CWSP Guide to Wireless Security

Active Wireless Attacks

Objectives

- Describe the basic vulnerabilities of a WLAN
- Tell how malware and spyware can infect wireless networks
- List the vulnerabilities involved with implementing unsecured wireless LANs
- Explain the different types of wireless infrastructure attacks

Security Vulnerabilities

Clip: http://computer.howstuffworks.com/internet/basics/internet-infrastructure.htm

- Security vulnerability
  - Weakness or flaw in an information system
  - Could be exploited to cause harm
  - Describes the points of risk regarding the penetration of a security defense
- Categories
  - Basic vulnerabilities
  - Vulnerabilities when using a public-access WLAN
  - Vulnerabilities associated with implementing an unsecured wireless network

Basic Vulnerabilities

- Default passwords
  - Authentication
    - Users must prove that they are who they claim to be
      - Based on what they have, know, or are
  - Password
    - Secret combination of letters and numbers
    - Validates or authenticates a user by what she knows
    - Used with user names to log on to a computer
  - APs are protected by manufacturers with default passwords

Basic Vulnerabilities (continued)



Figure 4-1 AP username and password

Basic Vulnerabilities (continued)

- Weak passwords
  - Password paradox
    - Passwords should never be written down, but instead must be committed to memory
    - Passwords must be of a sufficient length and complexity
      - Difficult to memorize these types of passwords
  - Most users today have an average of 20 passwords
    - Impossible to remember all of them

Basic Vulnerabilities (continued)

- Weak passwords (continued)
  - Characteristics of weak passwords
    - A common word used as a password
    - Not changing passwords unless forced to do so
    - Passwords that are short
    - Personal information in a password
    - Using the same password for all accounts
    - Writing the password down
  - Password guessing attacks
    - Brute force
    - Dictionary

Basic Vulnerabilities (continued)

- Weak passwords (continued)
  - Minimum criteria for creating good passwords
    - Password must be at least eight characters long
    - Password contains characters from at least three of the following five categories:
      - English uppercase characters (A–Z)
      - English lowercase characters (a–z)
      - Base 10 digits (0–9)
      - Non-alphanumeric (For example: !, $, #, or %)
      - Extended ASCII characters
    - Password does not contain three or more characters from the user's account name

Basic Vulnerabilities (continued)

- Weak passwords (continued)
  - Additional settings
    - Enforce password history
    - Maximum password age
    - Minimum password age
    - Minimum password length

Basic Vulnerabilities (continued)

Table 4-1 Password settings for wireless equipment

Password Category	Recommended Setting
Password length	Minimum 8 characters, recommended length 10 characters
Password content	Contains characters from three of the following categories: uppercase, lowercase, digit, non-alphanumeric, extended ASCII
Password history	Must create 12 new passwords before old password can be reused
Maximum password age	Change password every 30 days
Minimum password age	Must keep password at least 7 days

Basic Vulnerabilities (continued)

- SNMP community strings
  - SNMP agents are protected with a password known as a *community string*
  - Types of community strings
    - Read-only string allows information from the agent to be viewed
    - Read-write string allows settings to be changed
  - Default SNMP community strings for read-only and read-write were *public* and *private*
  - Community strings are transmitted in cleartext

Basic Vulnerabilities (continued)

- Improper configuration
  - Can often result in easy access to a system
  - Universal Plug and Play (UPnP)
    - Allows devices on a network to discover other devices and determine how to work with them
    - Vulnerabilities
      - Can enable an attacker to gain complete control over an affected device
      - Can enable an attacker to prevent an affected system from performing its intended service

Basic Vulnerabilities (continued)

Table 4-2 Windows UPnP support

Windows Version	UPnP Support
Windows XP Professional and Home	Native UPnP capability; installed and running by default.
Windows Server 2003	No UPnP support.
Windows ME	Native UPnP capability but is not installed or used by default.
Windows NT 4.0 and Windows 2000	No UPnP support.
Windows 98 and 98SE	No native support; can only be added by installing the client software for Internet Connection Sharing (ICS) provided in Windows XP.

Basic Vulnerabilities (continued)

- Improper configuration (continued)
  - Remote access
    - Allows for the wireless gateway to be configured remotely over the Internet
    - Allows an attacker to attempt to break into the wireless gateway or access point
      - Wireless gateway will permit an unlimited number of attempts to break the password

Basic Vulnerabilities (continued)

