Chapter Eleven

Computer Security and Risks

After Reading This Chapter, You Should Be Able To:

- Describe several types of computer crime and discuss possible crime-prevention techniques
- Describe the major security issues facing computer users, computer system administrators, and law-enforcement officials

After Reading This Chapter, You Should Be Able To:

- Describe how computer security relates to personal privacy issues
- Describe how security and computer reliability are related

Chapter Outline

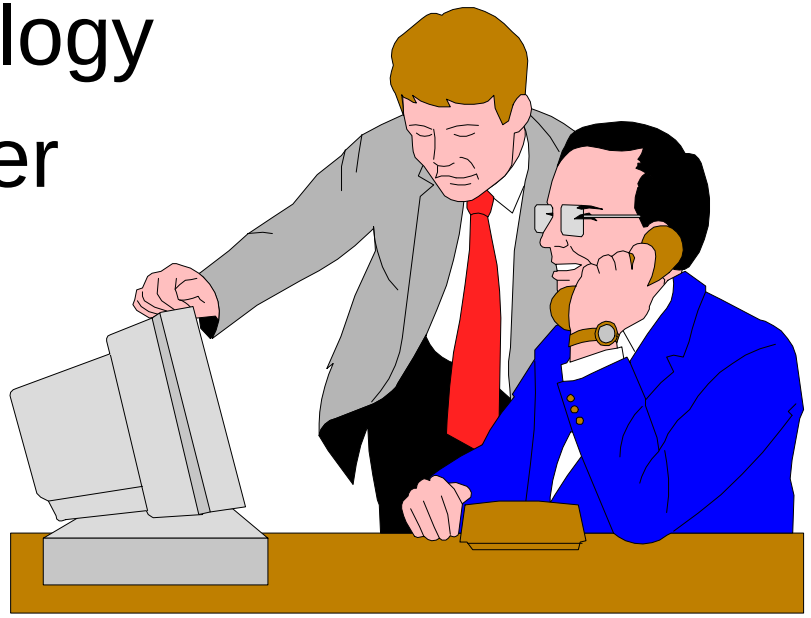
- On-line Outlaws: Computer Crime
- Computer Security: Reducing Risks
- Security, Privacy, and Freedom: The Delicate Balance
- Safe Computing
- Security and Reliability

On-line Outlaws: Computer Crime

- Computers are used to break laws as well as uphold them
- Computer crime involves:
  - Theft by computer
  - Software piracy and intellectual property laws
  - Software sabotage
  - Hacking and electronic trespassing

The Computer Crime Dossier

- Computer crime is defined as any crime accomplished through knowledge or use of computer technology
- The typical computer criminal is a trusted employee with no criminal record



The Computer Crime Dossier

- According to the FBI:
  - The average computer crime is worth $600,000
  - More than 40 percent of corporate, university, and government sites report at least one break-in per year

Theft by Computer

- Theft is the most common form of computer crime
- Computers are used to steal:
  - Money
  - Goods
  - Information
  - Computer resources

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NIC/ W721660021)

NAME: .....MITNICK, KEVIN DAVID
AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number(s): 550-39-3695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19TTCI9

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).
If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102; (24 hour telephone contact) NLETS access code is VAUSM0000.

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

Theft by Computer

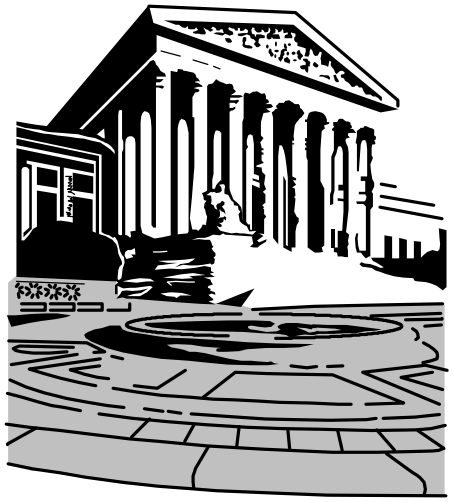
- These crimes cost businesses, law enforcement agencies, taxpayers, and consumers, who ultimately pay for the theft

