 167 foreign cryptographic products use strong encryption algorithms, and 512 foreign companies manufacture or distribute cryptographic products in at least 67 countries outside the United States.[47]

Probably the most interesting case in the pipeline is Bernstein v. Department of Justice. On May 6, 1999, a federal appeals court confirmed that all source code is a form of expression protected by the First Amendment. The Bernstein case involved a challenge to the federal regulations restricting the export of software, which includes strong encryption. The Bureau of Export Administration (BXA) is in near shock, and this is their response verbatim:

May 6 Court Decision in Bernstein Encryption Case

You may have read about a recent court decision regarding encryption exports. Please be advised that this decision does not mean that encryption products may be exported without regard to the Export Administration Regulations (EAR). Regardless of how the decision might be interpreted, the decision is subject to a stay. This stay is in effect for at least 45 days. (See Department of Justice press release.)

On May 6, the U.S. Court of Appeals for the Ninth Circuit rendered a decision in Bernstein v. the United States Department of Justice. Professor Daniel Bernstein filed suit against the U.S. Government after he was notified by the State Department that his "Snuffle" encryption program was subject to the

International Traffic in Arms Regulations (ITAR) and would require an export license to post the source code on the Internet. Bernstein subsequently amended his petition to challenge the controls on encryption products maintained under the EAR after President Clinton placed encryption exports under the Commerce Department's jurisdiction in 1996. In a 2-1 decision, the Ninth Circuit court upheld the district court's decision that the regulation of Bernstein's export of his "Snuffle" program "constitute[s] an impermissible prior restraint on speech."

Exporters should be aware that the decision does not affect the applicability of the EAR to exports and reexports of encryption hardware and software products or encryption technology. This includes controls on the export of encryption software in source code. The EAR remains in effect for these items. The Commerce Department will apprise exporters of any changes to the encryption controls.[48]

The Department of Justice statement shows more balance, but they are clearly not happy about the decision. The next strategic decision that must be made after it fails a rehearing (requested by President Clinton) by the federal court is to take the case to the Supreme Court. A loss here would be final, and BXA employees would need to update their résumés. Here is the DOJ statement verbatim:

Department of Justice Statement On Ninth Circuit Court of Appeals Decision in Encryption

On May 6, a three judge panel of the United States Court of Appeals for the Ninth Circuit in San Francisco issued a decision in a case involving government controls on encryption exports. The Department of Commerce and the Department of Justice are currently reviewing the Ninth Circuit's decision in Daniel Bernstein v. United States Department of Justice and United States Department of Commerce. We are considering possible avenues for further review, including seeking a rehearing of the appeal en banc in the Ninth Circuit.

The regulations controlling the export of encryption products currently remain in full effect. The Ninth Circuit's decision will not take effect until the court issues its mandate, which will not occur for at least 45 days. If the government asks the Ninth Circuit to rehear the appeal during that time, the mandate will not issue until after the Ninth Circuit has acted on the government's request.

The district court injunction in this case relating to the encryption export regulations has been stayed by orders issued earlier by the district court and the Ninth Circuit, and the stays of the injunction remain in effect until the mandate issues. Accordingly, all persons who wish to engage in encryption export activ-

> ity, including the posting or other distribution of encryption software on the Internet, must still comply with the export licensing requirements of the Export Administration Regulations, administered by the U.S. Department of Commerce's Bureau of Export administration (BXA).
>
> Information about the regulations is available at the BXA website at www.bxa.doc.gov. 99-178[49]

Electronic eavesdropping methods allow law enforcement officers to legally compromise privacy. Privacy activists argue that law enforcement already has many technologies available to them that can be used as alternatives to wiretaps. Alternatives not defeated by the use of encryption, include:

- Improved call-tracing methods
- Surveillance with infrared scanners
- Aerial surveillance
- Bugging
- Filtering that picks certain voices or keywords out of the babble of telecommunications traffic, formerly precluded by the sheer volume of calls
- Supersensitive satellite photography that lets the police peer into windows or identify a license plate from 20 miles up in the sky
- Vast electronic databases [many combined]
- Plaintext readers such as Tempest, which read text appearing on computer screens through closed doors and walls as we type
- Laser light beams that allow conversations to be deduced from vibrations of the windowpane
- Credit card transactions, e-mail, Internet transactions, and clickstream data are all easy to intercept or subject to other electronic surveillance methods.