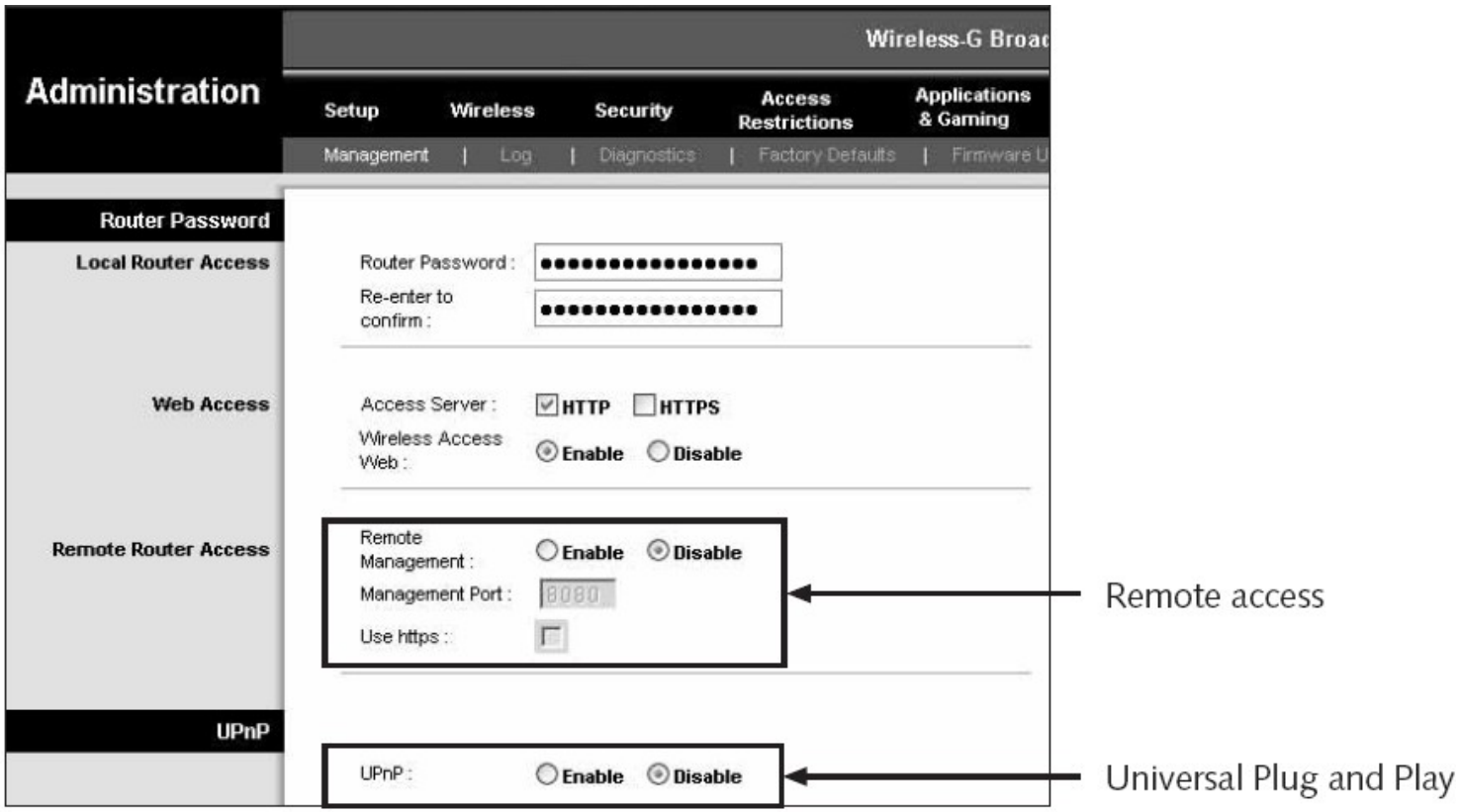

Figure 4-2 UPnP and remote access

Vulnerabilities Associated with Using Public WLANs

- Malware
  - Computer programs designed to break into and create havoc on portable or desktop computers
  - Most common types of malware are viruses, worms, and logic bombs
- Virus
  - Program that secretly attaches itself to another document or program
    - Executes when that document or program is opened
  - One new virus is written and released every hour

Vulnerabilities Associated with Using Public WLANs (continued)

- Virus (continued)
  - Actions performed by viruses
    - Cause a computer to repeatedly crash
    - Erase files from a hard drive
    - Install hidden programs, such as stolen (“pirated”) software, which is then secretly distributed or even sold from the computer
    - Make multiple copies of itself and consume all of the free space in a hard drive
    - Reduce security settings and allow intruders to remotely access the computer
    - Reformat the hard disk drive

Vulnerabilities Associated with Using Public WLANs (continued)

