Computer Crime and Cybercrime

- **Computer crimes**
  - Computer-based activities that violate the law

- **Cybercrimes**
  - Crimes perpetrated through the Internet
  - Many Web sites educate users about cybercrime and cybercriminals

- **Cyberlaw**
  - Area of law dedicated to computer crime
Computer Crime and Cybercrime

• Types of computer crime
  o **Identify theft**—criminal access to personal information in order to impersonate someone
  o **Dumpster diving**—disgruntled employees or thieves go through a company’s trash to find information they can steal
  o **Phishing attacks**—legitimate-looking e-mails or Web sites created in an attempt to obtain confidential data about a person
  o **Spear phishing** (similar to phishing)—uses targeted fake e-mails and social engineering to trick recipients into providing personal information to enable identity theft
Computer Crime and Cybercrime

• Types of computer crime (cont.)
  o **Malware** (short for *malicious software*)—programs that intentionally harm a computer system or allow individuals to gain access without permission

• Tips to protect yourself from malware:
  o Know who you are dealing with
  o Keep your Web browser and operating system up to date
  o Back up important files
  o Protect children online
  o Use security software tools and keep them up to date
  o Use strong passwords
  o Learn what to do if something goes wrong
Computer Crime and Cybercrime

• Types of computer crime (con’t.)
  o Spyware—software that gathers private information and tracks Web use
  • Adware—form of spyware that generates annoying pop-up and banner ads
  • Keyloggers—record keystrokes to provide cybercriminals with confidential data
Computer Crime and Cybercrime

- **Types of computer crime (con’t.)**
  - **Computer virus**—code concealed inside a program that can harm or destroy files
    - Many spread through e-mail attachments
    - **File infectors**—attach themselves to files
    - **Payload**—refers to the dangerous actions a virus performs.
    - **Macro viruses**—attach to data files and take advantage of application **macros**
    - **Boot sector viruses**—execute each time you start the computer
    - **SPIM**—spam text message sent via a cell phone or instant messaging service
Computer Crime and Cybercrime

How Viruses Work

1. The virus arrives on your system, most often through an e-mail attachment.

2. The virus is activated by opening or running the attachment and spreads to other documents on your system.

3. The virus can spread through a network connection, forwarded e-mail, or use of a portable storage device with the other computer.

4. The payload is triggered and performs its programmed activity, which can be a simple joke or the destruction of data on your system.
Computer Crime and Cybercrime

• Rogue programs
  - Logic bomb—hidden computer code that sits dormant on a system until triggered
  - Time bomb—virus program that remains dormant on a computer system until activated
  - Worm—similar to a virus but does not need action of a user to execute
Computer Crime and Cybercrime

• More rogue programs
• Denial of service (DoS) attack—assaults an Internet server with so many requests it can’t function
  o Distributed denial of service (DDoS)—attack involves multiple computer systems
    • Commandeered computers form a botnet (robot network)
  • Bot (short for robot)—connects individual computers to the controller, usually a server under the control of the botnet controller
  • The individual computers are called zombies.
Computer Crime and Cybercrime

• **More rogue programs (con’t.)**
  
  o **Syn flooding**—form of denial of service attack in which synchronization packets are repeatedly sent to every port on the server
    * Uses up all available network connections
    * Locks them until they time out
  
  o **Rootkit**—malicious program that is disguised as a useful program
    * Enables attacker to gain administrator level access
    * Allows attacker to have repeated and undetected access
  
  o **Trojan horse**—normal-looking program that includes concealed instructions to cause harm
Computer Crime and Cybercrime

- Fraud, theft, and piracy
  - Memory shaving
  - Software piracy
- Cybergaming crime
- Tricks for obtaining passwords
- Salami shaving and data diddling
- Forgery
Computer Crime and Cybercrime

• The attackers
  o **Hackers**—computer hobbyists attempting unauthorized access, generally subscribing to an unwritten code of conduct—**hacker ethic**
  o **Cybergangs**—groups of hackers working together to coordinate attacks
  o **IP spoofing**—sends a message with an IP address disguised as a message from a trusted source
  o **Honeypots**—computers baited with fake data and purposely left vulnerable to study how intruders operate to prepare stronger defenses
Computer Crime and Cybercrime

