

7 Computer Crime

7.1 Introduction

Computers and the Internet also make many illegal activities easier for criminals: the distribution of child pornography, copyright infringement, and stock manipulation.

Computers and the Web provide a new environment for fraud, embezzlement, theft, forgery, and industrial espionage.

Crimes committed with computers and on the Web are more devastating and harder to detect than similar crimes committed without computers.

A thief who steals a credit card gains access to a much larger amount of money than the thief who stole a wallet in the past with only cash.

Criminals can steal, commit fraud, or destroy data from miles away or from another country, by modem.

A 1907 magazine called telephone companies “allies of the criminal pool-rooms.”

7.2 Hacking

7.2.1 What is “Hacking”?

We describe three phases of hacking:

Phase 1—the early years (1960s and 1970s), when hacking was a positive term;

Phase 2—the period from the 1970s to the 1990s, when hacking took on its more negative meanings.

Phase 3—beginning in the mid-1990s with the growth of the Web and of e-commerce and the participation of a large portion of the general public online.

PHASE 1:

In the early days of computing, a “hacker” was a creative programmer who wrote very elegant or clever programs. A “good hack” was an especially clever piece of code.

The early hackers were interested primarily in learning and in intellectual challenges—they frowned on doing damage.

PHASE 2:

Hacking behavior included pranks, thefts, and *phone phreaking* (manipulating the telephone system).

Hacking a computer at a big research center, corporation, or government agency was a challenge that brought a sense of accomplishment, a lot of files to explore, and respect from one’s peers.

Hackers committed pranks and small crimes, spoofed e-mail, hacked a credit-reporting service, hacked a McDonald’s payroll computer, using programs called “sniffers,” they extracted passwords.

A Russian man, with accomplices in several countries, used stolen passwords to steal \$400,000 from Citicorp.

Kevin Mitnick is one of the more notorious hackers of the 1980s. Tracked down and arrested in 1995, he was a fugitive who had gone into hiding while on probation for a 1988 hacking conviction.

The damage done by Mitnick was estimated at several million dollars.

The vulnerability of the Internet as a whole was demonstrated by Robert T Morris with his Internet Worm in 1988.

The worm spread quickly to computers running particular versions of the UNIX operating system.

The worm disrupted research and other activities and inconvenienced a large number of people. This incident raised concern about the potential to disrupt critical computer services and cause social disruption.

A worm is a program that copies itself to other computers. The concept was developed to make use of idle resources, but was adopted by people using it maliciously. A worm might destroy files or just use resources.

PHASE 3: THE WEB ERA

Hacking now affects almost everyone. With basic infrastructure systems (for example, water and power, hospitals, transportation, emergency services, in addition to the telephone system) accessible on the Net, the risk increased.

Even before Windows 98 was shipped, a hacker wrote a virus for it.

Hackers modified the programming at an online gambling site so that everyone won; the site lost \$1.9 million.

By mid-2001, attrition.org's online archive had copies of more than 15,000 defaced Web pages. In the U.S., hackers modified or defaced the Web pages of the White House, the Bureau of Labor Statistics, and the FBI. They revised the Department of Justice page to read "Department of Injustice" in protest of the Communications Decency Act. They changed the CIA's site to read "Central Stupidity Agency" and added links to pornography sites.

According to the FBI, hacker groups in Russian and the Ukraine broke into more than 40 online businesses and stole more than a million credit-card numbers.

After Creditcards.com refused to pay for 55,000 stolen card numbers, hackers posted the numbers on Web sites in three countries.

Hackers in England impersonated air-traffic controllers and gave false instructions to pilots. In 1998, the U.S. Deputy Defense Secretary described a series of attacks on numerous U.S. military computers as "the most organized and systematic attack the Pentagon has seen to date." Two boys, aged 16 and 17, were caught and pleaded guilty.

In 2000, the "Love Bug," or "ILOVEYOU" virus, spread around the world in a few hours, propagating among computers using Microsoft's Windows and Outlook programs.

The virus hit tens of millions of computers worldwide and did an estimated \$10 billion in damage.

In 2000, almost a dozen major Web sites were shut down, some for several hours, by *denial-of-service attacks*. Victims included Yahoo!, eBay, Amazon, E*Trade, Buy.com, CNN, and others.