Software Piracy and Intellectual Property Laws

- Software piracy is the illegal duplication of copyrighted software
- Intellectual property includes the results of intellectual activities in the arts, sciences, and industry

Software Piracy and Intellectual Property Laws

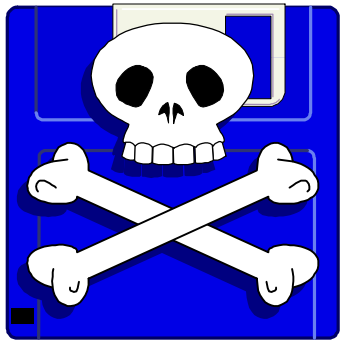
- Property laws:
  - Inventions are patented
  - Trade secrets are covered by contract law
  - The expression of intellectual property can be copyrighted



- Look-and-feel lawsuits can result from mimicking intellectual property

Software Sabotage

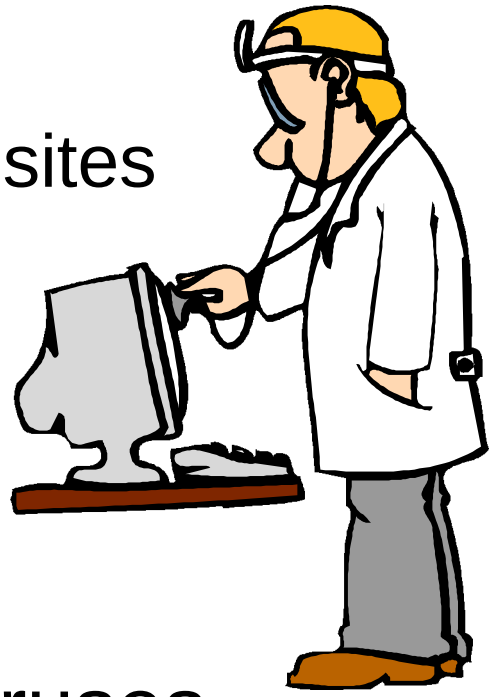
- Sabotage of software may include a Trojan horse, virus, or worm
  - Trojan horse: a program that performs a useful task while also being secretly destructive (examples: logic bombs and time bombs)



  - Virus: program that spreads by making copies of itself from program to program or disk to disk

Software Sabotage

  - Worm: a program that travels independently over computer networks, seeking uninfected sites



- Frequently, Trojan horses, viruses, and worms are all called computer viruses
- Virus detection software can find and remove most viruses

Hacking and Electronic Trespassing

- In the late 1970s, hackers were people who enjoyed learning the details of computer systems
- Today, hackers (or crackers) refers to people who break into computer systems

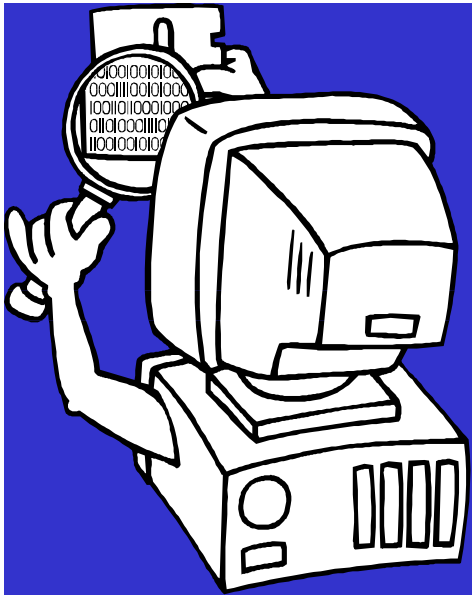
Hacking and Electronic Trespassing

- Some malicious hackers use Trojan horses, logic bombs, and other means to infiltrate computer systems

- Breaking into other computer systems is called electronic trespassing
- On-line espionage is becoming commonplace as Internet use grows