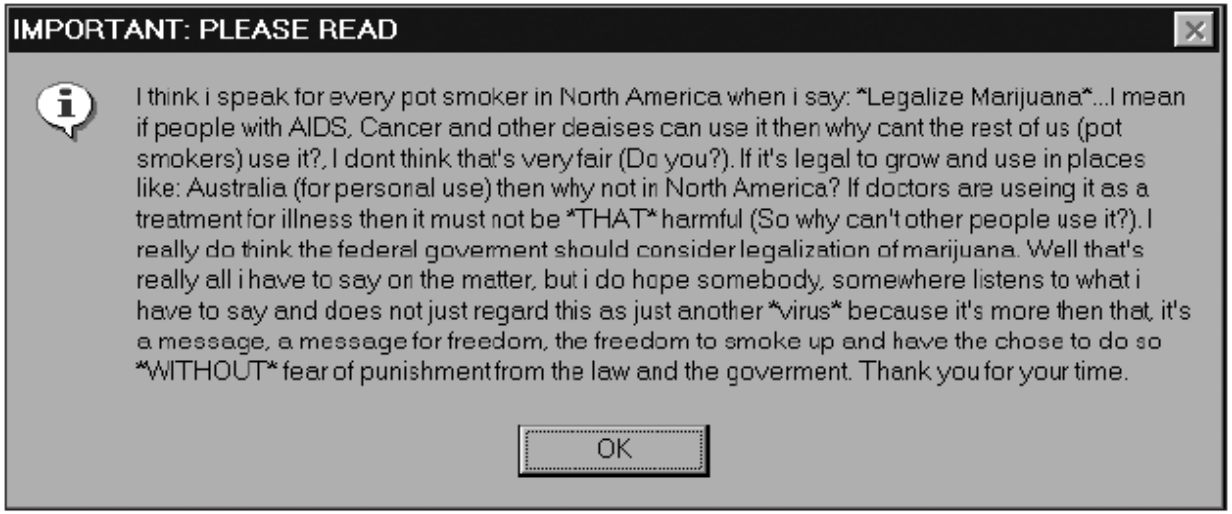

Figure 4-3 Annoying virus message

Vulnerabilities Associated with Using Public WLANs (continued)

- Virus (continued)
  - Symptoms
    - A program suddenly disappears from the computer
    - New icons appear on the screen
    - New programs do not install properly
    - Out-of-memory error messages appear
    - Programs stop responding
    - The computer sometimes starts normally, but at other times it stops responding before it finishes loading
    - Unusual dialog boxes or message boxes appear
    - Sounds or music play from the speakers unexpectedly

Vulnerabilities Associated with Using Public WLANs (continued)

- Virus (continued)
  - Symptoms (continued)
    - Computer runs very slowly and takes a long time to start
    - There is a significant amount of modem activity
    - The computer restarts unexpectedly
    - Error messages appear listing “critical system files” that are missing, and the operating system refuses to load
- Worms
  - Can travel by themselves
  - Do not always require action by the computer user to begin their execution

Vulnerabilities Associated with Using Public WLANs (continued)

- Logic bomb
  - Lies dormant until triggered by a specific logical event
  - Once triggered, the program can perform various malicious activities
  - Extremely difficult to detect before they are triggered
  - Often embedded in large computer programs
- Spyware
  - Software that violates a user's personal security
  - Impairs control over the use of system resources

Vulnerabilities Associated with Using Public WLANs (continued)

- Spyware (continued)
  - Functions performed
    - Advertising
    - Collecting personal information
    - Changing computer configurations
  - Tool attackers employ spyware to gather personal information about users
  - Identity theft
    - Occurs when an individual uses the personal information of someone else

Vulnerabilities Associated with Using Public WLANs (continued)

- Spyware (continued)
  - Adware delivers advertising content
    - In a manner or context that is unexpected and unwanted by the user

Vulnerabilities Associated with Implemented Unsecured WLANs

- Information theft
  - Attacker can gain access to any folder set with file sharing enabled
    - This would include sensitive documents on a file server
- Repository for illegal content
  - Attacker can set up storage space on a file server
    - Or a home computer
  - Attacker can also set up a Web site
- Spam site
  - Spam: unsolicited e-mail

Vulnerabilities Associated with Implemented Unsecured WLANs (continued)

- Spam site (continued)
  - Approximately 50% of e-mail messages are spam
  - Spam also reduces work productivity
  - Spammers often build their own lists of e-mail addresses
    - Using special software that rapidly generates millions of random e-mail addresses from well-known ISPs
  - Spammers often swap or buy lists of valid e-mail addresses from other spammers
  - Spam is a lucrative business
  - Spam may also be dangerous

Vulnerabilities Associated with Implemented Unsecured WLANs (continued)

Table 4-3 CAN-SPAM law

Provisions of Bill	Description
Who is affected	• Spammers and those who procure their services • Organizations or individuals who know (or should know) that the promotion of their services or goods is prohibited
What is legal	• E-mail that contains a transaction or relationship message, such as order processing or product update information • Unsolicited commercial e-mail that contains accurate contact information for the sender
What is illegal	• Fraudulent or deceptive subject lines, headers, or e-mail addresses • Sending e-mail to addresses that have been harvested from Web sites or randomly generated • Sending sexually oriented e-mail without an identifying subject line • Not maintaining a functioning unsubscribe system for at least 30 days from the mailing • Registering for e-mail addresses under a false identity • Not removing an e-mail address in a timely fashion after receiving a request from a recipient

Vulnerabilities Associated with Implemented Unsecured WLANs (continued)

Table 4-3 CAN-SPAM law

Provisions of Bill	Description
Who may bring litigation	• Federal Trade Commission (FTC) • State Attorneys General • Internet service providers (Individual e-mail recipients are not eligible to bring litigation)
What are the penalties	• State Attorneys General may sue for $250 per spam message, up to $2 million • Internet service providers may sue for $100 per spam message, up to $1 million • Three to five years imprisonment

