Computers: Tools for an Information Age

Chapter 10
Security and Privacy:
Computers and the Internet
Objectives

- Explain the different types of computer crime and the difficulties of discovery and prosecution
- Describe the aspects of securing corporate data, including software and data security, disaster recovery plans, and security legislation
- Describe in general terms how viruses work, the damage they can cause, and procedures used to prevent this damage
- Explain the threats to personal privacy posed by computers and the Internet. Describe actions you can take to maximize your privacy
Security and Privacy

- Security – data stored on computer must be kept safe
- Privacy – private data must be kept from prying eyes
Computer Crime

- **Hacker** – someone who attempts to gain access to computer systems illegally
  - Originally referred to as someone with a high degree of computer expertise
  - Social engineering – a tongue-in-cheek term for con artist actions
    - Persuade people to give away password information
- **Cracker** – someone who uses the computer to engage in illegal activity
Computer Crime

- Most commonly reported categories
  - Credit card fraud
  - Data communications fraud
  - Unauthorized access to computer files
  - Unlawful copying of copyrighted software
Methods Computer Criminals Use

- Bomb
- Data diddling
- Denial of service attacks
- Piggybacking
- Salami technique

- Scavenging
- Trapdoor
- Trojan horse
- Zapping
Bomb

- Causes a program to trigger damage under certain conditions
  - Usually set to go off at a later date
- Sometimes planted in commercial software
  - Shareware is more prone to having a bomb planted in it
Data Diddling

- Refers to changing data before or as it enters the system
- Auditors must verify accuracy of the source data as well as the processing that occurs
Denial of Service Attack

- Hackers bombard a site with more requests than it can possibly handle
  - Prevents legitimate users from accessing the site
  - Hackers can cause attacks to come from many different sites simultaneously
Piggybacking

- An illicit user “rides” into the system on the back of an authorized user
  - If the user does not exit the system properly, the intruder can continue where the original user has left off
- Always log out of any system you log into
Salami Technique

- An embezzlement technique where small “slices” of money are funneled into accounts
Scavenging

- Searching company trash cans and dumpsters for lists of information
  - Thieves will search garbage and recycling bins of individuals looking for bank account numbers, credit card numbers, etc.
- Shred documents that contain personal information
Trapdoor

- An illicit program left within a completed legitimate program
  - Allows subsequent unauthorized and unknown entry by the perpetrator to make changes to the program
Trojan Horse

- Involves illegal instructions placed in the middle of a legitimate program
  - Program does something useful, but the Trojan horse instructions do something destructive in the background
Zapping

- Refers to a variety of software designed to bypass all security systems
White-Hat Hackers

- Hackers that are paid by a company to break into that company’s computer systems
  - Expose security holes and flaws before criminals find them
  - Once exposed, flaws can be fixed
Discovery and Prosecution

- Crimes are often undetected
  - When they are detected, they are often not reported

- Prosecution is difficult
  - Law enforcement agencies and prosecutors are ill-equipped to handle computer crime
  - Judges and juries often don’t understand computer crime

- Congress passed the Computer Fraud and Abuse Act to increase awareness of computer crime
Computer Forensics

- Uncovering computer-stored information suitable for use as evidence in courts of law
  - Restores files and/or e-mail messages that someone has deleted
- Some experts are available for hire, but most are on the staffs of police departments and law firms
Security: Playing It Safe

- Security – a system of safeguards
  - Protects system and data from deliberate or accidental damage
  - Protects system and data from unauthorized access
Controlling Access

- Four means of controlling who has access to the computer
  - What you have
  - What you know
  - What you do
  - What you are
What You Have

- Requires you to have some device to gain access to the computer
  - Badge, key, or card to give you physical access to the computer room or a locked terminal
  - Debit card with a magnetic strip gives you access to your bank account at an ATM
  - Active badge broadcasts your location by sending out radio signals
What You Know

- Requires you to know something to gain access
  - Password and login name give you access to computer system
  - Cipher locks on doors require you to know the combination to get in
What You Do

- Software can verify scanned and online signatures
What You Are

- Uses biometrics – the science of measuring body characteristics
  - Uses fingerprinting, voice pattern, retinal scan, etc. to identify a person
- Can combine fingerprinting and reading a smart card to authenticate
A Disaster Recovery Plan

- A method of restoring computer processing operations and data files in the event of major destruction
- Several approaches
  - Manual services
  - Buying time at a service bureau
  - Consortium
- Plan should include priorities for restoring programs, plans for notifying employees, and procedures for handling data in a different environment
A Consortium

- A joint venture among firms to support a complete computer facility
  - Used only in the event of a disaster
  - Hot site – a fully equipped computer center
  - Cold site – an empty shell in which a company can install its own computer system
Software Security

- Who owns custom-made software?
- What prevents a programmer from taking a copy of the program?
- Answer is well established
  - If the programmer is employed by the company, the software belongs to the company
  - If the programmer is a consultant, ownership of the software should be specified in the contract
Data Security

Several techniques can be taken to prevent theft or alteration of data

- Secured waste
- Internal controls
- Auditor checks
- Applicant screening
- Passwords
- Built-in software protection
Personal Computer Security

- Physical security of hardware
  - Secure hardware in place with locks and cables
  - Avoid eating, drinking, and smoking around computers
Protecting Disk Data

- Use a surge protector to prevent electrical problems from affecting data files
- Uninterruptible power supply includes battery backup
  - Provides battery power in the event power is lost
  - Allows users to save work and close files properly
- Back up files regularly
Backing Up Files

