Crime, Use of Computers in

by M. E. Kabay, PhD, CISSP

An article from

Encyclopedia of Information Systems, Volume 1

Hossein Bidgoli, Ed. (2003)

Academic Press (Amsterdam)

ISBN 0-12-227240-4 (set)

Outline:

I. The foundations of information security
   A. Basic concepts
   B. Threats to security
II. The legal foundations
   A. United States computer-crime laws
   B. Criminal law and civil law
   C. International developments
   D. Jurisdictional problems
III. Classifications of breaches of information security
   A. Levels of information warfare
   B. John D. Howard's analysis
IV. Crimes where computers and networks are tools only
   A. Fraud
   B. Counterfeits of documents, money
   C. Extortion
   D. Slamming
   E. Industrial espionage
   G. Gambling
   H. Pornography
   I. Stalking and assault
   J. Libel, misrepresentation and harassment
   K. Theft of intellectual property
V. Where computers, networks and software are the targets as well as tools
   A. Denial of Service and Jamming
   B. Penetration
   C. Covert Breaches of
   D. Viruses, Worms and Trojans
   E. Logic bombs
   F. Penetration
   G. Sabotage
   H. Counterfeit Software

Glossary:

Authenticity:	Validity, conformance and genuineness of information.
Availability:	Timely accessibility of information for a specific purpose.
Confidentiality:	Limited observation and disclosure of knowledge.
Data diddling:	Unauthorized modification of data.
Denial of service:	Prevention of availability due to resource saturation or resource destruction.
Eavesdropping:	Unauthorized interception of communications.
Integrity:	Completeness, wholeness, and readability of information; quality of being unchanged from a prior state.
Logic bomb:	Unauthorized, harmful executable code whose actions are triggered by a logical condition such as presence or absence or specific data or by a particular time or date.
Malware:	Contraction of "malicious software;" executable code intended by its writer to violate information security of its victims. Examples include viruses, worms, logic bombs, Trojan Horses, and denial-of-service programs.
Penetration:	Unauthorized access to resources through violation of access-control restrictions.
Possession:	Holding, control and ability to use information.
Social engineering:	The use of deceit to persuade other human beings to help an attacker violate information security restrictions.
Trojan Horse:	Software having undocumented and unauthorized functions in addition to or instead of expected useful functions.
Utility:	Usefulness of information for a purpose.
Virus:	Self-replicating executable code that inserts unauthorized instructions into other executable code.
Worm:	Self-replicating executable code that passes copies of itself through computer communications networks.

Concise definition of subject (opening paragraph)

This article reviews the most important types of crimes involving computers and networks. Computers and computer networks are tools for obtaining, storing, manipulating and transmitting information. Like any other tool, they can be used for social good or for social ill. Criminals have used every technological innovation in history as the basis for new or variant crimes, and the criminal subculture has been active in turning computers and networks towards its ends. Computers and networks play a role in crime both as mediating instruments of crime and, in contrast, as the objects or targets of crime.

I. The foundations of information security

The classic definition of information security was developed in the 1970s: Data security involves the protection of information from unauthorized or accidental modification, destruction and disclosure. The "classic triad" of information security names confidentiality, integrity and availability. To these three, the respected security expert Donn B. Parker has added possession, authenticity and utility.

A. Basic concepts

Protection means reducing the likelihood and severity of damage. Another way of putting this is that information security strives to reduce risks. It is not possible in practice to provide perfect prevention of security violations. Common sense suggests that the degree of protection must match the value of the data.

Information is protected by caring for its form, content and storage medium.

Unauthorized means forbidden or undocumented. The very concept of authorization implies classification: there must be some definition of which data are to be protected and at what level.

Modification means changes of any kind. The ultimate modification is destruction. However, small but significant changes in data are more trouble than destruction. For example, the damage caused by a vandal who damages a Web site by adding pornography and vile language can be spotted at once and can be removed quickly. In contrast, some kinds of malicious software can make small random changes (e.g., in spreadsheets) that can accumulate for months. Backup copies of the corrupted files may make it impossible to recover valid versions of these files.

Disclosure means allowing people to see or use data. The critical element is authorization: permission by a *data owner* for selected others to have access to these data.

Confidentiality is a wider concept than disclosure. For example, certain files may be confidential; the data owner may impose operating system controls to restrict access to the data in the files. Nevertheless, it may be possible for an unauthorized person to see the names of these files or find out how often they are accessed. Changing a file's security status may be a breach of confidentiality; for example, copying data from a secure file to an unsecured file is a breach of confidentiality.

Possession means control over information. For example, when thieves copy proprietary software without authorization, they are breaching the owner's possession of the software. Such *counterfeit* software represents a breach of possession or control. Similarly, if someone obtains an unauthorized copy of a confidential document, there is a breach of possession or control even before anyone actually looks at the document because the owner no longer determines when the data will be disclosed to unauthorized people.

From the *Encyclopedia of Information Systems* (2003), H. Bidgoli, ed. Used with permission of, Academic Press.

Integrity refers to internal consistency. A database is termed structurally corrupt when its internal pointers or indexes no longer correspond to the actual records they point to. For example, if the next record in a group is in position 123 but the index pointer refers to position 234, the structure lacks integrity. Surreptitiously using a disk editor to bypass security and alter pointers in such a data structure would impair integrity even if all the data records were left intact. Logical corruption occurs when data are inconsistent with each other or with system constraints. For example, if the summary field in an order header contains a total of $5,678 for all items purchased but the actual sum of the costs is $6,789 then the data structure is logically corrupt; it lacks integrity.

Authenticity refers to correspondence between data and what the data represent; accordance with reality, correctness. A typical example of impaired authenticity is electronic mail sent using a false name – or worse, someone else's name.

Availability means that data can be used in a timely fashion; the data are convenient or handy. If a server crashes, the data on its disks are no longer available; but if a mirror disk is at hand, the data may still be available.

Utility refers to the usefulness of data for specific purposes. Even if the information is still intact, it may have been transformed into a less useful form. For example, unauthorized encryption of a firm's source code for production program is a breach of utility. In a formal sense, the data were authentic, accurate and available – they just were not useful.

B. Threats to security

Enterprise systems are faced with two kinds of threat: people and disasters. People include managers, employees, service personnel, temporary workers, suppliers, clients, thieves, liars and frauds. Disasters include fire, flood, earthquake, civil disturbance and war.

The difficulty in describing the risk of facing these threats is that we lack proper statistical information about how often different types of damage occur. In statistical work, this difficulty is known as the problem of ascertainment. Most organizations are reluctant to admit, let alone publicize, successful attacks on their information systems.

The second part of the ascertainment problem is that even if people were reporting all the computer crimes and accidents they knew about, we would still not know about the crimes and accidents that have not yet been discovered.

Keeping in mind that all statistics about computer crimes are problematic, the information security field has arrived at a shaky consensus about the origins of damage to computer systems and networks. In brief,

- Perhaps as much as half of the damage is due to errors and omissions by authorized users of the systems;

