Chapter 7
Networking and Security:
Connecting Computers and Keeping Them Safe from Hackers and Viruses
Peer-to-Peer Networks

- Nodes communicate with each other
  – Peers
- Share peripheral devices
- Used in home and small office networks
- Poor Security
Client/Server Networks

- Client computers
  - Users who make requests
- Server computers
  - Provide resources to clients
  - Central network control
- Internet
  - A large, multiserver, multiclient network.
LANs and WANs

• Local area network (LAN)
  – Nodes are within a small geographic region
  – Less than a mile across
    • Homes
    • School Campus
    • Commercial Campus

• Wide area network (WAN)
  – LANs connected over long distances
    • A few miles to thousands of miles
    • Use telecommunications lines
    • Use microwave towers, satellites
MANs

• Metropolitan area network (MAN)
  – Nodes are within a specific geographic region, such as a city
  – Sponsored by a government entity to provide access to city residents and/or visitors
  – Usually Wi-Fi service
Network Components

- Transmission media
- Network communication devices
- Software
Transmission Media

• Provide communications channel between nodes

• Forms of media
  – Twisted pair
  – Coaxial cable
  – Fiber-optic cable
  – Radio waves
  – (Bluetooth)
  – Microwave (Wi-Fi)

• Bandwidth (frequencies)
  – Data transfer rate
  – Throughput
Network Adapters

• Devices connected to or installed in nodes
  – Network interface cards (NICs)--Ethernet
  – External or internal network adapters

• Enable communication between nodes
Network Navigation Devices

• Devices that help make data flow possible
• Routers
  – Route data between networks
• Switches
  – Receive data and retransmit it to nodes on the same network
Networking Software

• Peer-to-peer software
  – Built into operating systems that support networking
    • Windows
    • Mac OS

• Client/server software
  – Network operating system (NOS) software
    • Windows Server 2008
    • SUSE Linux Enterprise
Types of Peer-to-Peer Networks

- Wired Ethernet networks
- Wireless Ethernet networks
- Power-line networks
Wired Ethernet Networks

- Ethernet network adapters are used to connect nodes
  - NIC card
  - PC card
  - USB adapter
- Computers are connected to each other using unshielded twisted pair cable
Ethernet Switches

- Keep track of data packets
- Amplify and retransmit signals
- Keep the network running efficiently
Ethernet Routers

• Transfer packets from one network to another
• Home Internet routers transfer data from the Internet to the home network (Wi-Fi capable).
• Allows for network-ready devices such as network printers or NAS (network attached storage)
Wireless Ethernet Networks

- Use micro waves to connect nodes
- Basically Ethernet networks that use micro waves instead of wires
- Based on the IEEE 802.11 standard, also known as Wi-Fi (Wireless Fidelity)
- Each node requires a wireless network adapter
  - Transceivers (dongle)
  - WEP—no security
  - WPA—no security
  - WPA2—safe as of 2009
Wireless Challenges

- 802.11n standard not yet standardized
- 802.11g maximum range of 250 feet
- As distance increases, throughput decreases.
- 802.11g works on a bandwidth of 2.4 Ghz (the same as many cordless phones).
- Obstacles such as walls and metal objects cause interference.
Wireless Access Point (WAP)

- Device added to a wireless network to extend the range of the network
- Must connect to either a switch, a router, or a node on the network
Power-Line Networks

• Computers are connected to a house’s electrical wiring to create a network.

• A power-line network adapter is used to connect nodes to electrical outlets.