- Back up to tape drive, CD-RW, or DVD-RAM
  - You can use software that automatically backs up at a certain type of day

- Disk mirroring
  - Makes second copy of everything you put on disk to another hard disk
Types of Backup

Three types of backup

- Full backup – copies everything from the hard drive
- Differential backup – copies all files that have been changed since the last full backup
- Incremental backup – copies only those files that have been changed since either the last full backup or the last incremental backup

Comprehensive backup plan involves periodic full backups, complemented by more frequent incremental or differential backups
Computer Pests

- Worm
- Virus
A program that transfers itself from computer to computer

- Plants itself as a separate file on the target computer’s disks
- Fairly rare
  - SQL Slammer worm disabled many Web servers in January 2003
Virus

- A set of illicit instructions that passes itself on to other files
  - Transmitting a virus
  - Can cause tremendous damage to computer and data files
  - Can be prevented
  - Common computer myths
Transmitting a Virus

- Viral instructions inserted into a game or file
  - Typically distributed via the Web or e-mail
- Users download the file onto their computers
- Every time the user opens that file, virus is loaded into memory
  - As other files are loaded into memory, they become infected
Damage from Viruses

- Some are benign, but many cause serious damage
  - Some attach themselves to operating systems, where they can affect how the computer works
  - Some delete data files or attempt to reformat your hard disk
  - Macro virus uses a program’s own programming language to distribute itself

- Organizations and individuals spend billions of dollars defending computers against viruses
Virus Prevention

- **Antivirus software**
  - Detects virus signature
  - Scans hard disk every time you boot the computer

- **Viruses tend to show up on free software or software downloaded from the Internet**
  - Use antivirus software to scan files before you load them on your computer

- **Often distributed as e-mail attachments**
  - Do not open e-mail attachments without scanning them or if you do not know the person sending the e-mail
Virus Myths

- You cannot get infected by simply being online
  - If you download and execute an infected file, you can get infected

- Although most e-mail viruses are in attachments that must be opened, it is possible to get infected by viewing an e-mail

- You cannot get infected from data
  - If graphics files include a viewer, that program could contain a virus
Privacy

- Where is my data?
- How is it used?
- Who sees it?
- Is anything private anymore?

Everything about you is in at least one computer file
Privacy: *How Did They Get My Data?*

“We’d just like a little information about you for our files…”

- Loans
- Charge accounts
- Orders via mail
- Magazine subscriptions
- Tax forms
- Applications for schools, jobs, clubs
- Insurance claim
- Hospital stay
- Sending checks
- Fund-raisers
- Advertisers
- Warranties
- Military draft registration
- Court petition
Privacy: *How Did They Get My Data?*
Protecting Your Privacy

- Data you give to organizations is often sold or rented to other organizations
  - Massive databases make it easy and inexpensive to learn almost anything about anybody
- Legislation exists to protect your privacy
Privacy Legislation

- Fair Credit Reporting Act
- Freedom of Information Act
- Federal Privacy Act
- Video Privacy Protection Act
- Computer Matching and Privacy Protection Act
- Health Insurance Portability and Accountability Act
Fair Credit Reporting Act

- Gives you access to your credit information
  - Must be provided free if you have been denied credit
- Gives you the right to challenge your credit records
Freedom of Information Act

- Allows ordinary citizens to have access to data gathered about them by federal agencies
Federal Privacy Act

- Stipulates there can be no secret personal files
- Individuals must know what is stored in files about them and how the data will be used
- Organizations must be able to justify the need to obtain information
Video Privacy Protection Act

- Prevents retailers from disclosing a person’s video rental records without a court order
Computer Matching and Privacy Protection Act

- Prevents the government from comparing certain records in an attempt to find a match.
Health Insurance Portability and Accountability Act

- Governs the security of health information records
- Requires employers, health care providers, and insurance companies to take steps to protect employees’ medical records
With so many people on the Internet, how do you keep data secure?

Several approaches

- Using a firewall
- Encryption

Privacy issues

- Being monitored
- Junk e-mail
A Firewall

A combination of hardware and software that sits between an organization’s network and the Internet

- All traffic between the two goes through the firewall
- Protects the organization from unauthorized access
- Can prevent internal users from accessing inappropriate Internet sites
Encryption

- Scrambling data so that it can only be read by a computer with the appropriate key
  - Encryption key converts the message into an unreadable form
  - Message can be decrypted only by someone with the proper key
- Private key encryption – senders and receivers share the same key
- Public key encryption – encryption software generates the key
Being Monitored

- Employers can monitor employees’ e-mail, use of the Internet, and count the number of keystrokes per minute
  - Employees are often unaware they are being monitored
- Web sites can easily collect information when a user just visits the site
  - Web sites use cookies to store your preferences
Cookies

- A small text file stored on your hard drive
- File is sent back to the server each time you visit that site
  - Stores preferences, allowing Web site to be customized
  - Stores passwords, allowing you to visit multiple pages within the site without logging in to each one
  - Tracks surfing habits, targeting you for specific types of advertisements
Spamming

Mass advertising via e-mail
- Can overflow your e-mail inbox
- Bogs down your e-mail server, increasing the cost of e-mail service

Preventing spam
Preventing Spam

- Many ways you can minimize junk e-mail
  - Be careful how you give out your e-mail address
  - Filtering software allows you to block messages or send them to designated folders
  - Don’t register at Web sites without a promise the Web site will not sell your information
  - NEVER respond to spam

- Anti-spamming legislation is being proposed in many states