• The Attackers (con’t.)
  o **Crackers** (also called **black hats**)—attempt to enter highly secure computer systems to destroy data or steal information
  o **Ethical hackers** (also called **white hats**) use expertise to shore up computer system defenses
  o Computer virus authors—create viruses and other types of malware to vandalize computer systems
  o Swindlers perpetuate frauds:
    • Bogus work-at-home opportunities
    • Illegal pyramid schemes
    • Bogus franchises
    • Phony goods that won’t be delivered
    • Over-priced scholarship searches
Computer Crime and Cybercrime

• **Cyberstalkers**
  - Use the Internet, social networking sites, and e-mail to harass or threaten
  - Most perpetrators are men
  - Most victims are college-age women

• **Cyberbullying**
  - Sending threatening messages via e-mail or text message
  - Usually involves minors
Security

• **Computer security risk**
  - Any intentional or unintentional action resulting in damaging a computer system or its data
  - Increased by wireless LANs because transmissions occur over shared airwaves instead of dedicated lines
Security

• **Computer security risk (con’t)**
  - Wireless LAN security options include:
    - **WEP (Wired Equivalent Privacy)**
    - **WPA (WiFi Protected Access)**
    - **WPA2**
  - **Vacation hacking**—tricking travelers into using phony WiFi hot spots—**evil twins**
Security

• **Computer system security threats**
  - **Corporate espionage**—unauthorized access of corporate information, usually to the benefit of a competitor
    - **Pod slurping**—using removable storage media to create unauthorized copies of confidential data
    - **Trap doors**—security holes created by employees allowing entry to company systems after leaving the firm
  - **Information warfare**—use of information technologies to corrupt or destroy an enemy’s information and industrial infrastructure
  - **Security loophole detection programs**
  - Attacks on safety-critical systems
  - Terrorism
• Protecting your computer system
  o **Uninterruptible power supply (UPS)**—provides additional power during outages or electrical current fluctuations
  o Control access to computer systems through appropriate password selection and **know-and-have authentication**, which requires using tokens to generate a login code.
Security

• Protecting your computer system (con’t.)
  o **Biometric authentication**—use of voice recognition, retinal scans, and fingerprint scans for authentication
  o **Firewalls**, hardware or software, to prevent unauthorized access
Security

• Protect yourself—avoid scams
  o Do business with reputable companies.
  o Read documents carefully.
  o Don’t give out personal information
  o Do not post a user profile.
  o Be skeptical of chat room information.
  o Be cautious if meeting someone you’ve contacted online.
  o If you become uncomfortable or afraid, contact the police
The Encryption Debate

- **Cryptography**
  - Study of transforming information into an encoded or scrambled format

- **Cryptographers**
  - Individuals who practice cryptography

- **Encryption**
  - Coding or scrambling process that renders a message unreadable by anyone other than the intended recipient
The Encryption Debate

- **Plaintext**
  - Readable message that has not been encrypted

- **Encryption key**
  - Formula that makes a plaintext message unreadable

- **Ciphertext**
  - Coded message
The Encryption Debate

• **Symmetric key encryption**
  - Uses same key for both encryption and decryption

• **Key interception**
  - Occurs when a symmetric key encryption is stolen, allowing others to decrypt messages encrypted with that encryption key
The Encryption Debate

• **Public key encryption**
  o Also referred to as **asymmetric key encryption**
  o Uses two keys:
    • Public key to encrypt
    • Private key to decrypt
  o Essential for e-commerce
  o Used to implement:
    • **Digital signatures**—guarantee messages are secure
    • **Digital certificates**—validate identity

• **Secure electronic transaction (SET)**
  o Uses digital certificates
  o Enable parties engaged in Internet-mediated transactions to confirm each other’s identities
The Encryption Debate

Diagram showing the process of encryption and decryption with public and private keys.
The Encryption Debate

- **Public key infrastructure (PKI)**
  - Uniform set of encryption standards
  - No dominant standard
  - Public fear of a monopoly if a PKI is chosen
The Encryption Debate

• Encryption and public security issues
  o U.S. government continues search for ways to balance the public’s right to privacy and the government’s need to know