Wireless Infrastructure Attacks

- Attacks include:
  - Direct attacks
  - Denial-of-service attacks

Direct Attacks Through Rogue Access Points

- Rogue access point
  - AP installed by an employee
    - Without the approval or supervision of the IT staff
  - Can provide open access to an attacker
    - Circumventing the security protections of the company's network
  - A rogue access point is behind the firewall
- Peer-to-peer attack
  - Attacker's wireless device attacks a similar device

Direct Attacks Through Rogue Access Points (continued)

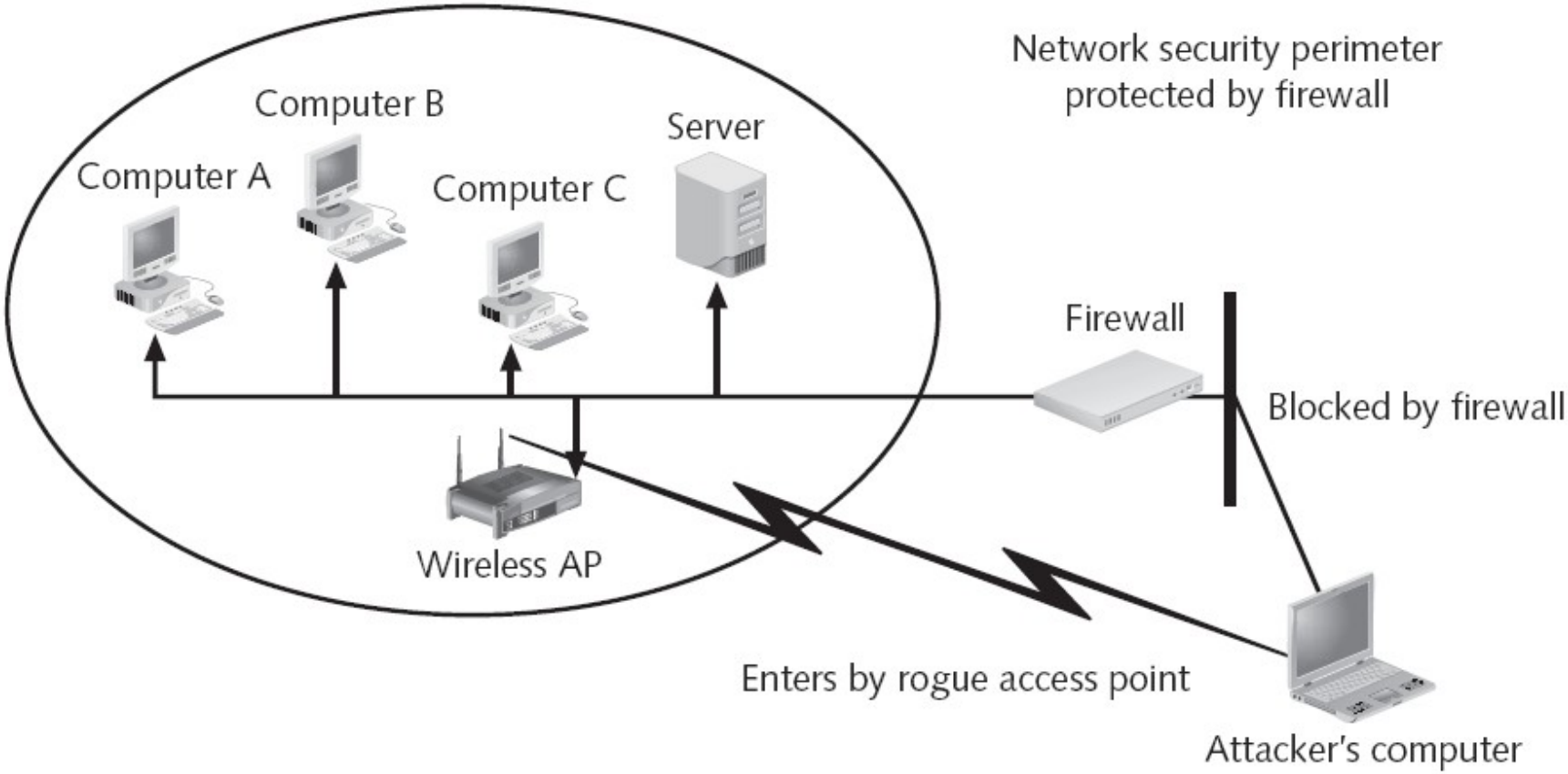

Figure 4-4 Rogue access point

Denial-of-Service Attack (DoS)

- Designed to prevent a device from performing its intended function
- DoS attacks are common against wired network servers
- SYN flood attack
  - Client sends server a request called a SYN
  - Server responds to the client with an ACK
    - And waits for a reply
  - Attacker never replies
    - Server runs out of resources and can no longer function

Denial-of-Service Attack (DoS) (continued)