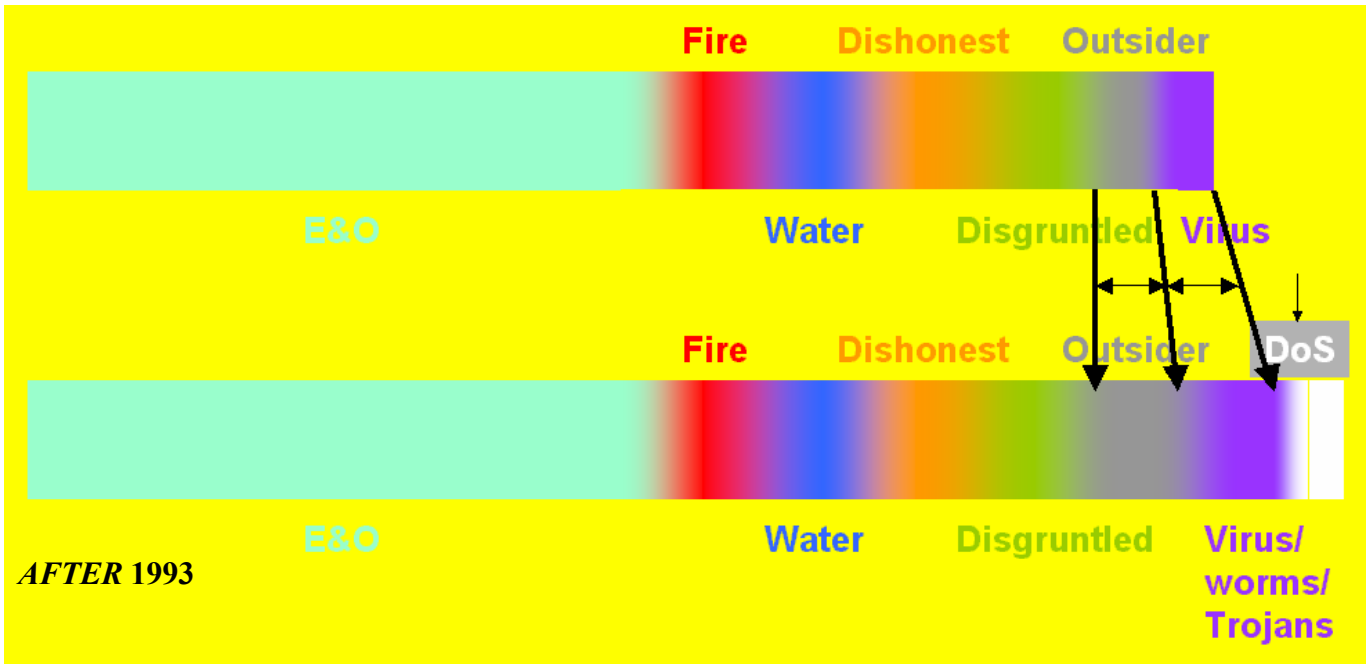
- Fire and water damage and problems resulting from poor electrical power account for perhaps a quarter of the problems;
- Authorized but dishonest or disgruntled employees are a significant source of difficulties;
- Malicious software and outside attacks were thought to account for a small portion of the threat to systems before the explosive growth in Internet usage in the early 1990s; however, by the turn of the millennium, both malicious software and outsiders posed a much greater source of danger, perhaps approximating the threat from angry and dishonest insiders.

Figure 1 shows the rough guesses about damage to computer systems before and after the explosion of Internet usage that occurred around 1993. Note that the edges of the categories are deliberately made fuzzy to remind the reader of the uncertainty of these estimates. The categories are

- E&O: errors and omissions; due to lack of training, poor motivation, or poor supervision.
- Fire, water: Arson, accident, sabotage; water damage often accompanies fire damage.
- Dishonest: Employees.
- Disgruntled: Employees.
- Outsider: Contractors, visitors, strangers.
- Virus: Self-replicating code that integrates into executable code.
- Worms: Self-replicating code that propagates through networks.
- Trojans: Software with undocumented and unauthorized functions.
- DoS: Denial of service attacks.

Figure 1. Rough Guesses about the Sources of Damage to Computer Systems Before and After the Internet Explosion.

***BEFORE* 1993**



II. The legal foundations

This section reviews some of the key laws that govern the use of computers and networks and which criminalize specific acts.

A. United States computer-crime laws

The most advanced set of laws criminalizing particular unlawful behavior involving computers and networks have been legislated in the United States. The *Computer Fraud and Abuse Act of 1986* (18 USC §1030) focuses primarily on protecting "government-interest" computers, including federal, state, county and municipal systems; financial and medical institutions; and computers used by contractors supplying such institutions. Specifically, the Act prohibits the use of "a program, information, code or command" with intent to damage, cause damage to, or deny access to a computer system or network. In addition, the Act specifically prohibits even unintentional damage if the perpetrator demonstrates reckless disregard of the risks of causing such damage.

Another law governing interstate electronic communications has been used in prosecutions of computer crimes: 18 USC §1343, dealing with wire fraud. Wire fraud requires the following elements: (a) a scheme to defraud by means of false pretenses; (b) knowing and willful participation with intent to defraud; (c) the use of interstate wire communications in furtherance of the scheme.

The Electronic Communications Privacy Act of 1986 (18 USC §1367 and others), generally known as the ECPA, assigns fines and prison sentences for anyone convicted of unauthorized interception and disclosure of electronic communications such as phone calls through land lines or mobile systems and e-mail. In addition, the ECPA specifically prohibits making use of an unlawfully overheard electronic communication if the interceptor knows that the message was unlawfully obtained. On the other hand, *providers* of electronic messaging systems, including employers, are permitted to intercept messages on their own systems in the course of their normal operations; naturally, they are authorized to transmit messages to other communications providers as part of the normal course of transmission to the ultimate recipient. The ECPA also prohibits access to stored messages, not just those in transit.

United States law also criminalizes the use of interstate communications for the transmission of threats, in kidnappings, and in extortion (18 USC §2518). Another form of prohibited speech is everything associated with child pornography: making, sending, publishing or storing images of children engaged in sexually explicit conduct (18 USC §2251).

The Communications Decency Act of 1996 (47 USC §223) was a highly controversial statute prohibiting anyone using interstate or communications from transmitting obscene or indecent materials when they know that the recipient is under 18 years of age – regardless of who initiated the communications. In June 1997, in a stinging rebuke to proponents of censorship, the United States Supreme Court issued its ruling on the Communications Decency Act, finding that it

violated First Amendment protection of free speech. The unanimous opinion stated that the effort to protect children from sexually explicit material went too far because it also would keep such material from adults who have a right to see it.

In addition to federal laws, the United States has a tapestry of state laws applying to computer crimes. States differ widely in the availability of computer-crime laws and in their definitions and penalties.

B. Criminal law and civil law

Another area of legal constraints originates in civil law. Issues of copyright, trademark, defamation, privacy, anonymity and pseudonymity, duty of care and digital signatures are too complex for this article, which focuses on the relatively simple concepts of unauthorized access to or interference with computer systems and networks. However, the interested reader will find additional material in the appropriate sections of this *Encyclopedia* and among the recommended readings at the end of this article.

C. International developments

Few countries have kept up with the United States in their legislation concerning computer crimes. However, there have been recent developments bringing hope to the targets and victims of computer criminals. The following sections give a few examples of legislation to illustrate the kinds of issues and penalties being developed around the world in cyberlaw.

1. Canada

Canadian law (section 342.1) specifies that "Every one who, fraudulently and without color of right, (a) obtains, directly or indirectly, any computer service, (b) by means of an electro-magnetic, acoustic, mechanical or any other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, or (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system

is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction."

In addition, Canadian law addresses "mischief" pertaining to computer systems (section 430.1): "Every one commits mischief who wilfully (a) destroys or alters data; (b) renders data meaningless, useless or ineffective; (c) obstructs, interrupts or interferes with the lawful use of data; or (d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto."

On January 1, 2001 Canada's Personal Information Protection and Electronic Documents Act took effect. The law defined statutory obligations for protecting privacy, among other security-related topics.

2. United Kingdom

In Britain, the Computer Misuse Bill of 1990 defines unauthorized access to computer material (including equipment and data), stipulates that there be intent to commit or facilitate commission of further offenses, and specifically addresses the issue of unauthorized modification of data. The law states that there is no need to prove that the defendant was aiming to harm any particular program or data, any particular kind of program or data, or indeed programs or data held in any particular computer. Penalties are limited to a maximum of five years in prison and various levels of fines.

3. Germany

German law (section 202a) defines "data spying" as unauthorized access to other people's data and comes down hard on "violation of private secrets," (section 203) which include in particular data held by physicians, dentists, veterinarians, pharmacists, psychologists, lawyers, patent agents, notaries public, defense counsel, certified public accountants, sworn auditors, tax advisors, auditors, marriage/family/educational/youth/addiction counsellors, social workers, insurance companies and several other categories of data owners. Violation of this provision can be punished by fines or imprisonment of up to one year.

Section 204 specifically identifies industrial espionage by augmenting the possible penalties to a maximum of two years in prison.

Section 263a increases the penalties yet again for anyone convicted of computer fraud: "Anybody who, with a view to procuring himself of a third person any unlawful property advantage, causes prejudice to the property of another by influencing the result of a data proceeding activity through improper program design, through the use of incorrect or incomplete data, through the unauthorized use of data, or otherwise through any unauthorized interference with the transaction, shall be sentenced to imprisonment not exceeding five years or to a fine."

Other sections of German law explicitly deal with forgery, deception by unauthorized modification of data, and computer sabotage.

4. Italy

Law number 547 dating to 1993 established Article 615.5 of the Penal Code: "Spreading of programs aimed at damaging or interrupting a computer system. Anyone who spreads, transmits or delivers a computer program, whether written by himself or by someone else, aimed at or having the effect of damaging a computer or telecommunication system, the programs or data contained in or pertaining to it, or interrupting in full or in part or disrupting its operation is punished with the imprisonment for a term of up to two years and a fine of up to It. L. 20,000,000."