The requests were generated by programs planted on numerous other systems to disguise their origin; thus it is also called a *distribution denial-of-service attack*. The attack was traced to a 15-year-old Canadian who used the name mafiaboy; he pleaded guilty to a long list of charges. The U.S. government estimated the cost of this incident at \$1.7 billion.

Mafiaboy apparently did not write the destructive programs himself; he found them on the Net, where other 15-year-olds can find them too.

In 2001, the Code Red worm program quickly spread to 300,000 server computers at thousands of businesses worldwide.

A variant of Code Red set up a "back door" on infected computers that allowed anyone to access infected servers and copy sensitive information such as credit numbers.

THE FUTURE

Hacking by terrorists and by government-sponsored military organizations is likely to increase. The governments of the U.S., China, and other countries are using or planning such attacks.

Appliances with embedded computer chips—from microwave ovens to cars to factory machinery to heart monitors. Many such appliances are going online, that is, connecting to the Internet. While driving home from work, you can tell your stove to start cooking dinner or tell your garden sprinklers to water the lawn.

Automated fleets of cars will communicate with each other to drive safely on highways. We have already seen that some hackers think misdirecting airplane pilots is fun. The potential for havoc will increase when hackers can control devices, not just information.

HARMLESS HACKING?

When a system administrator detects an intruder, the administrator's responsibility is to protect the system and its data.

The large number of young people hacking into sensitive systems just for fun help to mask the people hacking with malicious intent. Nonmalicious, prank hacking also uses up resources that could be needed to respond to serious threats.

A group of young Danes broke into the National Weather Service computer and computers of numerous other government agencies, businesses, and universities in the U.S., Japan, Brazil, Israel, and Denmark.

If the hackers had damaged Weather Service files, for example, they could have halted air traffic that is dependent on weather reports.

Uncertainty causes harm, or expense, even if hackers have no destructive intent.

Almost all hacking is a form of trespass. Hackers with nonmalicious intentions must understand that they will often not be viewed kindly.

7.2.2 Hacktivism, or Political Hacking

Hacktivism is the use of hacking to promote a political cause.

A hacker posted anti-Israel messages on the site of a pro-Israel lobbying organization (He also posted personal information about a few hundred of the group's members, including their credit-card numbers.)

Pro-Zapatista hackers hit Mexican government sites. Someone posted a pro-drug message on a U.S. police department anti-drug Web site.

In several cases, hackers posted political messages on Web pages they hacked to direct suspicion at others or to divert attention from their true motives, including theft of credit-card numbers or other data.

To some political activists, any act that shuts down or steals from a large corporation is a political act. To the customers and owners, it is vandalism and theft.

Some writers argue that hacktivism should be considered a legitimate form of civil disobedience and not subject to felony prosecution. Civil disobedience has a respected, nonviolent tradition. Henry David Thoreau, Mahatma Gandhi, and Martin Luther King, Jr., refused to cooperate with rules that violated their freedom.

Freedom of speech does not include the right to hang a political sign in a neighbor's window or paint one's slogans on someone else's fences, even if that "someone else" is a group of people organized as a business or corporation. We have the freedom to speak, but not the right to compel others to listen.

It is common for people involved in political causes to see their side as unquestionably morally right, and anyone on the other side as morally evil, not simply someone with a different point of view.

Human rights groups like Amnesty International use the Web effectively. Groups supporting all kinds of mainstream causes, from animal rights to anarchism to odd religions, have Web sites. None of this activism requires hacktivism.

How should defacing government Web pages be treated in relatively free countries like the U.S.?

Some consider such hacking a juvenile act of minor vandalism, while others see it as a serious symbolic attack on the authority of the government.

The just approach is to treat defacing a government Web page the same as defacing a Web page belonging to any business, individual, or organization. The penalty should depend more on the seriousness of the damage than the status of the owner.

7.2.3 The Law

Congress passed the main federal computer crime law, the Computer Fraud and Abuse Act (CFAA), in 1986. There are more than a dozen other federal laws that can be used to prosecute people for crimes related to computer and telecommunications systems in specific areas.