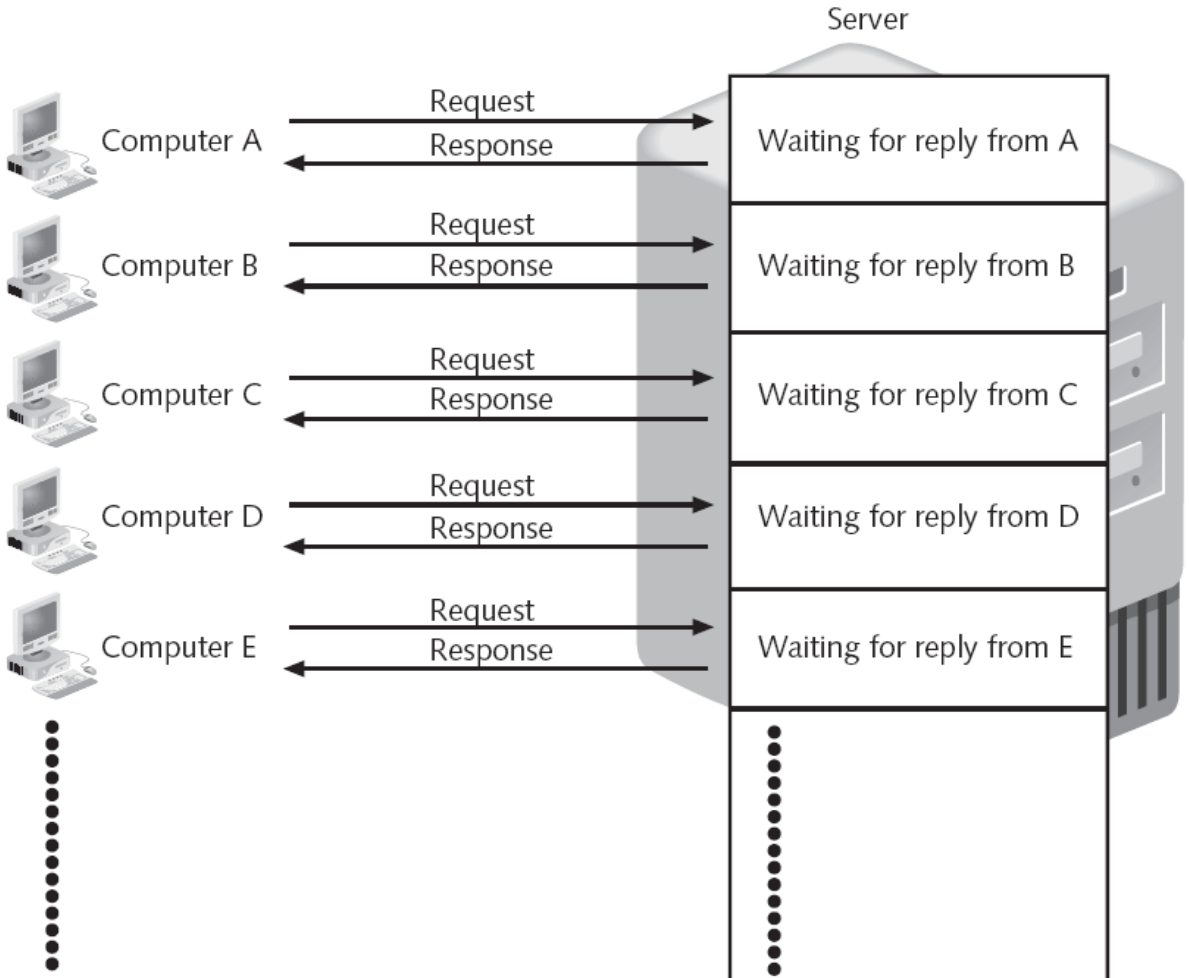

Figure 4-5 Server waiting for response

Denial-of-Service Attack (DoS) (continued)

- Wireless DoS attacks
  - Deny wireless devices access to the access point
  - Categories
    - Physical layer attacks
    - MAC layer attacks
- Physical layer attacks
  - Flood the spectrum with radiomagnetic interference
    - To prevent a device from communicating with the AP

Denial-of-Service Attack (DoS) (continued)