5. Switzerland

Article 144bis, in force since 1995, stipulates that "Anyone, who without authorization deletes, modifies or renders useless electronically or similarly saved or transmitted data, will, if a complaint is filed, be punished with the imprisonment for a term of up to 3 years or a fine of up to 40000 Swiss francs. If the person charged has caused a considerable damage, the imprisonment will be for a term of up to 5 years."

As for malicious software, "Anyone, who creates, imports, distributes, promotes, offers, or circulates in any way programs, that he/she knows or has to presume to be used for purposes according to the item above, or gives instructions to create such programs, will be punished with the imprisonment for a term of up to 3 years or a fine of up to 40000 Swiss francs. If the person charged acted for gain, the imprisonment will be for a term of up to 5 years."

6. Other countries

For a comprehensive and frequently-updated review of computer crime laws in 37 countries (at the time of writing in January 2001), see Stein Schjolberg's review, "The Legal Framework: Unauthorized Access to Computer Systems – Penal Legislation in 37 countries." The Web address in 2001 was http://www.mossbyrett.of.no/info/legal.html . The 37 countries covered were:

Argentina	Egypt	Japan	Spain
Australia	Finland	Luxembourg	Sweden
Austria	France	The Netherlands	Switzerland
Belgium	Germany	New Zealand	Tunisia
Brazil	Greece	Norway	Turkey
Canada	Hungary	Poland	United Kingdom
Chile	Ireland	Portugal	United States
China	Iceland	Romania	
Czech Republic	Israel	Singapore	
Denmark	Italy	South Africa	

D. Jurisdictional problems

Cyberspace crime poses a jurisdictional problem because the perpetrator of a crime can reside in one country, act through computers and networks in several other countries, and cause harm to computer systems in yet other countries. Trying to investigate and prosecute crimes that are carried out in milliseconds when international cooperation can take days and weeks means that many computer crimes simply go unpunished.

The most irritating aspect of computer crime investigations and prosecutions is the jurisdictional quagmire resulting from incomplete and inconsistent laws. In international law, no one may legally be extradited from one country to face prosecution in another country unless both counties involved have *dual criminality.* That is, an offense must be similar in law and at the

same level of criminality (misdemeanor, felony) before extradition can be considered by courts of law.

A good example of the frustration felt by law enforcement officials and victims of computer crime occurred in the year 2000, when a world-wide infestation by the e-mail-enabled worm *Love Bug* caused damage and lost productivity estimated in the hundreds of millions of dollars. The putative originator of the worm was a computer programming student in Manila, The Philippines. Even though the alleged perpetrator came close to admitting his responsibility for the infection – and was lionized by the local press – there were no applicable laws in The Philippines under which he could be prosecuted locally. As a result, he was never extradited to the United States for prosecution.

III. Classifications of breaches of information security

The study of computer crime has not reached the state of academic rigor characteristic of a mature field. Classifications of computer crimes remain relatively primitive. However, there are two ways of referring to computer crimes that are sometimes used to organize discussions. Many authors provide lists of computer crimes, but there is rarely any obvious underlying principle for the sequence of crimes in their lists.

A. Levels of information warfare

One approach to organizing the types of computer crime is based on the work of Winn Schwartau, a controversial author and speaker who has been active during the decade of the 1990s in warning of the danger of an "electronic Pearl Harbor" and has succeeded in bringing electronic attack methods and countermeasures to public attention. Schwartau points out in his *Information Warfare* (2nd ed. 1996, Thunder's Mouth Press, ISBN 1-56025-132-8) that there are three obvious levels of target in electronically-mediated conflict: individuals, corporations and other organizations, and countries. He refers to these classes as Interpersonal, Intercorporate and International Information Warfare. This schema permits a crude but useful level of organization for discussions of crime and warfare directed at and mediated through information technology.

B. John D. Howard's analysis

In his 1997 doctoral dissertation (*An Analysis of Security Incidents on the Internet 1989 – 1995,*

Department of Engineering and Public Policy, Carnegie Institute of Technology at Carnegie Mellon University: http://www.cert.org/research/JHThesis/Start.html), John D. Howard presents a far more thorough analysis of computer incidents than anything else up to the time of publication of this *Encyclopedia*.

Howard starts by defining the following elements of a computer security *event*:

- Attacker
- Tool
- Vulnerability
- Action
- Target
- Unauthorized Result
- Objective.

Security events may involve more than one factor from each of the elements; in that sense, the analysis is not a *taxonomy* because it cannot be used to assign any given crime to a single class. Nonetheless, Howard's work is most helpful in thinking about computer crime.

The *attackers* include

- Hackers
- Spies
- Terrorists
- Corporate Raiders
- Professional Criminals
- Vandals
- Voyeurs.

The *tools* available to computer criminals include

- Physical Attack
- Information Exchange
- User Command
- Script or Program
- Autonomous Agent
- Toolkit
- Distributed Tool
- Data Tap.

The *vulnerabilities* that can be exploited by an attacker include

- Design
- Implementation
- Configuration.

Attackers can use their tools on specific vulnerabilities by taking the following *actions*:

- Probe
- Scan
- Flood
- Authenticate
- Bypass
- Spoof
- Read
- Copy
- Steal
- Modify
- Delete.

The specific *targets* addressed by these actions include

- Account
- Process
- Data
- Component
- Computer
- Network
- Internetwork.

The *unauthorized results* include

- Increased Access
- Disclosure of Information

- Corruption of Information
- Denial of Service
- Theft of Resources.

The *objectives* of all this effort include

- Challenge, Status, Thrill
- Political Gain
- Financial Gain
- Damage.

IV. Crimes where computers and networks are tools only

For the purposes of this *Encyclopedia*, this article makes a distinction between computer crimes that use computers and networks as tools versus those where the computers and networks are the primary targets of the crime as well as being tools. We start with computers and networks as tools.

A. Fraud

One of the most common forms of computer crime is data diddling – illegal or unauthorized data alteration. These changes can occur before and during data input or before output. Data diddling cases have included banks, payrolls, inventory, credit records, school transcripts, and virtually any other form of data storage known. In most of these cases, the purpose was to defraud victims by using the modified data to misrepresent reality and thereby to trick the victims into granting or allowing gain to the perpetrators.

1. The Equity Funding Fraud

Perhaps the most notorious case of computer-mediated fraud through data diddling was the *Equity Funding Fraud,* a case of organized data diddling on a scale unparalleled to date which took place from 1969 through 1972.

The case began with computer problems at the Equity Funding Corporation of America, a publicly-traded and highly successful firm with a bright idea. The idea was that investors would buy insurance policies from the company and also invest in mutual funds at the same time, with profits to be redistributed to clients and to stock-holders. Through the late 1960s, Equity's shares rose dizzyingly in price; there were news magazine stories about this wunderkind of the Los Angeles business community.

The computer problems occurred just before the close of the financial year. An annual report was about to be printed, yet the final figures simply could not be extracted from the mainframe. In despair, the head of data processing told the president the bad news; the report would have to be delayed. The president ordered him to make up the bottom line to show about $10,000,000.00 in profits and calculate the other figures so it would come out that way. The DP chief obliged, rationalizing it with the thought that it was just a temporary expedient, and could be put to rights later anyway in the real financial books.

The expected profit didn't materialize, and some months later, the head of DP was in trouble again. The books were not going to balance; where were the large inflows of cash from investors that the company had counted on? The executives at Equity manufactured false insurance policies which would make the company look good to investors. They inserted false information about nonexistent policy and identified the fraudulent records with special customer codes to exclude then from audit listings, thus tricking a lackadaisical auditor who saw only records which had corresponding paper files for real policyholders.

In time, Equity's corporate staff decided to sell the policies to other insurance companies via the redistribution system known as re-insurance, which spreads the risk of insurance policies across cooperating groups of insurers. The imaginary policies brought in large amounts of real cash. When it came time to start paying real money to the re-insurers for the policies in the names of fake people, the criminals "killed" the imaginary holders of the fake policies. Equity naturally demanded real money for the imaginary beneficiaries of the ghostly policy holders. Re-insurers poured cash into Equity -- over a million dollars for these false deaths.

By the spring of 1971, the executives were churning out from 20,000 to 50,000 fake policies per year; by 1972, 64,000 of the companies 97,000 policies were fraudulent. The face value of these invented people's insurance policies totaled $2.1 billion out of a total of $3.2 billion. About 25% ($185 M) of the company's total assets ($737 M) reported in 1971 were imaginary.

As has often happened in cases of conspiracy, an angry computer operator who had to work too much overtime reported the fraud to the Securities and Exchange Commission. Although the crooked managers tried to erase incriminating computer tapes, they were arrested, tried, and condemned to prison terms.