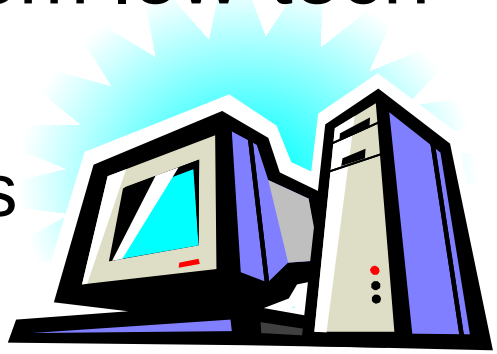
Computer Security: Reducing Risks

- Computer crime has led to a need to protect computer systems
- Computer security attempts to protect computers and the information they contain
- Computer security protects against unwanted access, damage, modification, or destruction



Computer Security

- A variety of security techniques are used to protect computer systems
- These techniques range from low-tech to high-tech and include:
  - Physical Access Restrictions
  - Passwords
  - Firewalls, Codes, Shields, and Audits
  - Backups



Physical Access Restrictions

- Physical access restrictions are based on:
  - **Something you have**, such as a key, ID card with photo, or a smart card
  - **Something you know**, such as a password, an ID number, or a piece of personal history
  - **Something you do**, such as your signature or your typing speed and error patterns

Physical Access Restrictions

– **Something about you**, such as voice print, fingerprints, retinal scans, or other measurements of individual body characteristics (biometrics)

Passwords

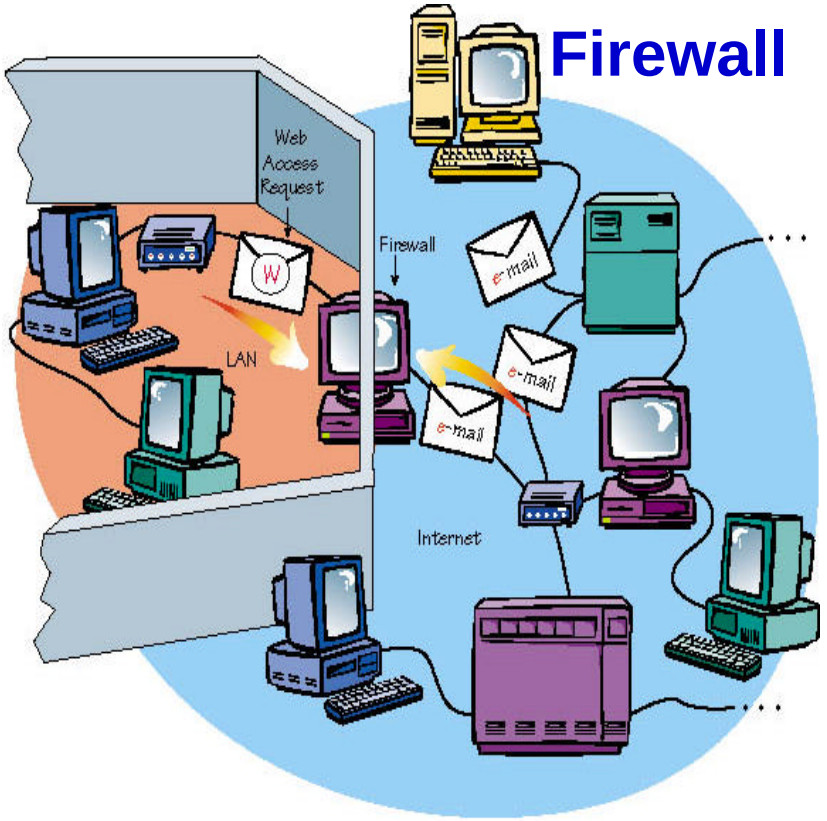
- Passwords are the most common tool for restricting access to computer systems
- Effective passwords are:
  - Not real words
  - Not names
  - Changed frequently
  - Kept secret
  - A mix of alphabet letters and numbers

Firewalls, Codes, and Shields

- These security systems reduce or prohibit the interception of messages between computers:
  - Firewalls are like gateways with a lock
  - Codes protect transmitted information and take a special key to decode
  - Shields are specially developed machines that prevent unwanted interception

Firewalls

- The computer serves as a firewall by scanning every message for security risks before allowing it of pass into or out of the LAN