Whitfield Diffie summarizes the privacy case as follows: "Throughout history, the science of cryptography repeatedly advanced beyond the ability of cryptanalysts to crack the codes. Law enforcement has always had the right to try to decipher encrypted messages; they never had a practical or constitutional guarantee of success. The government's right to search one's house does not entail a power to forbid people to hide things."[50]

Do not count the USDOJ or BXA out of the game. Congress has usually supported their requirements. It is easy to see the USDOJ position; it is in the tough job of catching the bad guys who have up-to-date com-

munication tools. Vice President Al Gore's recent call for balance to keep encryption out of the hands of terrorists and criminals is a noble request. It may be difficult to achieve in a world (outside of the United States) that does not share our policy or views.

Wrap-Up

The scope of a *family* of crimes under the title of *Digital Espionage* has been identified and classified. The MOMM of computer crimes and the tools that investigators, such as the USDOJ, may use to stop computer crime in situ have been reviewed. Since targets of computer crime tend to be information-based, *infocrimes* have an enormous financial impact. Because of its overall effectiveness, a point-of the-pin look at encryption and the political environment in which it exists was introduced. The authors contend that computer crimes and digital espionage occur because of a failure to provide appropriate information security (INFOSEC) countermeasures in organizations. Chapter 2 introduces the concept of INFOSEC and risk and applies it in a more global scope. Subsequent chapters introduce due diligence implementation of INFOSEC technologies.

Notes

1. Statement of Robert S. Litt, Deputy Assistant Attorney General, U.S. Department of Justice, Criminal Division, before the Subcommittee on Social Security, Senate Ways and Means Committee, United States Senate, Washington, DC, 20530, May 6, 1997.
2. Ibid. (CSI, the Computer Security Institute, is a leading security training organization that publishes surveys and reports such as computer crime and information security program assessment. It jointly works with the FBI on its annual surveys. Their Web site is at *http://www.gocsi.com/homepage.shtml*.)
3. Zwillinger, Marc J., "Investigation and Prosecution of Computer Crime," Computer Crime and Intellectual Property Section Criminal Division, U.S. Department of Justice, 4 November 1998, *http://www.amc.army.mil/amc/ci/nov4a/tsld005.htm*. Also, WarRoom Research is a firm specializing in business and competitive intelligence. Their Web site is at *http://www.warroomresearch.com*.
4. Ibid.
5. Ritchey, Barbara D. DISC6341, Professor Hirschheim, "Computer Crimes and How to Prevent Them," *http://disc.cba.uh.edu/~rhirsch/fall96/barba.htm*.
6. Violino, Bob. "Your Worst Nightmare," *Information Week*, February 1996,