2. Vladimir Levin

In February 1998, Vladimir Levin was convicted to three years in prison by a court in New York City. Levin masterminded a major conspiracy in 1994 in which the gang illegally transferred $12M in assets from Citibank to a number of international bank accounts. The crime was spotted after the first $400,000 were stolen in July 1994 and Citibank cooperated with the FBI and Interpol to track down the criminals. Levin was also ordered to pay back $240,000, the amount he actually managed to withdraw before he was arrested. This case illustrates the international, boundary-crossing nature of today's computer-mediated crime.

3. Salamis

A particular kind of computer fraud is called the *salami* technique. In the salami technique, criminals steal money or resources a bit at a time. Two different etymologies are circulating about the origins of this term. One school of security specialists claim that it refers to slicing the data thin – like a salami. Others argue that it means building up a significant object or amount from tiny scraps – like a salami.

The classic story about a salami attack is the "collect-the-roundoff" trick. In this scam, a programmer modifies the arithmetic routines such as interest computations. Typically, the calculations are carried out to several decimal places beyond the customary 2 or 3 kept for financial records. For example, when currency is in dollars, the roundoff goes up to the nearest penny about half the time and down the rest of the time. If the programmer arranges to collect these discarded fractions of pennies in a separate account, a sizable fund can grow with no warning to the financial institution.

More daring salamis slice off larger amounts. The security literature includes case studies in which an embezzler removed $0.20 to $0.30 from hundreds of accounts two or three times a year. These thefts were not discovered or reported until an audit found them: most victims wouldn't bother finding the reasons for such small discrepancies.

In another scam, two programmers made their payroll program increase the federal tax-withholding amounts by a few cents per pay period for hundreds of fellow employees. The excess payments were credited to the *programmers*' withholding accounts instead of to the victims' accounts. At income-tax time the following year, the thieves received fat refunds from Internal Revenue.

In January 1993, four executives of a Value Rent-a-Car franchise in Florida were charged with defrauding at least 47,000 customers using a salami technique. The defendants modified a computer billing program to add five extra gallons to the actual gas tank capacity of their vehicles. From 1988 through 1991, every customer who returned a car without topping it off ended up paying inflated rates for an inflated total of gasoline. The thefts ranged from $2 to $15 per customer--rather thick slices of salami but nonetheless difficult for most victims to detect.

In 1998, In Los Angeles, district attorneys charged four men with fraud for allegedly installing computer chips in gasoline pumps that cheated consumers by overstating the amounts pumped. The problem came to light when an increasing number of consumers charged that they had been sold more gasoline than the capacity of their gas tanks. However, the fraud was difficult to prove initially because the perpetrators programmed the chips to deliver exactly the right amount of gasoline when asked for five- and ten-gallon amounts, which were the standard volumes used by inspectors.

4. Stock fraud

Fraud artists have used letters and newspapers to trick victims into giving away money for nothing; naturally, today's confidence tricksters use e-mail and the World Wide Web for similar purposes.

One of the more popular scams is the *pump-and-dump* stock fraud. The perpetrators uses e-mail or the Web to stimulate manipulate specific stocks; depending on when and how they buy the stocks, the crooks can make a profit either by raising the stock price or by lowering it. For example, a former employee of online press release distributor Internet Wire was arrested in August 2000 and charged with securities and wire fraud in connection with the distribution of a phony press release that sent a tech company's stock price plummeting the week before. Shares of Emulex, a maker of fiber-optic equipment, lost up to 60% of their value, most of it during one 15-minute freefall, after some financial news services, including Dow Jones and Bloomberg, ran stories based on the release. The suspect netted profits of $240,000.

B. Counterfeits of documents and money

Creating false documents long predates the use of computers; however, the digital scanners, digital-image editing programs, and high-resolution color printers have made forgeries easy. People have created convincing counterfeit money, sent authentic-looking faxes leading to the premature release of prisoners, and used impressive but false letters of recommendation – complete with digitized logos of prestigious institutions copied from Web sites – to get jobs for which they were unqualified.

One of the more ingenious forgeries occurred in the 1970s, when automatic processing of checks and deposits were still relatively new. A young man in Washington, DC printed his own account's routing numbers in magnetic ink at the bottom of the deposit slips he stole from a bank. He replaced the blank deposit slips in the public areas of the bank by the doctored ones. All the slips with magnetic ink were automatically sorted and processed, diverting $250,000 of other people's money into the criminal's bank account, from which the thief withdrew $100,000 and disappeared.

Credit-card numbers include *check-digits* that are computed using special algorithms to help prevent creation of authentic-looking account numbers. Unfortunately, programs for creating such authentic credit-card accounts, complete with check digits, are widely available in the computer underground. Even children have taken to forging credit-card numbers. For example, a 16-year-old Australian from Brisbane started defrauding businesses using stolen and forged credit-card numbers just after leaving school. By 1997, he had stolen $100,000 in goods and services. In October 1997, he pleaded guilty to 294 counts of fraud.

C. Extortion

Computer data can be held for ransom. For example, in an early case dating to 1971, two reels of magnetic tape belonging to a branch of the Bank of America were stolen at Los Angeles International Airport. The thieves demanded money for their return. The owners ignored the threat of destruction because they had adequate backup copies.

In the 1980s and 1990s, rumors persistently circulated in the financial community that banks and other institutions were giving in to extortion. For example, The June 3, 1996 issue of the *London Times* reported that hackers had been paid 400 million pounds sterling in extortion money to keep quiet about having electronically invaded banks, brokerage firms and investment houses in London and New York with logic bombs (programs with harmful effects that could be launched as a result of specific conditions such as a given date or time). According to the article, banks chose to give in to the blackmail over concerns that publicity about such attacks could damage consumer confidence in the security of their systems.

In September 1999, the *Sunday Times* of London reported that British banks were being attacked by criminal hackers attempting to extort money from them. The extortion demands were said to start in the millions and then run down into the hundreds of thousands of pounds. Mark Rasch, a former attorney for computer crime at the United States Department of Justice and later legal

counsel for Global Integrity, said, "There have been a number of cases in the UK where hackers have threatened to shut down the trading floors in financial institutions. . . . The three I know of (in London) happened in the space of three months last year one after the other. . . . In one case, the trading floor was shut down and a ransom paid." The International Chamber of Commerce (ICC) confirmed it had received several reports of attempted extortion.

There was a case of attempted extortion directed at a retail Web site in December 1999. A 19-year-old Russian criminal hacker calling himself Maxus broke into the Web site of CD Universe and stole the credit-card information of 300,000 of the firm's customers. When the company refused his $100,000 ransom, he posted 25,000 of the accounts on a Web site (Maxus Credit Card Pipeline). After investigation showed that the stolen card numbers were in fact being used fraudulently, 300,000 people had to be warned to change their card numbers.

In January 2000, information also came to light that VISA International had been hacked by an extortionist who demanded $10M for the return of stolen information — information that VISA spokesperson Chris McLaughlin described as worthless and posing no threat to VISA or to its customers. The extortion was being investigated by police but no arrests were made.

D. Slamming

Slamming is the fraudulent, unsolicited switching of long-distance services to another long-distance carrier; the practice has caused consternation among victims confronted with larger phone bills than they expected from their normal carrier. In mid-December1996, Connecticut's Department of Public Utility Control (DPUC) was slammed by a firm called Wiltel, which converted six of its 14 lines to its service without authorization.

By July 1997, the United States Federal Trade Commission were overwhelmed with over 16,000 complaints from enraged customers whose long-distance telephone service had been switched without their permission. For example, the Fletcher Companies engaged in systematic slamming and the United States Federal Communications Commission (FCC), responding to over 1400 complaints, fined the group of companies $5M in April 1998. In June 2000, long-distance company WorldCom Inc agreed to pay $3.5 million to settle an inquiry by the Federal Communications Commission into 2,900 complaints from persons charging that WorldCom telemarketers illegally switched them away from other phone service carriers. WorldCom president Bernard J. Ebbers said the slamming incidents were perpetrated by a few sales employees who were subsequently fired.

E. Industrial espionage

Teenage hackers who deface government sites or steal credit card numbers attract a lot of attention, but experts say the real problem of cybercrime is corporate-sponsored proprietary information theft committed by professionals who rarely get caught. According to a report from the American Society for Industrial Security in September 2000, Fortune 1000 companies sustained losses of more than $45 billion in 1999 from thefts of proprietary information, and a

survey by the Computer Security Institute in 2000 indicated over half of 600 companies polled said they suspected their competitors were a likely source of cyberattack.

In 1995, San Jose, CA prosecutors announced indictments in a case of industrial espionage in Silicon Valley. Two executives of the defunct Semiconductor Spares Inc. were charged with stealing over 500 technical drawings from Lam Research Corp.