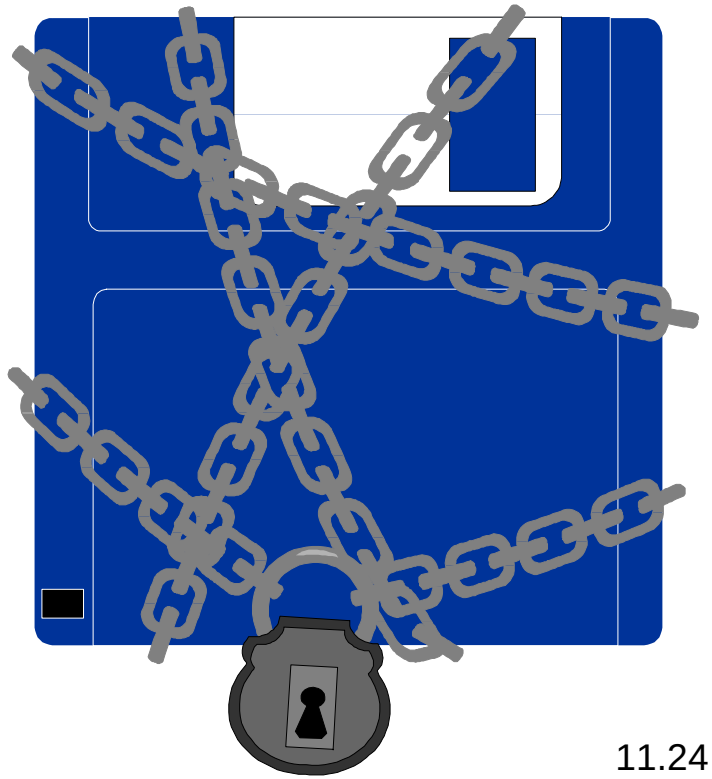


Cryptography

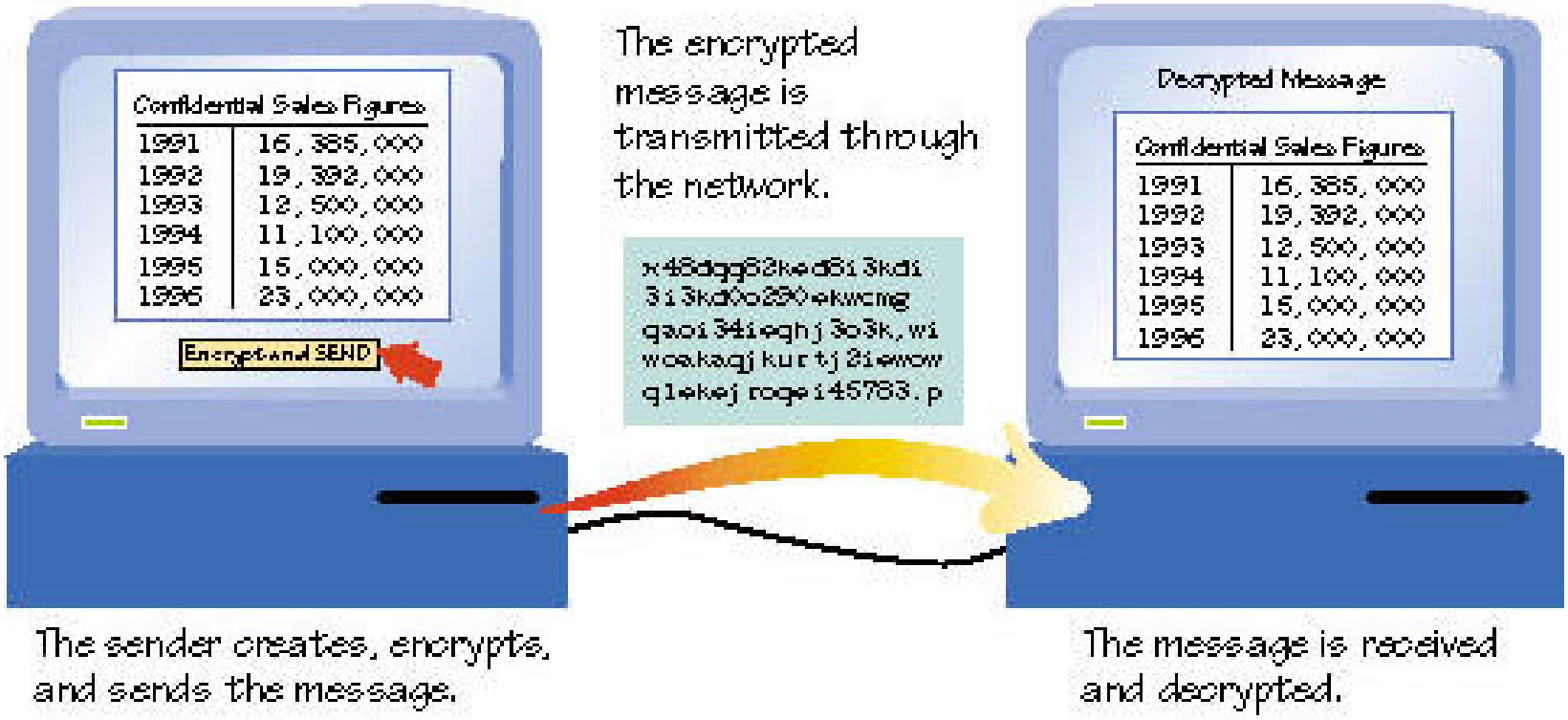
- To make a message secure from outsiders requires encryption software
- Encryption software scrambles the sent message using a key
- A different key is needed to unscramble the received message