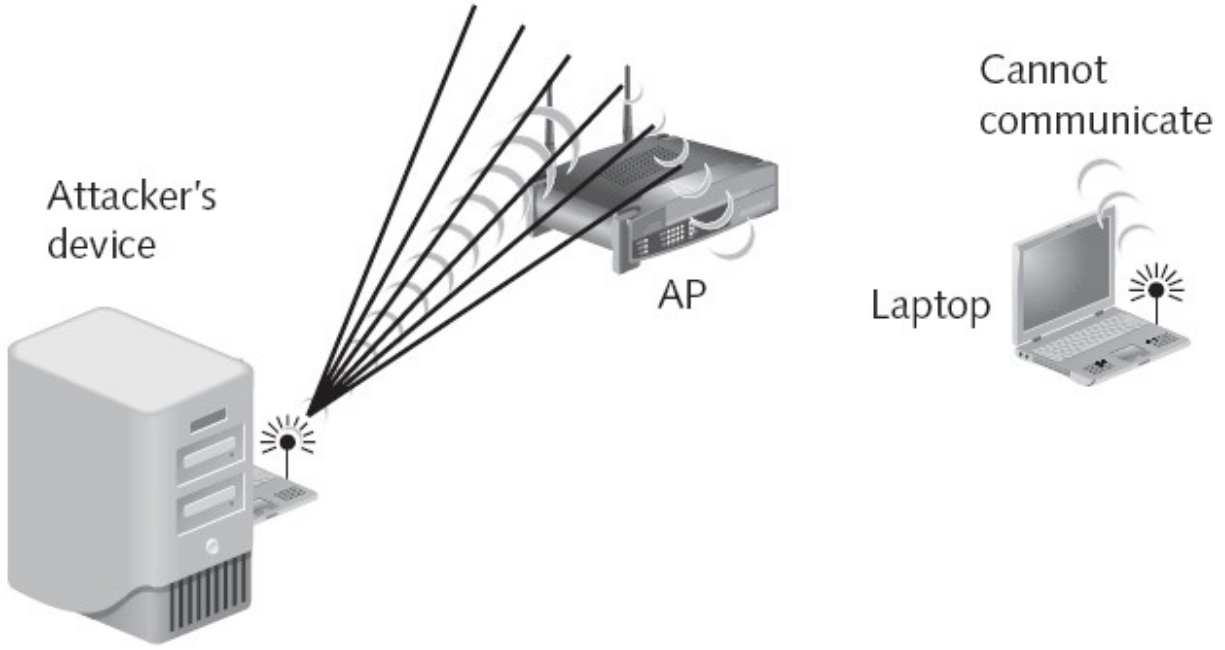

Figure 4-6 Physical layer attack

Denial-of-Service Attack (DoS) (continued)

- Physical layer attacks (continued)
  - Generally rare because sophisticated and expensive equipment is necessary
  - It is possible to identify the location of the transmitter
  - Other devices that use the ISM band
    - Cordless telephones
    - Microwave ovens
    - Baby monitors
    - Bluetooth personal area network devices

Denial-of-Service Attack (DoS) (continued)

- MAC layer attacks
  - Wireless medium is shared among all devices
  - Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
    - Attempts to prevent multiple wireless devices from transmitting at the same time
    - Uses slot times and explicit frame acknowledgement
  - Slot time
    - Time that a device must wait after the medium is clear
  - Frame acknowledgement
    - ACK frame is sent back to sending device

Denial-of-Service Attack (DoS) (continued)