In 1996, Britain's Davy International initiated a lawsuit over industrial espionage against the Austrian firm VA Technologie AG. In another case of alleged industrial espionage that came to light in 1996, the American subsidiary of Boehringer Mannheim Corp., a pharmaceutical firm based in Germany, accused Lifescan Inc., the diabetes-products division of Johnson & Johnson, of encouraging industrial espionage by presenting "Inspector Clouseau" and "Columbo" awards to employees who got the most information about their competitor, regardless of ethics.

In June 1997, two citizens of Taiwan were arrested after allegedly trying to bribe a Bristol-Myers Squibb Co. scientist into turning over technological secrets for the manufacture of Taxol, a drug used to fight ovarian cancer.

In 1998, Pixar, makers of the recent animated movie, "Toy Story," filed suit for a restraining order barring persons unknown from spreading stolen information about the salaries of their 400 employees. The report was widely circulated on the Net and damaged the company's ability to hire and retain employees (because competitors could outbid Pixar easily and inexpensively).

In a settlement of one of the few documented cases of industrial espionage involving intercepted e-mail, the Alibris company paid a $250K fine in 1999 for the firm it acquired in 1998. That company, Interloc, admitted intercepting and copying 4,000 e-mail messages sent to Amazon.com through its own ISP, Valinet. Prosecutors said that the e-mail was intercepted to gain a competitive advantage against Amazon in Interloc's own book business. The managers of Interloc steadfastly denied any wrongful intention but failed to explain why they copied the e-mail.

In June 2000, Microsoft complained that various organizations supporting Microsoft in its anti-trust battle with the United States government had been victimized by industrial espionage agents who attempted to steal documents from trash bins.

Echelon, an international surveillance network, was in the news in the late 1990s. Echelon, which is jointly operated by the U.S., the U.K., Australia, Canada and New Zealand, is capable of intercepting phone, fax and e-mail signals around the world and is intended to gather intelligence regarding terrorist and other threats to the U.S. and its allies. In 1997, the *Covert Action Quarterly*, an intelligence newsletter, said: "Unlike many of the electronic spy systems developed during the Cold War, Echelon is designed primarily for non-military targets: governments, organizations, businesses, and individuals in virtually every country. It potentially affects every person communicating between (and sometimes within) countries anywhere in the world." In July 2000, the European Parliament renewed its attack on Echelon by forming a temporary committee to investigate whether the spy network was used for commercial espionage

against European businesses. The parliament said the committee would also determine Echelon's legality. Later in 2000, a Green Party member of the European Parliament filed criminal charges in Germany against Echelon.

F. Gambling

One of the more lucrative scams focuses on bilking credulous gamblers by offering games of chance and betting on sports and other events via the Internet. Interstate gambling is illegal in the United States, but the operators of the gambling sites have been setting up their servers in offshore locations, free of U.S. law. The likelihood that any of the games of chance are in fact programmed to be honestly conducted is unknown. In one embarrassing incident in 1998, an analyst discovered that nobody who chose the digit "9" as part of their bet ever won the Arizona Lottery's new Pick 3 game -- because the algorithm was incapable of generating a 9 in the winning three-digit numbers. Observers noted that the risk of accidental or deliberate distortions of probability distributions might be even higher in software written by unknown persons working for unknown private organizations in offshore locations. If gambling is a tax on people with a limited understanding of probability, offline gambling seems like a tax on people with limited reasoning powers.

G. Auctions

Auctions have always been a risky way to buy goods, since dishonest sellers can engage *shills* to pretend to bid the price of an item up beyond its value. The risk is higher when goods have no intrinsic value but depend solely on demand for determination of the price. When there is no visual contact or screening of the participants in the group bidding for an item, however, the risk is much greater.

Another aspect of online auctions is the possibility of buying stolen or illegal goods. For example, in September 1999, someone put up a human kidney for sale through the online auction-house eBay and received bids of up to $5.8M. The auction service canceled the sale because selling human organs is a Federal felony with up to $250,000 in fines and at least 5 years in jail. Other offers – some of which may have been pranks – included an offer to sell a human baby; prices (possibly also from pranksters) had reached over $100,000 before eBay interrupted the (illegal) sale.

Online auctions have become the most serious source of complaints to the Internet Fraud Complaint Center, a project of the FBI and the Department of Justice. In November 2000, the Center opened and began receive more than 1,000 complaints a day. However, the online auction industry denies that fraud is a serious problem, and eBay says that only one of every 40,000 listings has resulted in a confirmed case of fraudulent activity. Complaints about Internet fraud can be reported to http://www.ifccbi.gov .

H. Pornography

Some monitors think that pornography is the single largest money-making use of the Internet and the World Wide Web. Pornography is governed by different standards in different countries, but all countries ban the creation, distribution and storage of *child pornography*. Many pornographers use tricks such as registering their domains with misleading names; a well-known example is http://www.whitehouse.com , which plays on novices' ignorance of the naming standards (U.S. government agencies have domain names ending in .gov, not .com). Other tricks include using misspellings. At one time, for example, a pornographer registered several misspellings of "microsoft.com;" people were astonished at what they would see appearing on screen after typing, say, http://www.micosoft.com . Trademark owners have been successful in stopping this obvious abuse of their trademark through civil litigation, but the pornographers keep coming up with alternatives.

I. Stalking and assault

Some of the worst abuses of the new communications media have involved lies by pedophiles. These sexual predators have successfully used e-mail and especially children's *chat rooms* to misrepresent themselves to naïve children as if they were in the same age range. The Internet Crime Forum in the U.K. reported in December 2000 that they estimate 20% of the children online have been approached by pedophiles. Pedophiles have exacerbated conflicts between their victims and their parents, lured youngsters into concealing their communications, persuaded them to send pornographic videos of themselves and even convinced a few to travel without parental approval for meetings with their new "friends." In January 2001, for example, a 32-year-old man was charged with raping a 14-year-old central upstate New York girl he met in an Internet chat room and lured to a hotel room in Albany, NY.

J. Libel, misrepresentation and harassment

The ease with which anyone can forge the identifying information used in e-mail or use pseudonyms on discussion groups has resulted in many instances of libel, distortion, misrepresentation, and harassment. For example, criminals sent out thousands of racist, hateful e-mail messages in the name of a Texas university professor who subsequently needed police protection for his home and family. Another criminal posted a victim's phone number in chat rooms catering to phone-sex enthusiasts and described the young woman in question as a prostitute. She had to change her phone number to escape hundreds of salacious callers a day.

Another kind of harassment is unsolicited commercial e-mail (often called "spam", much to the disgust of the trademark owner for the luncheon meat called *Spam*). Spammers often use anonymous e-mail identities to flood the Net with millions of unwanted advertising messages, much of it fraudulent. Some jurisdictions (e.g., Washington, Virginia and Massachusetts) have criminalized the use of *forged headers* in such e-mail. Many observers predict that unsolicited commercial e-mail will eventually be regulated as unsolicited facsimile (fax) messages were in the 1980s.

A different kind of junk e-mail is hoaxes and hoax virus warnings. These nuisances spread through the ill will of pranksters who write or modify the hoaxes and, unfortunately, through the good will of credulous novices who cannot recognize the nonsense they are obediently forwarding to everyone they know. Pathognomonic signs of a hoax include:

- Absence of a specific date, name of contact, or originating organization's Web site;
- Absence of a valid digital signature;
- Improbably catastrophic effects or consequences of a supposed danger;
- Use of exclamation marks, ALL CAPS TEXT and presence of misspellings;
- Claims that anyone can monitor exactly how many e-mails are sent with copies of the message;
- Instructions to send the message to "everyone you know."

K. Theft of intellectual property

Electronic communications are ideal for sharing files of all kinds; unfortunately, some people share other people's property. In 1999 and 2000, concern grew in the recording industry over the widespread pirating of music tracks through a variety of networks such as MP3.com, Napster, Gnutella and others. At some universities, traffic in unauthorized copies of songs (and later, videos) grew so frantic that available bandwidth was exhausted, leading to prohibitions on such transfers and stringent filtering at the firewalls. After extensive negotiations, several copyright-violation lawsuits and considerable debate among people with divergent views on the ownership of commercial music and video, several facilitating companies in the U.S. agreed to cooperate with the entertainment industry to provide access to their products at reasonable cost.

V. Where computers, networks and software are the targets as well as tools

In a sense, any attack on a computer is an attack on its users. However, this section focuses on types of crime where interference with the computing equipment and communications networks are themselves prime targets, not just incidental mechanisms in the crime.