• Security OK
Choosing a Peer-to-Peer Network

• Things to consider
  - Whether you want wireless communications
  - How fast you want your network connection to be
  - Whether existing wiring is available
  - How much money you can spend on your network
  - How much security needed

<table>
<thead>
<tr>
<th>Comparing the Major Types of Home Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wired Ethernet</td>
</tr>
<tr>
<td>Maximum data Transfer rate (bandwidth)</td>
</tr>
<tr>
<td>Relative installation and equipment costs for networking two computers</td>
</tr>
</tbody>
</table>
Configuring Software for a Home Network

• Windows
  – Windows Vista Home versions
    • Network Setup Wizard
      – Wired or wireless
  – Windows XP
    • Network Setup Wizard
  – Windows 98
    • Configure manually
      – Help has a clear instruction
Computer Threats

- Cybercrimes are criminal acts conducted through the use of computers by cybercriminals.
Hackers

- Anyone who unlawfully accesses a computer system
- Types of hackers
  - White hat
  - Black hat
  - Script kiddies
What Hackers Do

• Steal information from computers
  – Credit card numbers
  – Bank account numbers
• Internet packet sniffing
  (eaves dropping)
• Commit identity theft
Identity Theft

• Thief steals your name, address, social security number, and/or bank account and credit card information
• Can result in credit problems and refusal of healthcare service if policy limits are exceeded
• Can be stolen using computer, theft of wallets and purses, mail, credit statements, or pretense of being a bank or credit company official
Preventing Identity Theft

1. Never reveal password or PIN.
2. Never reveal personal information without first verifying you are dealing with a legitimate representative.
   - Use a combination of letters and numbers
   - Avoid using obvious passwords
4. When shopping online, beware of unfamiliar merchants.
5. If you are a victim of identity theft, freeze credit history or place an extended fraud alert.
How Computers Are Attacked

- Trojan horse (game, screensaver)
- Backdoor program
  - Zombies
- Denial of service attacks (DoS)
- Distributed denial of service attacks (DDoS)
How Hackers Gain Access

• Direct access (physically present)
  – Install Hacking software

• Indirect access
  – Internet connection
  – Logical ports (router prevents)
Computer Safeguards: Firewalls

• Software programs or hardware designed to close logical ports to invaders
  – A firewall is built into Windows Vista.
  – More robust firewalls are available from other vendors.
  – Firewalls are critical if you have an always-on broadband connection.
Protecting a Wireless Network

• Wireless network range doesn’t stop at the property line.
• Default device and network ID settings allow intruders to enter the network.
• Internet bandwidth can be stolen.
• Computers can be vulnerable to hacker intrusion and takeover.
Computer Threats: Viruses

• A virus is a program that attaches itself to another program and spreads itself to other computers.

• Viruses are hidden within the code of a host program.
How Does a Computer Catch a Virus?

- Viruses copy themselves
- Infect a file on your computer
- Spread by sharing disks or flash drives
- E-mail attachments are the most likely source of a virus
What Viruses Do

• Replicate themselves
  – Slow down networks
• Secondary objectives
  – Display annoying messages
  – Delete files on the hard drive
  – Change computer settings
Types of Viruses

• Boot-sector viruses
  – Replicate themselves in the boot sector of the hard drive
• Logic bombs
  – Activate when certain conditions are met
• Time bombs
  – Triggered by the passage of time or on a certain date
• Worms
  – Travel between systems through networks
Types of Viruses

• Script viruses
  – Hidden on Web pages as mini programs

• Macro viruses
  – Attached to Word documents or Excel spreadsheets
  – Series of commands

• E-mail viruses
  – Use e-mail address books to distribute the virus

• Encryption viruses
  – Compress files using a complex encryption key
  – User must pay to get the files unlocked
Virus Classifications

• Polymorphic viruses
  – Periodically rewrite themselves to avoid detection

• Multipartite viruses
  – Infect multiple file types

• Stealth viruses
  – Erase their code from the hard drive and reside in the active memory
Antivirus Software

• Programs designed to detect viruses
  – Scan files looking for virus signatures (unique code)
  – Provide options for deleting or fixing infected files
  – Inoculate files against further infection

• Detects known viruses
• Needs to be updated frequently

• Norton, McAfee, Eset
• AVG—free at download.com
Other Security Measures

• Keep operating system (OS) up to date.
• Load security patches as soon as they are available.
• Enable automatic updates.
• Use the latest version of your Web browser.