Computers connected to the Internet are covered. Denial-of-service attacks and the launching of computer viruses and other malicious programs are covered by the law in sections addressing the altering, damaging, or destroying of information and the prevention of authorized use of a computer.

Most laws apply only if damage is above a specified amount, for example \$5000.

The USAPA expanded the definition of loss to include the cost of responding to a hacking attack, assessing damage, and restoring systems.

It increased penalties for hacking government computers used by the criminal justice system or the military. It allows the government to monitor online activity of suspected hackers without a court order.

7.2.4 Catching Hackers

Law-enforcement agents specializing in computer crime get technical training.

A police detective specializing in financial crime and hacking told me that 30% of hackers are government informers.

The sheriff has arrived on the frontier and speaks the language.

The field of collecting evidence from computer files and disks is called *computer forensics*, or sometimes *digital forensics*.

The same tools that threaten privacy aid in catching criminals. Some viruses and hacking attacks are traced by using ISP records and the logs of routers, the machines that route messages through the Internet.

The man who released the Melissa virus, for example, used someone else's AOL account, but AOL's logs contained enough information to enable law-enforcement authorities to trace the session to Smith's telephone line. Most people are unaware that word processors, such as Microsoft Word, include a lot of "invisible information" in files—in some cases, unique identifying numbers and the author's name.

Hackers learn what mistakes to avoid. Investigators of the Code Red worm, for example, said the code held no clues to its author.

Law-enforcement and security personnel continue to update their skills and tools as hackers change theirs.

The Computer Emergency Response Team (CERT), based at Carnegie Mello University, was established in 1988 in response to the Internet Worm.

(CERT itself was the victim of a denial-of-service attack in 2001, bogging down its Web site for 30 hours.) The Financial Services Information Sharing and Analysis Center was formed by large banks to provide early warning of computer attacks; it learned of the ILOVEYOU virus hours before the FBI.

THE ISSUE OF VENUE

When computer crimes cross state and international borders, what laws apply and where should the trial be held?

The man suspected of writing and releasing the ILOVEYOU computer virus in 2000, which jammed computers and destroyed files worldwide, was not prosecuted because he lived in the Philippines, which had no law that applied to his actions.

7.2.5 Penalties Appropriate to the Crime

Sentences for hacking, as for other crimes, should depend on the person's intent, the person's age, and the damage done.

ACTUAL SENTENCES

In 2000, a 16-year-old was sentenced to six months detention. He was the first juvenile to be incarcerated for hacking; he had broken into NASA and Defense Department computers and was a member of a hacker group that vandalized government Web sites.

As more young people cause more disruption, there is increasing pressure for more severe penalties.

DISCOURAGING AND PUNISHING YOUTHFUL HACKING

The actions of young hackers raise difficult ethical, social, and legal issues.

For some, the goal is adventure; some hack for thrills, respect in the hacking community, and bragging rights. But some do extensive damage by accident, or out of sheer immature irresponsibility. And some are malicious and intentionally destructive. Some steal.

Justice requires that punishments be in proportion to the specific case of the specific person being punished, not increased dramatically because of the potential of what someone else might do.

If minor hacking offenses are severely punished, we may find hackers doing worse damage because the cost to them if caught will be the same.

We want young hackers to mature, to learn the risks of their actions, and to use their skills in better ways. Most of them do grow up and go on to successful, productive careers. We do not want to turn them into resentful, hardened criminals or wreck their chances of getting a good job by putting them in jail. This does not mean that young hackers should not be punished if they trespass or cause damage.

Sometimes a hacker who is caught is given a job by the company whose computers he invaded.

Decisions about penalties must depend on the character of the particular offender.

How can we dissuade young teens from breaking into computers, launching viruses, and shutting down Web sites? We need a combination of appropriate penalties, education about ethics and risks, and parental responsibility.

7.2.6 Security

Hacking is a problem, but so is poor security.

Security of many critical business and government computer systems is weaker than it should be. Direct studies of security in government systems lead to the same conclusion, year after year. The Defense Information Systems Agency estimated that there were 500,000 hacker attacks on Defense Department networks in 1996, that 65% of them were successful, and that the Department detected fewer than 1%.

The fact that files accessed by hackers are not "classified" is not reassuring. Military officials point out that unclassified information such as payroll and personnel records can be used destructively by an enemy.