Cryptography

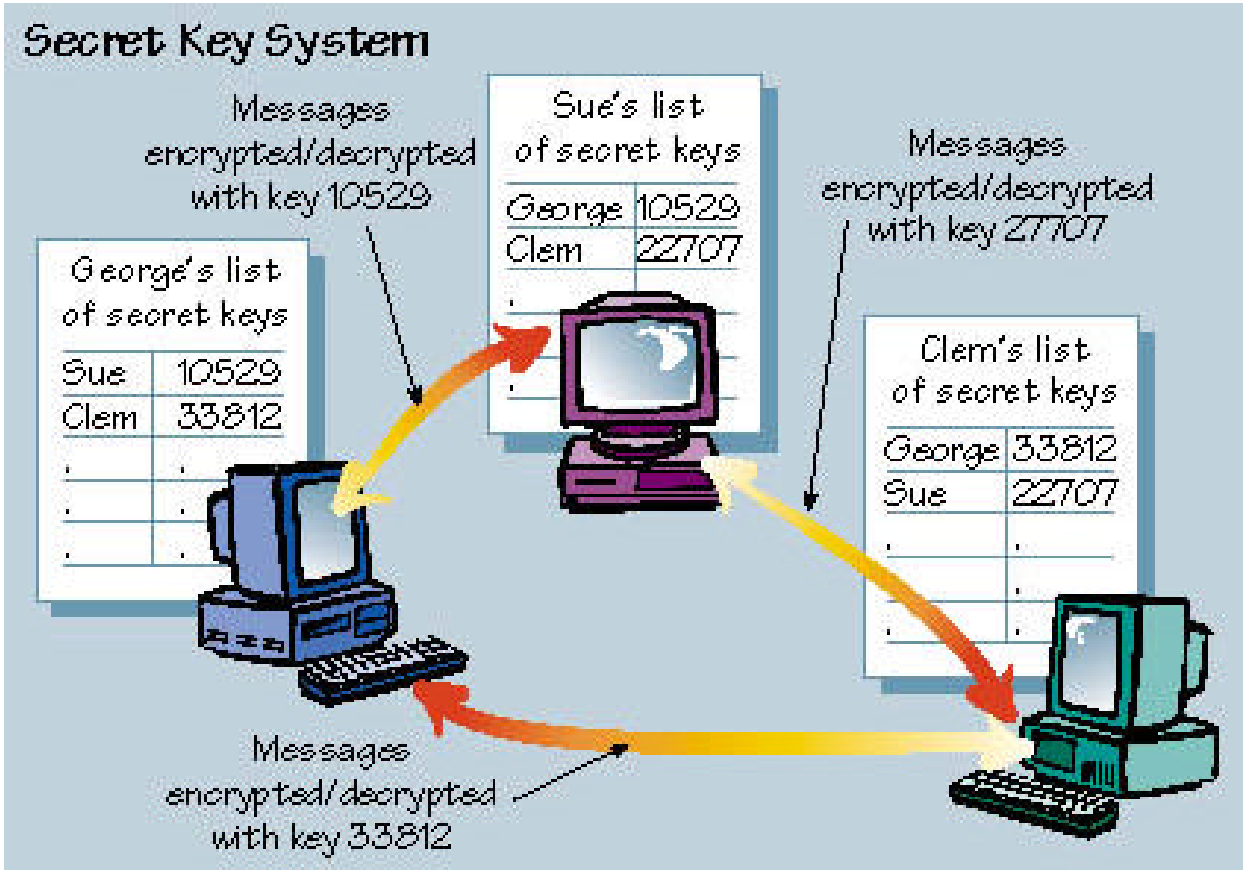
- Managing the keys is the biggest problem with some encryption schemes
- Public key cryptography gets around this problem