A. Denial of Service and Jamming

Saturating resources without falling afoul of security restrictions has been a common attack method for decades. However, such *denial of service* (DoS) attacks have grown rapidly in frequency and severity in recent years. Factors contributing to such harassment techniques include

- The explosive growth of Internet access by individuals, including children, in the 1990s
- The growing number of sites online
- Faster modems
- Widespread distribution of attack scripts
- A subculture of criminal hacking
- Easy anonymity on the Net.

E-mail bombing is a popular method; for example, in one case a victim received 25,000 identical e-mail messages containing the single word "IDIOT." *Subscription-list bombing* involves subscribing victims to hundreds of list servers; in an early case, the criminal calling itself "Johnny [x]chaotic" harassed several dozen recipients with thousands of postings from these unwanted subscriptions. This technique is harder to use today because list servers typically now ask for a written confirmation of all subscription requests.

Another kind of DoS often occurs by mistake: *mailstorms* occur when an autoresponder sends mail to another autoresponder, which sends mail back to the originating autoresponder. Mailstorms can generate thousands of messages very quickly, causing mailboxes to reach their limits and even crashing susceptible systems. Such feedback loops can be exploited by an attacker who forges a REPLY-TO address in an e-mail message designed to spark such a storm. Mailstorms are greatly amplified when a list server can be tricked into communicating with an autoresponder.

Many other types of DoS attacks use attributes of TCP/IP. Some involve sending malformed datagrams (packets) that crash recipient processes (e.g., Ping of Death); others send bad data to a process (e.g., buffer-overflow attacks).

Towards the middle of 1999, security agencies noticed that a new generation of DoS attacks were brewing: *Distributed DoS* (DDoS). In these attacks, criminals use automatic scanning software to identify systems with known vulnerabilities and install *slave* (also known as *zombie*) programs that initiate concealed (*stealth*) processes (*daemons*) on the victimized machines. These zombies wait for encrypted instructions from a *master* program controlled by the criminals; at a specific time, hundreds or thousands of zombies can be ordered to use their host-machine's resources to send an overwhelming flood of packets to the ultimate victim machines. Such attacks materialized in February 2000, when major Web sites such as eBay, Amazon and other high-profile systems were swamped with so much spurious traffic that they were unable to service legitimate users. Damages were estimated in the tens of millions of dollars.

B. Penetration

The classic computer crime is *penetration* of a security perimeter. Such penetration has become a hobby with a subculture of criminal hackers, but it can also be part of a more serious effort to obtain information illicitly. The popular press frequently includes reports of such penetrations; perhaps one of the most spectacular recent cases in terms of publicity occurred in October 2000, when Microsoft reported that criminal hackers appeared to have entered their production systems and made copies of valuable source code for the latest versions of its flagship MS-Windows and MS-Office products.

Most penetration occurs through exploitation of known security vulnerabilities. Although *patches* are known and available for new vulnerabilities within hours or days, many overworked or untrained or careless system administrators fail to install these patches. All studies of known vulnerabilities have the same result: a majority (two-thirds and up) of all Net-connected systems have old, unpatched vulnerabilities that can be penetrated even by children (*script-kiddies*) using automated tools (*exploits, scripts*) they barely understand.

Another class of attacks involves *social engineering*, which is the hacker phrase for lying, cheating, dissimulation, impersonation, intimidation, seduction and extortion. Criminals such as the notorious Kevin Mitnick use such techniques in persuading employees to betray user identification and authentication codes that can then be used for surreptitious access to systems.

So many Web sites are vandalized by the criminals who penetrate their inadequate security perimeters that the incidents now barely make the news. Archives of copies (*mirrors*) of the vandalized pages are available on the Web; e.g., http://www.antionline.com . Most of the vandalized pages are not suitable for viewing by children due to the presence of foul language, bad grammar, and lots of pornographic images; ironically, it is thought that most of the vandalism is *by* children, many of whose parents are delighted that their unsupervised offspring are ensconced in front of a computer "keeping out of trouble."

An important point about all penetrations is that, contrary to criminal-hacker cant, all penetrations are harmful. Criminal propaganda claims that unauthorized entry is harmless as long as no data are modified; some go further and argue even against unauthorized disclosure of confidential data. However, operations staff know that when intruders break into any system, they destroy the basis for trust of that violated system. All data and all software must be validated after every penetration; such work is tedious, difficult and expensive.

C. Covert Breaches of Confidentiality

Even without breaching the security perimeter in an obvious fashion, criminals can intercept confidential communications. For example, in August 1997, three New Jersey businessmen were arrested and charged with illegally intercepting and selling messages sent via a paging service to the senior New York City officials such as the mayor, top police officers and leaders of the fire department. Interception of domestic cordless telephones is an easy method for collecting information that can be used for blackmail or for sale to unscrupulous buyers. Many

wireless mobile phones still use no encryption and their signals can be intercepted by commonly-available equipment (with minor modifications) costing a few hundred dollars. Land-lines are easy to tap at the point-of-presence of the telephone company, at the neighborhood distribution cabinet, or – in office buildings – in the usually-unlocked junction panels in basements or corridor walls.

Another form of electronic eavesdropping involves the use of *spyware*. Some software is written to allow automatic transmission of information from a user's system to specified sites on the Internet. A typical and harmless example is the registration process of many products; the user has a choice on whether to transmit information or not, and if so, how (by modem, by Internet connection, by fax, or by mail). Spyware, in contrast, by definition conceals its transmissions. Users with *firewalls* that monitor inbound and outbound TCP/IP communications may be surprised by occasional requests for outbound transmission from processes they know nothing about. For example, Comet Systems cute cartoon cursors were downloaded by millions of people, many of them children. However, the free software turned out to be a Trojan: the modified programs initiated TCP/IP communications through the users' Internet connections and reported on which sites were being visited by each copy of the programs when the users went to any of 60,000 sites providing links to the cursor programs. Purpose: gathering statistics about Web usage patterns. Company officials argued that there were no links between the serial numbers and any identifying information about the users. Privacy advocates argued that the reporting function ought to have been overt and optional.

D. Viruses, Worms and Trojans

Disregarding DNA, which is the ultimate self-reproducing information-storage structure, self-reproducing computer programs and processes have been around since the Bell Labs scientists started playing "Core Wars" on company mainframes in the 1960s.

1. Early viruses

Hobbyists in the 1980s had more scope for their experiments because the operating systems of personal computers lacked a security kernel and therefore allowed any process to access any part of memory. Apple II microcomputer users invented computer viruses in the early 1980s such as Festering Hate, Cyberaids and Elk Cloner. In 1983, Fred Cohen, then a student, created a self-replicating program for a VAX 11/750 mainframe at the University of Southern California. His thesis advisor, Len Adelman, suggested calling it a virus. Cohen demonstrated the virus to a security class. Cohen continued his work on viruses for several years; his PhD thesis presented a mathematical description of the formal properties of viruses. He also defined viruses neatly and simply as "A computer program that can infect other computer programs by modifying them to include a (possibly evolved) copy of itself."

On October 22, 1987, a virus apparently written by two brothers in Lahore, Pakistan was reported to the Academic Computer Center of the University of Delaware in Newark. This virus

destroyed the data on several hundred diskettes at U of D and also at the University of Pittsburgh School of Business. It destroyed the graduate thesis of at least one student.

In November 1987, students at Lehigh University in Bethlehem, PA began complaining to the staff at the computer center that they were getting bad diskettes. At one point, 30 students returned diskettes in a single day. It turned out that there was a virus adding itself to the COMMAND.COM file on the DOS system diskettes. When the Lehigh staff examined the virus, they discovered that it was programmed to copy itself four times after each infection. On the fourth replication for any given copy, the virus would destroy the file allocation table of the diskette or hard disk, making the data unrecoverable (at that time, there were no utilities available for reconstituting files easily once the pointers from cluster to cluster on the disk had been lost). Several hundred students lost their data.

Until 1995, there were two main virus *vectors* and therefore *types*: *boot-sector* viruses and *file-infectors*. There were a few thousand distinct *kinds* of viruses (defined by *signature strings* of specific recognizable executable code) and industry surveys suggested that the rate of infection (measured in terms of numbers of PCs infected) was rising tenfold per year. Viruses were restricted to single *platforms*: MS-DOS, MS-Windows and the Apple Macintosh operating system. UNIX and other operating systems with real security features were largely unaffected.