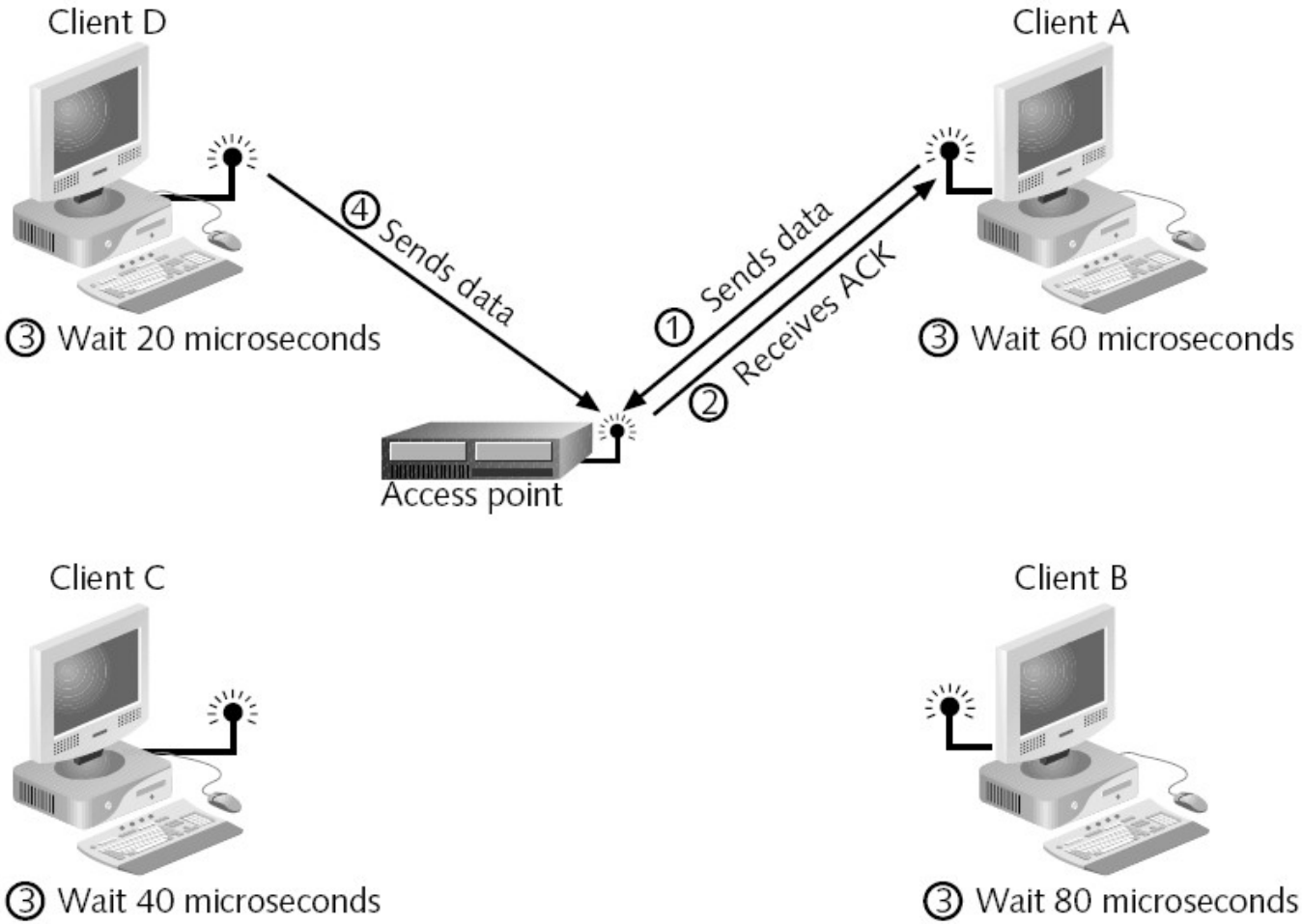

Figure 4-7 CSMA/CA and ACK

Denial-of-Service Attack (DoS) (continued)

- MAC layer attacks (continued)
  - Attacker who has already become associated with the WLAN can download an extremely large file
    - This will effectively “tie up” the network
  - Packet generator
    - Creates fake packets and floods the wireless network
  - Attacker sends disassociation frames to wireless devices
    - Device will disassociate from the access point

Denial-of-Service Attack (DoS) (continued)

