Technology In Action

Chapter 7
Networking and Security:
Connecting Computers and Keeping Them Safe from Hackers and Viruses
Chapter Topics

- Networking fundamentals
- Network architecture
- Network components
- Peer-to-peer networks
- Computer threats
- Computer safeguards
- Computer viruses
Networking Fundamentals

• Computer network:
  – Two or more computers connected together
    • Each is a Node

• Benefits of a network:
  – Sharing resources
  – Transferring files
Network Architecture

• Network designs:
  – Individual PC controlled:
    • Peer-to-peer (P2P)
  – Centrally controlled:
    • Client/server
Peer-to-Peer Networks

- Nodes communicate with each other:
  - Peers
- Share peripheral devices:
  - Printers
  - Scanners
- Home and small office networks
Client/Server Networks

• Client computers:
  – Users

• 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:
    • Homes
    • Schools
    • Small businesses

• Wide area network (WAN):
  – LANs connected over long distances:
    • A few miles to thousands of miles
    • Use telecommunications lines
Network Components

- Transmission media
- Network adapters
- Navigation devices
- Network software
Transmission Media

- Provides communications channel between nodes
- Forms of media:
  - Telephone wire:
    - Twisted pair
  - Coaxial cable
  - Fiber-optic cable
  - Radio waves:
    - Wireless
- Bandwidth:
  - Data transfer rate
  - Throughput
Network Adapters

• Devices connected to or installed in nodes:
  – Network interface cards (NIC)
  – External network adapter

• 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 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 XP Professional
    – Windows Server 2003
    – Novell Netware
    – Windows Vista Enterprise
Types of Peer-to-Peer Networks

- Power-line
- Phoneline
- Ethernet
- Wireless
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.
Wireless Networks

- Use radio waves to connect nodes
- Basically an Ethernet network that uses radio waves instead of wires
- Each node requires a wireless network adapter:
  - Transceiver
Power-Line Networks

- Computers are connected to a house’s electrical wiring to create a network.
- Power-line network adapter is used to connect nodes to electrical outlets.
Phoneline Networks

- Computers are connected to a house’s telephone wiring to create a network
- Home phoneline network adapter is used to connect nodes to phone jacks
Choosing a Peer-to-Peer Network

- Things to consider:
  - Existing wiring
  - Wireless or wired
  - Speed of the network
  - Cost of the network

<table>
<thead>
<tr>
<th>Comparing the Major Types of Home Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Wired Ethernet</td>
</tr>
<tr>
<td>-------------------------------------------</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 operating system:
  - Windows Vista home versions
    - Network setup wizard
      - Wired or wireless
  - Windows XP:
    - Network setup wizard
  - Windows ME:
    - Network setup wizard
  - Windows 98:
    - Configure manually
      - Help has a clear instructions
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
• Commit identity theft
Denial of Service Attacks

- Backdoor programs
  - Trojan horse
  - Zombies
- Denial of service attacks
How Hackers Gain Access

- **Direct access:**
  - Hacking software
- **Indirect access:**
  - Internet connection
  - Logical ports
Computer Safeguards

Firewalls

- Software programs or hardware designed to close logical ports to invaders
  - A firewall is built into Windows XP
  - 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 Threat - Viruses

• 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
- Viruses spread by sharing disks
- E-mail attachments are the most likely source of a virus
What Viruses Do

• Replicate themselves:
  – Slow down networks

• Secondary objectives:
  – 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

• **Worms:**
  – Travel between systems through networks
Types of Viruses

• **Script viruses:**
  – Hidden on Web pages
  – Mini programs

• **Macro viruses:**
  – Attached to documents
  – Series of commands

• **Encryption viruses**
  – Search for common data files
  – Compress files using a complex encryption key
  – User must pay to get the files unlocked

• **Trojan horses:**
  – Backdoor programs
  – Control remote computers
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)
  – Provides options for deleting or fixing infected files
  – Inoculates files against further infection

• Detect known viruses

• Antivirus programs need to be updated frequently