Encryption

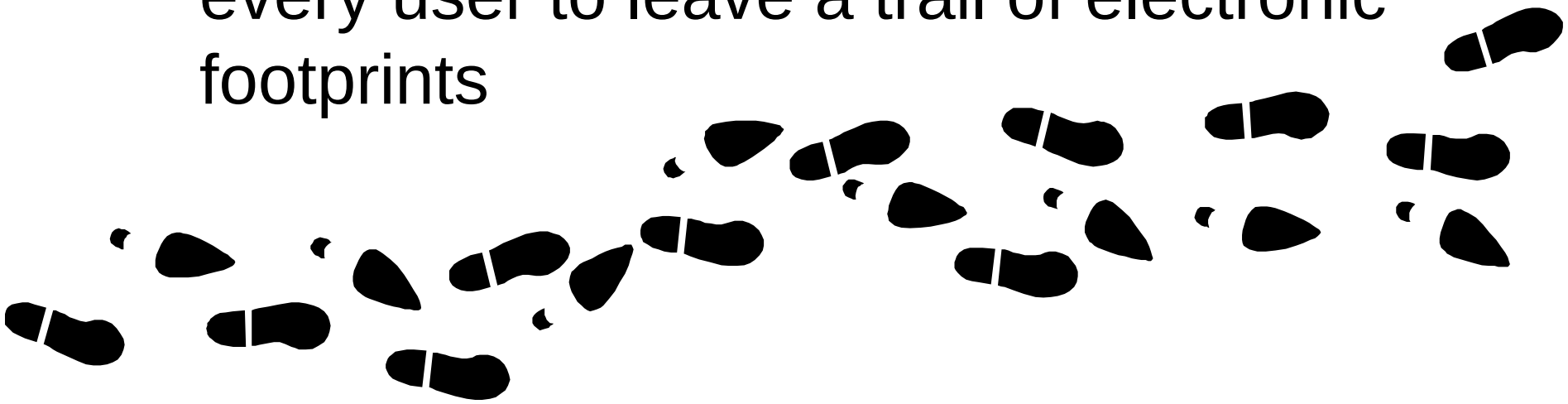


Cryptography



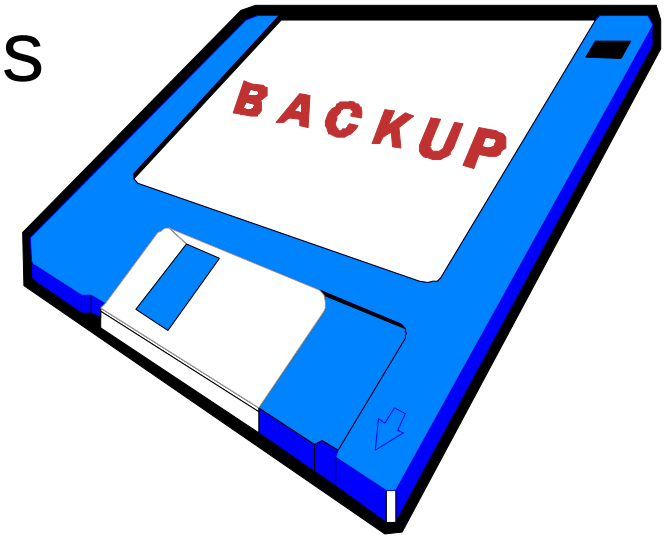
Audit-Control Software

- Audit-control software monitors and records computer activity
- Effective audit-control software forces every user to leave a trail of electronic footprints