In August of 1995, everything changed. Reports appeared of a new form of harmful self-replicating code: macro-language viruses. The first instance, dubbed "winword.concept" by anti-virus specialists, contained no harmful *payload*: it merely contained text explaining that it was an illustration of the concept of *macro viruses*. Within the next few years, macro viruses came to dominate the lists of virus types. By January of 2001, there were over 56,000 viruses in antivirus laboratories, of which more than half were macro viruses. However, in the wild, almost all infections were by macro viruses. In the *2000 Annual Virus Prevalence Survey* run by ICSA Labs, there were no significant reports of boot-sector or file-infector viruses in the population studied.

The dominance of macro viruses is due to their cross-platform capability. Microsoft decided to ignore warnings by security specialists and incorporated extensive macro capabilities into its MS-Office products – products that run under a number of different operating systems. The default state allows automatic execution of such macros without direct user intervention, leading to the situation we face today. The problem has been exacerbated in the final years of the 1990s because Microsoft also decided to incorporate automatic execution of *any* executable attachment to e-mail received in its MS-Outlook products.

2. Worms

a. Early worms

In December 1987, a German student released a self-reproducing program that exploited electronic mail networks on the ARPANET and BITNET networks. This program would display the request, `Please run me. Don't read me.' While the victim ran the program, it displayed a Christmas tree on screen; at the same time, it used the victim's email directory and automatically sent itself to everyone on the list. Because this rogue program did not embed itself into other programs, experts call it the Christmas-Tree Worm.

Unfortunately, this worm had no mechanism for remembering where it had come from. Since most people to whom we write include our names in their address list, the worm usually mailed itself back to the computer system from which it had originated as well as to all the other computer systems named in the victim's directory. This reflection from victim to infector reminds me of an uncontrolled nuclear chain reaction. The greater the number of cross references among email address directories, the worse would be the growth of the worm.

The original version of this worm worked only on IBM VM/VMS mainframe computers; luckily, there weren't very many of them on the ARPANET and BITNET networks. However, a source-code version of the worm was installed into the IBM internal email network and recompiled. Because of the extensive cross-references in the email system, where many employees corresponded with hundreds of other employees, the worm reproduced explosively. According to Phillips, the network was clogged for three hours before IBM experts identified the problem, wrote an eradicator, and eliminated the worm.

b. The Morris Worm of 1988

The first worm that garnered worldwide attention was a self-reproducing program launched at 17:00 EST on the 2nd of November 1988 by Robert T. Morris, a student at Cornell University in Ithaca, New York. In addition to sending itself to all the computers attached to each infected system, the worm superinfected its hosts just like the Christmas-Tree Worm had done, leading to slowdowns in overall processing speed. By the next morning, the Internet was so severely affected by the multitudes of copies of the worm that some systems administrators began cutting their networks out of the Internet. The Defense Communications Agency isolated its Milnet and Arpanet networks from each other around 11:30 on November 3rd.

By late on November 4th, a comprehensive set of patches was posted on the Internet to defend systems against the Worm. That evening, the author of the Worm was identified. By November 8th, the Internet seemed to be back to normal. A group of concerned computer scientists met at the National Computer Security Center to study the incident and think about preventing recurrences of such attacks. The affected systems were no more than 5% of the hosts on the Internet, but the incident alerted administrators to the unorganized nature of this worldwide network. The incident contributed to the establishment of the Computer Emergency Response

Team Coordination Center at the Software Engineering Institute of Carnegie-Mellon University, whose valuable Web site is at http://www.cert.org .

In 1990, Morris was found guilty under the Computer Fraud and Abuse Act of 1986. The maximum penalties included five years in prison, a $250,000 fine and restitution costs. Morris was ordered to perform 400 hours of community service, sentenced to three years probation, and required to pay $10,000 in fines. He was expelled from Cornell University. The Supreme Court of the United States upheld the decision by declining to hear the appeal launched by his attorneys.

c. The Melissa Worm

On Friday 26 March 1999, the CERT-CC received initial reports of a fast-spreading new MS-Word macro virus. *Melissa* was written to infect such documents; once loaded, it used the victim's MAPI-standard e-mail address book to send copies of itself to the first 50 people on the list. The virus attached an infected document to an e-mail message with subject line "Subject: Important Message From <name>" where <name> is that of the inadvertent sender. The e-mail message read, "Here is that document you asked for ... don't show anyone else ;-)" and included an MS-Word file as an infected attachment. The original infected document, "list.doc" was a compilation of URLs for pornographic Web sites. However, as the virus spread it was capable of sending any other infected document created by the victim.

Because of this high replication rate, the virus spread faster than any previous virus in history. On many corporate systems, the rapid rate of internal replication saturated e-mail servers with outbound automated junk e-mail. Initial estimates were in the range of 100,000 downed systems. Anti-virus companies rallied immediately and updates for all the standard products were available within hours of the first notices from CERT-CC.

The Melissa macro virus was quickly followed by the PAPA MS-Excel macro virus with similar properties.

d. The Love Bug

In May 2000, the I LOVE YOU ("Love Bug") computer worm struck computers all over the world, starting in Asia, then Europe. The malicious software spread as an e-mail attachment, sending itself to all the recipients in standard e-mail address books. Within days, new variants appeared; for example, one variation used a subject line purporting that the carrier message contained a joke. These worms not only spread via e-mail, they also destroyed files on the infected systems.

Within a week, Philippine authorities detained several young people for questioning after the computer used to launch the worm. On the 11th of May, Filipino computer science student Onel de Guzman of AMA Computer College in Manila told authorities that he may accidentally have launched the Love Bug but he did not take responsibility for creating it, saying in Tagalog: "It is one of the questions we would rather leave for the future." All suspects were released without

prosecution because of the absence of laws in their country that would criminalize their alleged actions.

3. Trojans

a. Early Trojans

Helpful volunteers in the early 1980s distributed a great deal of useful software for free; such *freeware* became a blind for malefactors who wrote harmful programs but described them as useful utilities. In March 1988, users noticed a supposed improvement to the well-known anti-virus program Flu-Shot-3. Flu-Shot-4 was a Trojan, however, and it destroyed critical areas of hard disks and floppy disks. One of the interesting aspects of this Trojan was that it was an early user of the *stealth technique* of self-modifying code: the harmful assembler instructions were generated only when the program was run, making it harder for conventional anti-virus signature scanner programs to identify it.

Other famous early Trojans included the supposed keyboard driver KEYBGR.COM which displayed a smiley face that moved randomly around on screen; the 12-Tricks Trojan, which was advertised as a hard-disk diagnostic program but actually caused a wide range of damage such as garbling print output and reformatting hard disks. A particularly notorious Trojan was the PC Cyborg or AIDS Trojan, which claimed to be an AIDS information program but actually used a simple monoalphabetic character substitution code to scramble the names of all files and directories as well as using up all free space on disk and issuing fake error messages for all DOS commands.

b. The Moldovan pornography scam

In late 1996, viewers of pornographic pictures on the http://www.sexygirls.com site were in for a surprise when they got their next phone bills. Victims who downloaded a "special viewer" were actually installing a Trojan Horse program that silently disconnected their connection to their normal ISP and reconnected them (with the modem speaker turned off) to a number in Moldova in central Europe. The long-distance charges then ratcheted up until the user disconnected the session – sometimes hours later, even when the victims switched to other, perhaps less prurient, sites. AT&T anti-fraud staff spotted the problem because of unusually high volume of traffic to Moldova, not usually a destination for many U.S. phone calls. A federal judge in New York City ordered the scam shut down. In November 1997, the US Federal Trade Commission won $2.74M from the bandits to refund to the cheated customers.

c. Back Orifice

In July 1998, *The Cult of the Dead Cow* (cDc, a long-running group supporting criminal hacking activities) announced BackOrifice (BO), a tool for analyzing and compromising MS-Windows security and named as a spoof on the *Back Office* product from Microsoft. The author, a hacker with the L0PHT group (http://www.l0pht.com), described the software as follows: "The main legitimate purposes for BO are remote tech support aid, employee monitoring and remote

administering [of a Windows network]." However, added the cDc press release, "Wink. Not that Back Orifice won't be used by overworked sysadmins, but hey, we're all adults here. Back Orifice is going to be made available to anyone who takes the time to download it [read, a lot of bored teenagers]." The product featured image and data capture from any Windows system on a compromised network, an HTTP server allowing unrestricted I/O to and from workstations, a packet sniffer, a keystroke monitor, and software for easy manipulations of the victims' Internet connections. BO's description qualified it as a Trojan that allowed infection of other applications and used stealth techniques to erase its own visibility once loaded into memory. Security experts pointed out that the key vulnerability allowing BO to contaminate a network was the initial step – running a corrupted application that would load the parasitic code into memory. Users should not download software from unknown sites or execute attachments to e-mail without assurance of their legitimacy. All the major firms offering anti-malicious-code software issued additions to their signature files to identify the Trojan code.