34-36.
7. Ritchey, op. cit.
8. Edwards, Owen, "Hackers from Hell," *Forbes ASAP Supplement*, October 1995, 182.
9. Denning, Dorothy E., "Who's Stealing Your Information," *Information Security*, April 1999, 29.
10. Ibid.
11. DeYoung, H. Garrett, "Thieves Among Us," *Industry Week*, Vol. 245, June 1996, 12-16.
12. Nichols, Randall K., COMSEC Solutions presentation to FBI Security CIITA agents, Quantico, VA, 27 May 1999. (COMSEC Solutions is a leading cryptographic, anti-virus and biometric countermeasures firm. Their Web site is at *http://www.comsec-solutions.com*.
13. Litt, op. cit.
14. Ibid.
15. Litt, op. cit. On February 22, 1993, the two defendants were sentenced to 5 years' probation, $30,000 restitution (joint and several), and 250 hours of community service. As a condition of probation, both hackers were restricted from owning or using a computer without permission from the probation officer.
16. Ibid.
17. Ibid.
18. Ritchey, op. cit.
19. Litt, op. cit.
20. Ibid.
21. Denning, op. cit.
22. Ibid.
23. Zwillinger, op. cit.
24. Litt, op. cit. One of the two was sentenced to incarceration of 15 months', and 36 months' probation, while the other was sentenced to 60 months' probation. Restitution was ordered jointly in the amount of $32,000.
25. Litt, op. cit. See United States v. Peterson, 98 F.3d 502, 504 (9th Cir. 1996), upholding two-level enhancement under sentencing guidelines for use of special skill to facilitate crimes, including crime described in text.
26. Ritchey, op. cit.
27. Interview, 3 March 1999.
28. Ritchey, op. cit.
29. Zwillinger, op. cit.
30. Pitorri, Peter, *Counterespionage for American Business*, (Oxford, Great Britain: Butterworth-Heinemann, 1998).
31. Barlow, J. P., et al., Forum: "Is Computer Hacking a Crime?" *Harper's Magazine*, March 1990, 46-57.
32. Nichols, op. cit.
33. Parker, Donn B., *Fighting Computer Crime* (New York: Wiley, 1999).
34. Denning, Dorothy, *Information Warfare and Security*, (Reading, Mass.: Addison Wesley, 1999).
35. Winkler, Ira, *Corporate Espionage*, (Rocklin, Calif.: Prima Publications, 1997).
36. Eells, Richard, and Peter Nehemkis, *Corporate Intelligence and Espionage*,

(Indianapolis: Macmillan, 1984).
37. Levine, Diane E., "Virus and Related Threats to Computer Security," *Computer Security Handbook*, ed. Arthur E. Hutt, Seymour Bosworth, and Douglas B. Hoyt (New York: Wiley, 1995).
38. Martin, Frederick Thomas, *Top Secret Intranet: How the U.S. Intelligence Built INTELINK* (Upper Saddle River, NJ: Prentice-Hall, 1997).
39. 18 U.S.C. 1030, *http://mailer.fsu.edu/~btf1553/ccrr/federal.htm*.
40. 18 U.S.C. 1831-1839, *http://mailer.fsu.edu/~btf1553/ccrr/federal.htm*.
41. 18 U.S.C. 1029, *http://mailer.fsu.edu/~btf1553/ccrr/federal.htm*.
42. 18 U.S.C. 1343, *http://mailer.fsu.edu/~btf1553/ccrr/federal.htm*.
43. 18 U.S.C. 2511, *http://mailer.fsu.edu/~btf1553/ccrr/federal.htm*.
44. 18 U.S.C. 2701, *http://mailer.fsu.edu/~btf1553/ccrr/federal.htm*.
45. Zwillinger, op. cit.
46. Singleton, Solveig, "Policy Analysis: Encryption Policy for the 21st Century," *http://www.cato.org/pubs/pas/pa-325es.html*.
47. Hoffman, Lance J., et al., "Growing Development of Foreign Encryption Products in the Face of U.S. Export Regulations," Report No. GWU-CPI-1999-02, June 10, 1999.
48. BXA Press release, June 1 1999, *www.bxa.doc.gov/encryption/state.htm*. Superseded by statement of Office of the White House Press Secretary, *Administration Announces New Approach to Encryption*, September 16, 1999, *www.bxa.doc.gov/encryption/whpr99.htm*. See also BXA FAQ on update to encryption policy, September 16, 1999.
49. U.S. Department of Justice statement on Ninth Circuit Court of Appeals Decision in Encryption Case, May 7, 1999, *www.usdoj.gov/opa/pr/1999/may/178civ.htm*.
50. Diffie, Whitfield and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (Cambridge, Mass.: MIT Press, 1998, 6.