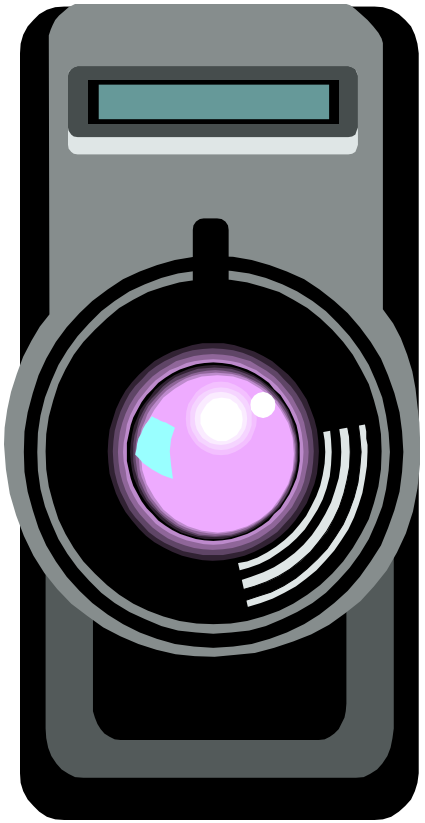
Making Backups

- The best and most widely used method to recover data is a routine for making regular backups
- Many computer systems are backed up at the end of each work day



Security, Privacy, and Freedom: The Delicate Balance

- Security measures prevent crime, but can also pose threats to personal privacy

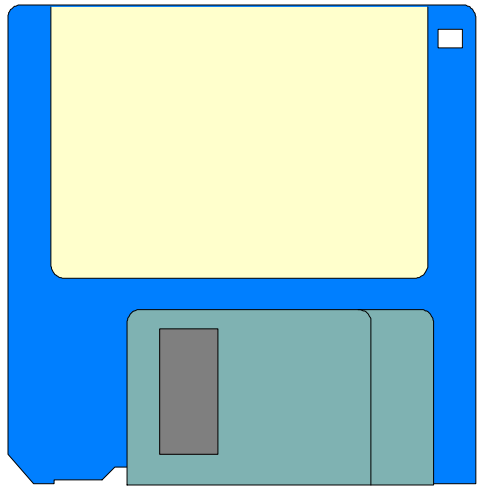


Security, Privacy, and Freedom: The Delicate Balance

- Active badges can simultaneously improve security and threaten privacy by:
  - identifying who enters a door or logs onto a machine
  - finding an employee's location or where they have been throughout the day