The GAO reported, in 2000, that Environmental Protection Agency (EPA) computers were "riddled with security weaknesses."

A government study in 2001 found that 155 federal computer systems had been taken over by hackers the previous year.

WHY IS SECURITY WEAK?

In its early years, the Internet was used primarily as a communications medium for researchers. Open access, ease of use, and ease of sharing information were desirable qualities. It was not designed for security against malicious intruders or teenage explorers. Many early systems did not have passwords.

Security depended primarily on trust. The World Wide Web was developed as a communications tool for physics researchers. Again, security was not a primary concern.

Security techniques and practices have improved dramatically in the past few decades, but there are still gaping holes.

Wireless networks are often insufficiently protected; A security consultant parked outside major Silicon Valley computer companies and followed internal network transmissions, including e-mail and file transfers, on his laptop.

Commenting on a worm program in 2001, a security expert said “It’s astonishingly easy to avoid,” but many system managers had not taken the appropriate steps.

In 2000, more than half the companies surveyed said lack of money prevented them from implementing necessary security.

It seems to be a common human trait not to take sufficient security precautions until after a serious problem has occurred. How many people do not back up their hard disks before they lose files? How many do not lose weight until after a heart attack?

IMPROVING SECURITY

Principles and techniques for developing safe systems exist and responsible software designers must learn to use them.

Systems can be designed security as a major goal.

Recognizing the risk of being open to the world, many network administrators installed “firewalls”—software or separate computers that monitor incoming communications (e-mail, files, requests for services, etc.) and filter out those that are from untrusted sites or fit a profile of suspicious activity.

The complexity of computer systems means that there will be unexpected flaws. We cannot expect perfection, but we should expect professionalism.

Digital signatures, biometrics, and other new tools for identification could replace or augment passwords and help reduce access by unauthorized people.

DOES HACKING IMPROVE SECURITY?

Many system operators do not close loopholes, even well-publicized ones, until there is a break-in. Chris Goggins, a well-known hacker and security consultant, said he repeatedly warned America Online of a flaw that allowed hackers to create free accounts, disconnect real subscribers, and access private files. The problems were not solved until a group of hackers exploited the flaws and caused significant problems.

Even if all hackers whose intent is to promote security and all teenagers were to quit hacking, administrators of most computer systems would still have a responsibility to ensure a high level of security.

HOW MUCH SECURITY?

If the owners of a computer system want to keep outsiders out, it is their responsibility to provide better security.

But was the 20-year-old man who released the “Anna Kournikova” virus in 2001, bogging down e-mail service around the world, correct when he claimed “after all, it’s their own fault they got infected”?

Does weak security justify intrusion? The hacker claim is analogous to saying that if someone can pick the lock on a house—or computer system—he or she has the right to enter. The fact that one can commit a crime does not justify the crime.

SECURITY THROUGH SECRECY?

Experience suggests that secrecy is not a good security tool.

Many researchers who discover security loopholes publish their findings after informing the companies responsible for the software so that they can prepare patches (corrections). Such publication encourages improvement and informs the public.

CRIMINALIZE VIRUS WRITING AND HACKER TOOLS?

Hacking scripts and computer code for thousands of computer viruses can be found on the Internet. Intentionally or recklessly making such programs available in a context that encourages their destructive use is irresponsible.

Some kinds of speech, such as inciting a riot, are not protected by the First Amendment. Would the Supreme Court consider virus codes in the same category?

7.3 Online Scams

Con artists and crooks of many sorts have found ample opportunity on the Web to cheat unsuspecting people. If an investment or bargain looks too good to be true, it probably is.

7.3.1 Auctions

Auction sites illustrate the basic benefits of the Web: convenient compilation of a large amount of information and a way for strangers all over the world to communicate and make trades.

SOLUTIONS

In the offline world, consumers know that it might be safer to buy from an established store like Macy's or Home Depot than from someone at a swap meet. Online auctions, where one interacts with invisible strangers all over the world, became, like some swap meets, places to find both bargains and rip-offs.

EBay set up a fraud unit with a staff of 100 people and a system whereby intellectual property owners can alert the company if their property is being sold illegally.