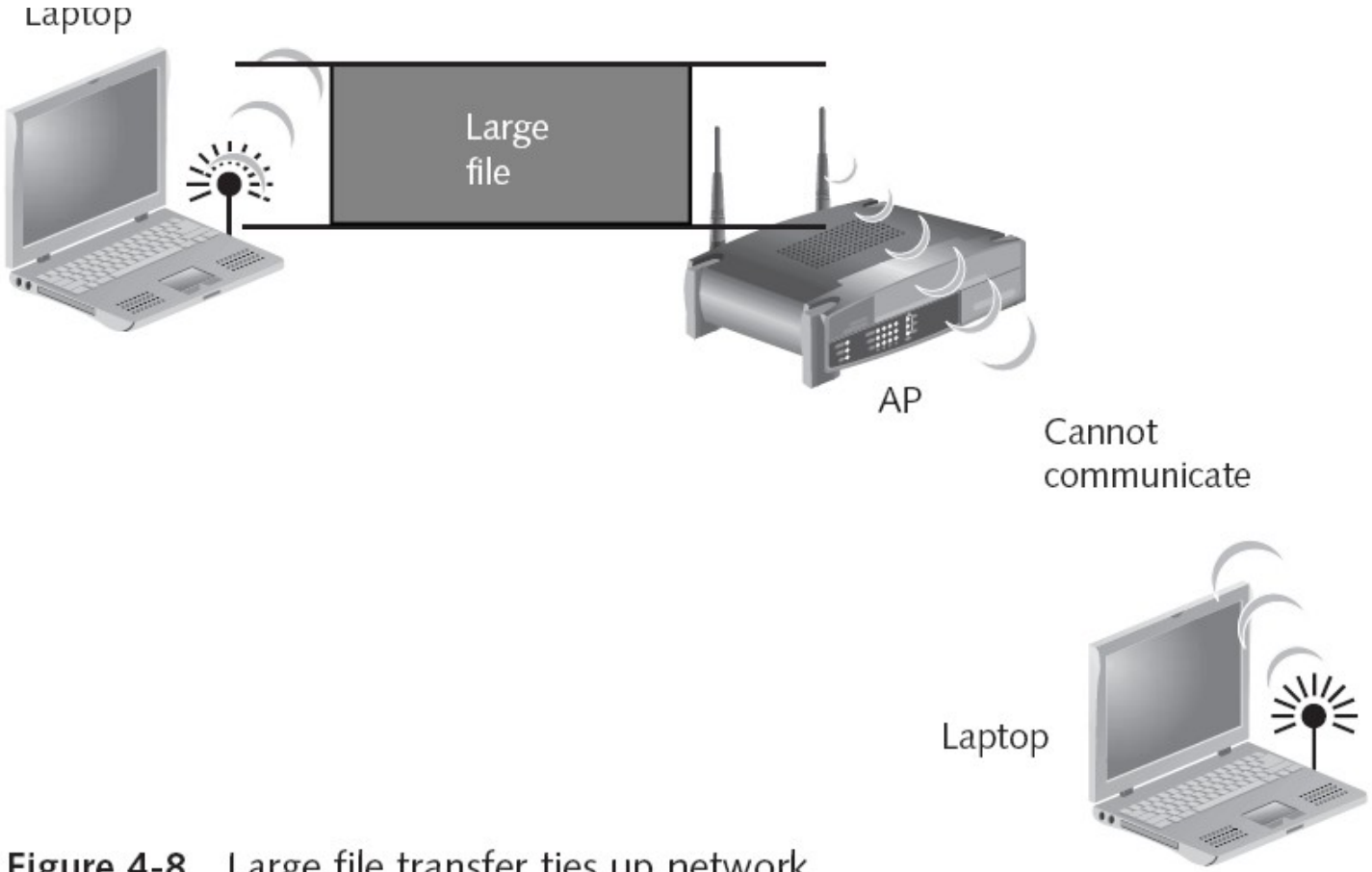

Figure 4-8 Large file transfer ties up network

Denial-of-Service Attack (DoS) (continued)

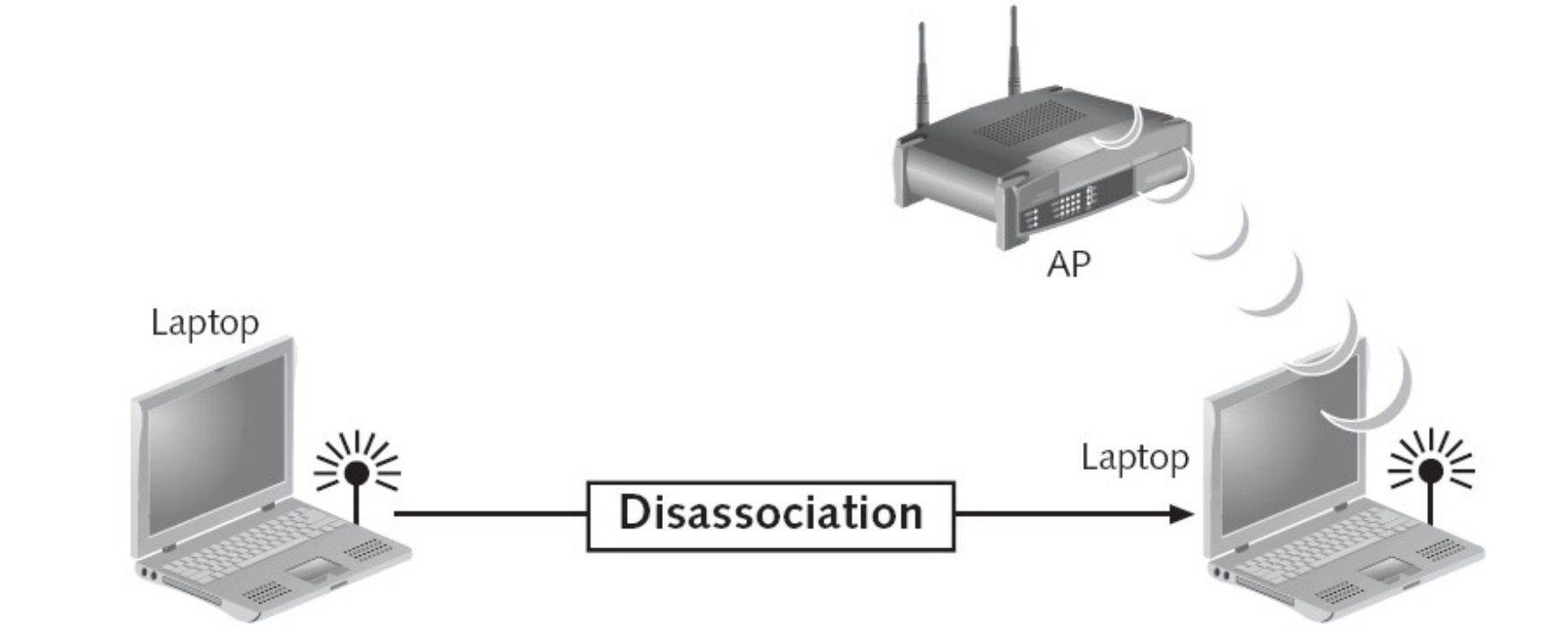

Figure 4-9 DoS using disassociation frames

Summary

- Security vulnerabilities for wireless LANs categories
  - Basic vulnerabilities
  - Vulnerabilities associated with using public WLANs
  - Vulnerabilities associated with implementing unsecured WLANS
- Basic vulnerabilities include:
  - Default passwords, weak passwords, SNMP community strings, and improper configuration
- Vulnerabilities when using a public-access WLAN include malware and spyware

Summary (continued)

- Vulnerabilities associated with implementing an unsecured WLAN
  - Information theft
  - Storing illegal content
  - Spam
- Direct attacks on the wireless infrastructure can be implemented through rogue access points
- Wireless DoS attacks can be physical layer attacks or MAC layer attacks