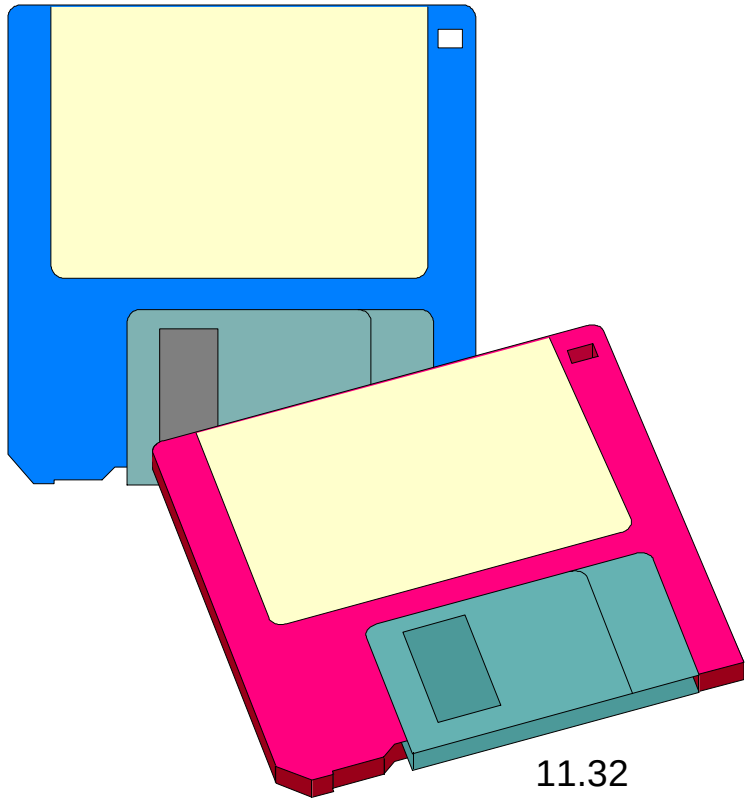
Safe Computing

- Share with care
- Beware of BBS risks
- Don’t pirate software
- Disinfect regularly
- Treat diskettes with care



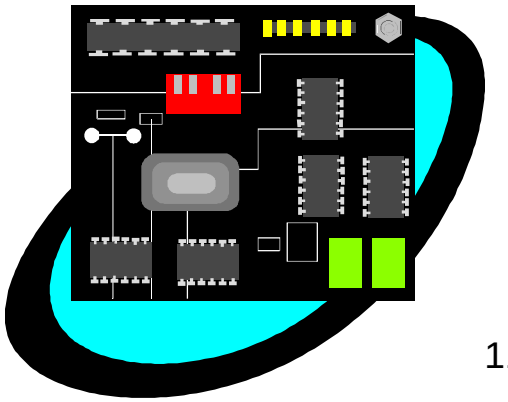
Safe Computing

- Take your password seriously
- Lock sensitive data
- Use backup systems
- Consider encryption for Internet activities
- Prepare for the worst



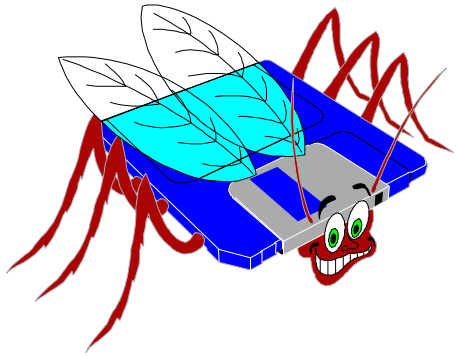
Security and Reliability

- Computer security involves more than protection from trespassing, sabotage, and other crimes
- Software errors and hardware glitches account for some of the most important security issues, such as:
  - Bugs and Breakdowns
  - Computers at War



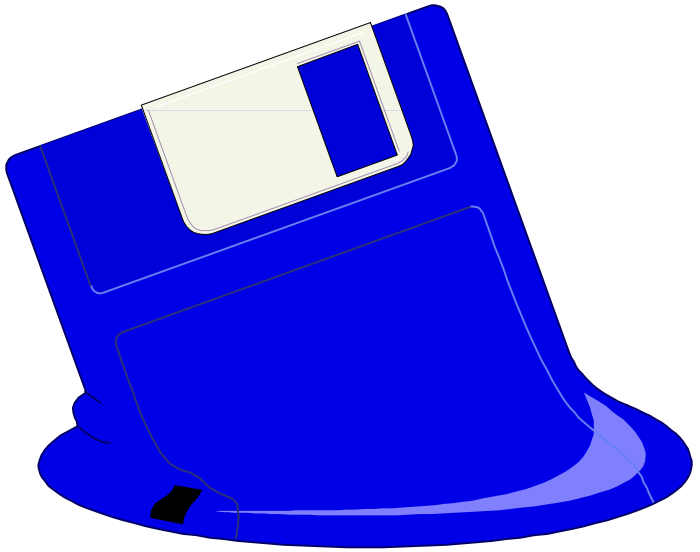
Bugs and Breakdowns

- Software bugs do more damage than viruses and computer burglars combined.
- Facts about software engineering:
  - It is impossible to eliminate all bugs.
  - Even programs that appear to work can contain dangerous bugs.
  - The bigger the system, the bigger the problem.



Bugs and Breakdowns

- Computer breakdowns pose a risk to the public and the incidence doubles every two years.
- Hardware problems are rare when compared with software failures



Computers at War

- Smart weapons are missiles that use computerized guidance systems to locate their targets.
- An autonomous system is a complex system that can assume almost complete responsibility for a task without human input.