EBay requires a credit-card number from sellers.

The solutions, of course, are not perfect.

A FEW MORE ISSUES

Companies called aggregators use automated software "bots" or "crawlers" to scan large auction sites, call lists of products offered, and relist them on their own Web sites for comparison shopping. EBay blocked such software.

Does a Web site have a right to exclude certain visitors, including software visitors? How should the concept of trespass apply to Web sites?

7.3.2 Stock Fraud

Internet stock fraud, a company gave a man 250,000 shares of its stock for promoting the company in his online stock newsletter. He sold while telling his subscribers to buy. He and officials of the company received prison terms in 1997.

A former employee of an online news-release service forged an announcement with bad news about Emulex and inserted it into the service's system for distribution. Emulex stock dropped from \$110 to \$45 in an hour.

The men responsible were caught within a week.

The 23-year-old who committed the Emulex fraud was sentenced to 44 months in prison.

The SEC used to take months to investigate suspected securities fraud. In response to fraud on the Web, it formed an Office of Internet Enforcement and now responds at the speed of the Web culture.

7.4 Fraud, Embezzlement, Sabotage, Information Theft, and Forgery

7.4.1 Credit Cards, Identity Theft, Cell Phones, and More

CREDIT-CARD FRAUD

On the Web, credit-card numbers can be stolen in transmission, if secure servers are not used, and from stored files.

It is relatively easy for thieves to make purchases with stolen numbers.

Losses from most credit-card fraud in stores are absorbed by the credit-card issuers, not the merchant. Thus the merchant does not have much incentive to check the cards.

The total amount of credit card sales in the U.S. was roughly \$1,470 billion in 2000.

IDENTITY THEFT

Our identity has become a series of numbers (Social Security number, driver's license number, account numbers) and computer files (credit history, driving record). *Identity theft*, where a criminal assumes the identity of the victim and runs up large credit-card charges or cashes bad checks, is a growing problem. It might cost the victim little in direct monetary losses, but much in anguish, disruption of his or her life, and legal fees.

The motor-vehicle departments and Social Security Administration are reluctant to issue a new driver's license number or SSN to a victim, because their record systems are designed for a person to have the same number all his or her life.

TELECOMMUNICATIONS FRAUD

To counter cell-phone cloning, a technique was developed to store each phone's unique electronic "signature" along with its serial number. The system checks that they match when a call is made.

DEFENDING AGAINST FRAUD

Solutions for credit-card, ATM, and phone fraud illustrate the continual leapfrogging of increased sophistication of security techniques and increased sophistication of the techniques used by criminals. They also illustrate the use of technology itself to solve problems created by technology.

The use of stolen credit cards to make large purchases was fairly safe for thieves when credit cards were new.

Now merchants (or Web software) check card numbers immediately by connecting to credit-card company computers. The thief's window of time to use the card has shrunk to the time it takes the owner to report it stolen.

Credit-card companies use caller ID to verify that the authorization call is made from the customer's home telephone.

Software for credit-card systems detects unusual spending activity.

PayPal and other companies that provide online payment services initially lost millions of dollars to fraud. Gradually, PayPal developed some clever solutions and sophisticated security expertise. For example, to reduce fraud by people setting up phony accounts with someone else's name, Paypal makes two small deposits in the person's checking account and requires the person to report the amounts correctly.

7.4.2 Swindling and Sabotaging Employers and Competitors

With the use of computers, trusted employees have stolen hundreds of thousands, in some cases millions, of dollars from their employers.

The complexities of modern financial transactions increase the opportunities for embezzlement.

The victims of some of the most costly scams are banks, brokerage houses, insurance companies, and other large financial institutions. Employees of insurance companies can set up phony insurance policies and make claims on them.

Employees who were fired, or angry at their employer for some other reason, sometimes sabotage the company computer systems.

An employer fired from an insurance company was convicted for destroying more than 160,000 records with a logic bomb.

What is new with computer sabotage is the ease with which a great amount of damage can be done.

DEFENDING AGAINST DISHONEST EMPLOYEES

It is recommended that responsibilities of employees with access to sensitive computer systems be rotated, so suspicious activity can be noticed by someone.

An employee's password should be deleted immediately after he or she quits or is fired.