About 15,000 copies of BO were distributed to Internet Relay Chat users by a malefactor who touted a "useful" file (*nfo.zip*)that was actually a Trojan dropper for BackOrifice.

In July 1999, cDc released BackOrifice 2K (BO2K), usually installed illegally on victim machines through a contaminated vector program that has been thereby transformed into a Trojan horse dropper. BO2K allowed complete remote control and monitoring of the infected PCs. BO2K was noteworthy because it attacked WindowsNT workstations and servers and thus has even more serious implications for information security. Anti-virus companies worked feverishly immediately after the release of the tool to update their virus-signature files. A criminal hacker calling himself Deth Veggie insisted that the CDC was involved in guerilla quality assurance — their penetration tools, he argued, would force Microsoft to repair the "fundamentally broken" Windows operating systems. Security specialists disagreed, saying that writing and releasing such tools was definitely malicious and were primarily damaging innocent users."

E. Logic bombs

A logic bomb is a program which has deliberately been written or modified to produce results when certain conditions are met that are unexpected and unauthorized by legitimate users or owners of the software. Logic bombs may be within standalone programs or they may be part of worms or viruses. An example of a logic bomb is any program which mysteriously stops working three months after, say, its programmer's name has disappeared from the corporate salary database.

In 1985, a disgruntled computer security officer at an insurance brokerage firm in Texas set up a complex series of Job Control Language (JCL) and RPG programs described later as "trip wires and time bombs." For example, a routine data retrieval function was modified to cause the IBM System/38 midrange computer to power down. Another routine was programmed to erase random sections of main memory, change its own name, and reset itself to execute a month later.

In 1988, a software firm contracted with an Oklahoma trucking firm to write them an application system. The two parties disagreed over the quality of the work and the client withheld payment, demanding that certain bugs be fixed. The vendor threatened to detonate a logic bomb which had been implanted in the programs some time before the dispute unless the client paid its invoices. The client petitioned the court for an injunction to prevent the detonation and won its case on the following grounds:

- The bomb was a surprise--there was no prior agreement by the client to such a device.
- The potential damage to the client was far greater than the damage to the vendor.
- The client would probably win its case denying that it owed the vendor any additional payments.

In public discussions among computer programmers and consultants, some have openly admitted installing such logic bombs in their customers' systems as a tool for extorting payment.

In 1998, a network administrator for Omega Engineering was convicted of activating a digital time bomb that destroyed the company's most critical manufacturing software programs. The company claimed more than $10 million in damages and lost productivity.

F. Sabotage

The quintessential sabotage story concerns the National Farmers Union Service Corporation of Denver, where a Burroughs B3500 computer suffered 56 disk head crashes in two years starting in 1970. Down time was as long as 24 hours per crash, with an average of 8 hours per incident. Technicians guessed that the crashes were due to bad power; the company spent $500,000 upgrading their power. The crashes continued.

The investigators began wondering about sabotage; all the crashes had occurred at night – specifically during a trusty operator's shift, old helpful Albert. Management installed a closed-circuit TV (CCTV) camera in the computer room – without informing Albert. Film of the next crash showed good ol' Albert opening up a disk cabinet and poking his car key into the read/write head solenoid, shorting it out and causing the 57th head crash.

Psychologists determined that Albert had been ignored and isolated for years in his endless night shift. When the first head crashes occurred spontaneously, he had been surprised and excited by the arrival of the repair crew. He had felt useful, bustling about, telling them what had happened. When the crashes had become less frequent, he had involuntarily, and almost unconsciously, re-created the friendly atmosphere of a crisis team. He had destroyed disk drives because he needed company.

Many other cases of sabotage involve disgruntled employees or ex-employees.

However, other cases do involve outsiders. For example, in the late 1980s, a New Jersey magazine publisher's voice mail system was corrupted a 14-year old boy and his 17-year old cousin, both residents of Staten Island. The younger child had ordered a subscription to a magazine dedicated to Nintendo games and never received the colorful $5 poster he had been promised. In retaliation, the children entered the company's voice mail, cracked the maintenance account codes and took over the system. They erased customer messages, changed employees' answering messages, and generally wreaked havoc. Their actions resulted in lost revenue, loss of good will, loss of customers, expenses for time and materials from the switch vendor, and wasted time and effort by the publisher's technical staff. Total costs were estimated by the victim at U$2.1M.

We have already seen that Web-site defacement, a form of sabotage, is so common that it no longer warrants much news coverage.

G. Counterfeit Software

All over the world, opportunistic criminals make illegal copies of copyrighted software. The problem is particularly serious throughout Asia, where some countries have more than 99% of all software in pirated form; however, counterfeit software is big business even in the U.S. For example, in June 2000, Pennsylvania State Police cracked a global software piracy operation involving at least $22M in counterfeit Microsoft software. Police collected over 8,000 copies of Windows 98, Microsoft Office and Windows NT and more than 25,000 counterfeit end-user license agreements. Authorities pointed out the following warning signs of counterfeit software:

- Impossibly low prices
- Unwillingness of companies or individuals to verify their identity or contact information
- Online distributors with inadequate descriptions of return and warranty policies
- Non-standard packaging such a CD in a jewel case but no documentation or authentication marks.

An unfortunate side-effect of the ease with which ordinary users can copy software – including even burning their own CD-ROMs – is that many adults and especially children have no clear conception that there is anything wrong with making copies of software for their friends and even for sale. In the U.S., however, penalties for copyright violations can reach as high as fines of $250,000 *per title* and up to five years in prison.

V. For further reading

Cavazos, E. & G. Morin (1996). *Cyberspace and the Law: Your Rights and Duties in the On-Line World.* MIT Press (Cambridge, MA). ISBN 0-262-53123-2. 220 pp. Index.

Fialka, J. J. (1997). *War by Other Means: Economic Espionage in America.* W. W. Norton (New York). ISBN 0-393-04014-3. xiv + 242. Index.

Fraser, B. (1997), ed. *Site Security Handbook.* RFC2196 (Network Working Group). http://www.cis.ohio-state.edu/htbin/rfc/rfc2196.html

Freedman, D. H. & C. C. Mann (1997). *@Large: The strange case of the world's biggest Internet invasion.* Simon & Schuster (New York). ISBN 0-684-82464-7. 315 pp. Index.

Howard, J. D. (1997). *An Analysis of Security Incidents on the Internet 1989 – 1995.* PhD Thesis accepted by the Department of Engineering and Public Policy, Carnegie Institute of Technology at Carnegie Mellon University. http://www.cert.org/research/JHThesis/Start.html

Icove, D., K. Seger, W. VonStorch (1995). *Computer Crime: A Crime Fighter's Handbook.* O'Reilly & Associates (Sebastopol, CA). ISBN 1-56592-086-4, $24.95 US.

Lessig, L., D. Post & E. Volokh (1997). *Cyberspace Law for Non-Lawyers.* Published via e-mail. http://www.ssrn.com/update/lsn/cyberspace/csl_lessons.html

Littman, J. (1996). *The Fugitive Game: Online with Kevin Mitnick--The Inside Story of the Great Cyberchase.* Little, Brown and Company (Boston). ISBN 0-316-5258-7. x + 383.

Parker, D. B. (1998) *Fighting Computer Crime: A New Framework for Protecting Information.* Wiley (NY) ISBN 0-471-16378-3. xv + 500 pp; index

Power, R. (2000). *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace.* Que. ISBN: 0-78972-443-X. 450 pp.

Schwartau, W. (1996). *Information Warfare, Second Edition.* Thunder's Mouth Press (New York). ISBN 1-56025-132-8. 768 pp. Index.

Shimomura, T. & J. Markoff (1996). *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw--by the Man Who Did It.* Hyperion (New York). ISBN 0-7868-6210-6. xii + 324. Index.

Slatalla, M. & J. Quittner (1995). *Masters of Deception: The Gang that Ruled Cyberspace.* HarperCollins (New York). ISBN 0-06-017030-1. 225 pp.

Smith, G. (1994). *The Virus Creation Labs: A Journey into the Underground*. American Eagle Publications (Tucson, AZ). ISBN 0-929408-09-8. 172 pp.

Sterling, B. (1992). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Bantam Doubleday Dell (New York). ISBN 0-553-08058-X. xiv + 328. Index.

Stoll, C. (1989). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. Pocket Books (Simon & Schuster, New York). ISBN 0-671-72688-9. viii + 356.

Tipton, H. F. & M. Krause (2000), eds. *Information Security Management Handbook, 4th edition.* Auerbach (Boca Raton, FL). ISBN 0-8493-9829-0. xiii + 711. Index.