In one case, a brokerage firm turned off its audit-trail software to speed processing of orders; an employee took the opportunity to swindle the company out of an estimated \$28 million. In large, impersonal institutions, it is often foolish to trade security for convenience or increased efficiency.

ATTACKS BY COMPETITORS

Businesses keep sensitive and valuable information on computers: plans for new products, product and market research, customer lists, pricing policies, and so on. This information is an appealing target for unethical competitors.

Large quantities of digital information can be copied quickly. There might be no clues to indicate that a theft took place; nothing is missing.

American Airlines complained that an ex-employee hired by Northwest copied American's proprietary fare-setting information and sent it to Northwest. An American Airlines employee guessed a password and accessed sensitive pricing and scheduling data of a rival airline.

7.4.3 Swindling the Customer

How do you know, when your groceries are scanned at the supermarket checkout counter, that the prices charged are the same as the ones posted on the supermarket shelves? How do you know that your computer-generated credit-card bill is accurate? How do you know you are not being robbed?

It is not the computer that one should trust or not trust; it is the company that is using it.

The reputation and character of the business are more important than the computer.

Computers can make cheating harder to identify and correct.

7.4.4 Digital Forgery

THE PROBLEM

Desktop publishing systems, color printers and copiers, and image scanners enable crooks to make fakes with relative ease—fake checks, currency, passports, visas, stock and bond certificates, purchase orders, birth certificates, identification cards, and corporate stationary, to name a few examples.

About 10% of counterfeit U.S. currency was produced by desktop forgery (rather than by the old method of printing from engraved plates).

Photographs and video are used as evidence in legal proceedings (e.g. crime-scene photos and surveillance-camera video). A trusted and reliable means of authentication will be essential for the justice system.

FAKING PHOTOS

The ease which digital images can be modified raises other intriguing ethical and social issues, not related to crime.

The National Press Photographers Association has a policy that considers any alteration of a photo's editorial content to be breach of ethical standards.

The general public must become more aware of the possibility of fakery and learn to have a reasonable skepticism.

7.5 Crime Fighting Versus Privacy and Civil Liberties

7.5.1 Scanning for Scams

Periodically, fraud investigators at the Federal Trade Commission (FTC) and the Securities and Exchange Commission (SEC) surf the Web looking for potentially illegal scams.

Is there a difference between human and automated surveillance?

We saw that court decisions allowed AOL and eBay to ban spam and information-collecting software from their sites. Should they have the right to ban government surveillance software too? Should the government need a search warrant, which requires a specific reason for a search, before running its automated surveillance software on a site?

7.5.2 Biometrics

Is there a “foolproof” way to identify someone?

Biometrics are biological characteristics that are unique to an individual.

Some states use a face scanner and digital image matching to make sure a person does not apply for extra driver’s licenses or welfare benefits (with different names). Some computer systems require a thumbprint match to log on to a computer, physically or over the Net, reducing access by hackers.

It appears that the use of biometrics will increase dramatically.

If a hacker gets a copy of the file with our digitized thumbprint or retina scan, we cannot get a new one.

Given the weak security of the Web, it is likely that hackers will be able to steal files of biometrics as easily as they now steal files of credit cards. They will rig their machines to transmit a copy of the file rather than scanning their own finger or eye.

Like the face-matching applications described, increased use of biometrics can increase surveillance and tracking of our activities by government agencies. The potential for more loss of privacy is huge.

7.5.3 Search and Seizure of Computers

Seizure of a computer presents new problems for both law enforcement and suspects because of the computer’s multipurpose use.

With an appropriate warrant, it is reasonable for such material to be copied or seized and removed from the suspect’s premises. But the computer may also contain files belonging to many other people, business records, subscriber lists, and myriad other things that are not covered by the warrant.

“It’s not easy to seize part of a computer.”

7.5.4 The Cybercrime Treaty

The U.S. and European governments participated in drafting the Council of Europe’s Treaty on Cybercrime, an attempt to assist law-enforcement agencies with investigations and foster internationally cooperation in fighting copyright violations, distribution of child pornography, and other online crime.

A deputy director of Privacy International said the treaty would “turn the Internet from a great medium for free speech into a great medium for government spying.”