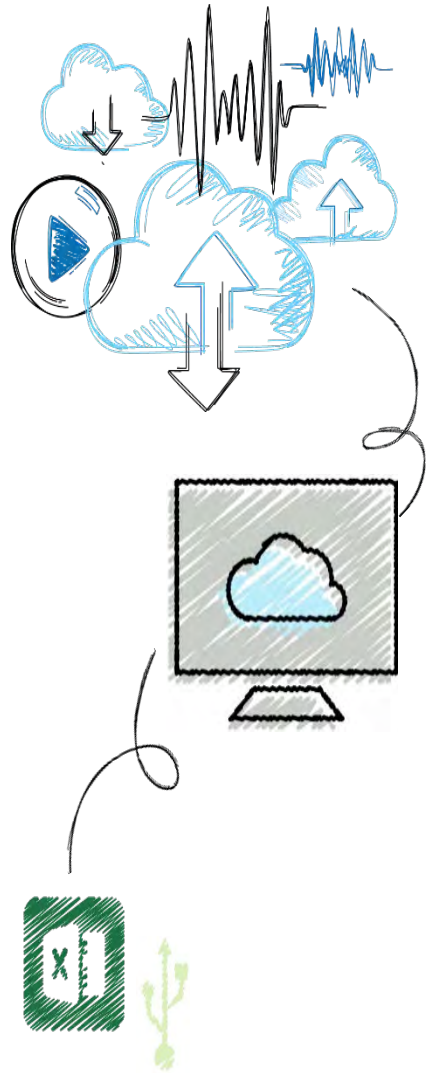


# CompTIA Security+

## Module 8

### Wireless Network Security





## Objectives

- 8.1** Describe the different types of wireless network attacks
- 8.2** List the vulnerabilities in IEEE 802.11 security
- 8.3** Explain the solutions for securing a wireless network



# Wireless Attacks

- Several attacks can be directed against wireless data system:
  - Bluetooth attacks
  - Near Field Communication (NFC) attacks
  - Radio frequency identification systems
  - Wireless local area network attacks

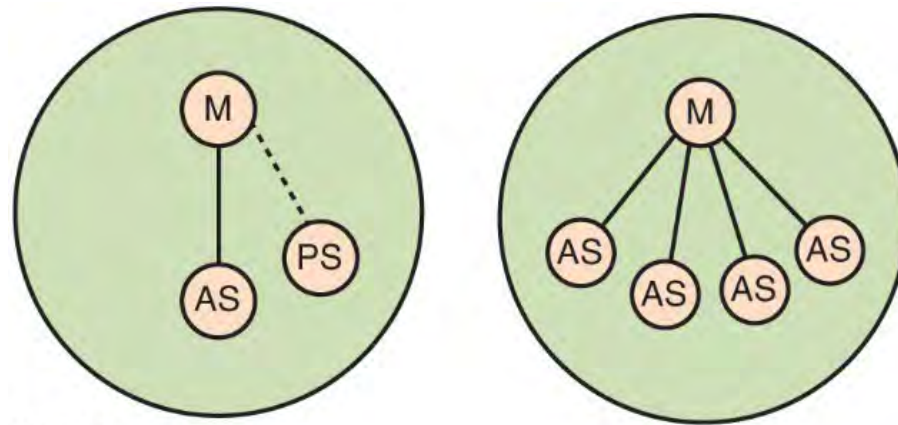


# Bluetooth Attacks (1 of 3)

- Bluetooth
  - Wireless technology that uses short-range radio frequency (RF) transmissions
  - Provides rapid device pairings
    - Example: smartphone and a Bluetooth mouse
  - Personal Area Network (PAN) technology
- Piconet
  - Established when two Bluetooth devices come within range of each other
  - One device (master) controls all wireless traffic
  - Other device (slave) takes commands
    - Active slaves are sending transmissions
    - Parked slaves are connected but not actively participating



## Bluetooth Attacks (2 of 3)



M = Master  
AS = Active slave  
PS = Parked slave

**Figure 8-1** Bluetooth piconet



## Bluetooth Attacks (3 of 3)

- Bluejacking - an attack that sends unsolicited messages to Bluetooth-enabled devices
  - Text messages, images, or sounds
- Bluejacking is considered more annoying than harmful
  - No data is stolen
- Bluesnarfing
  - An attack that accesses unauthorized information from a wireless device through a Bluetooth connection
  - Often between cell phones and laptops
  - Attacker copies e-mails, contacts, or other data by connecting to the Bluetooth device without owner's knowledge

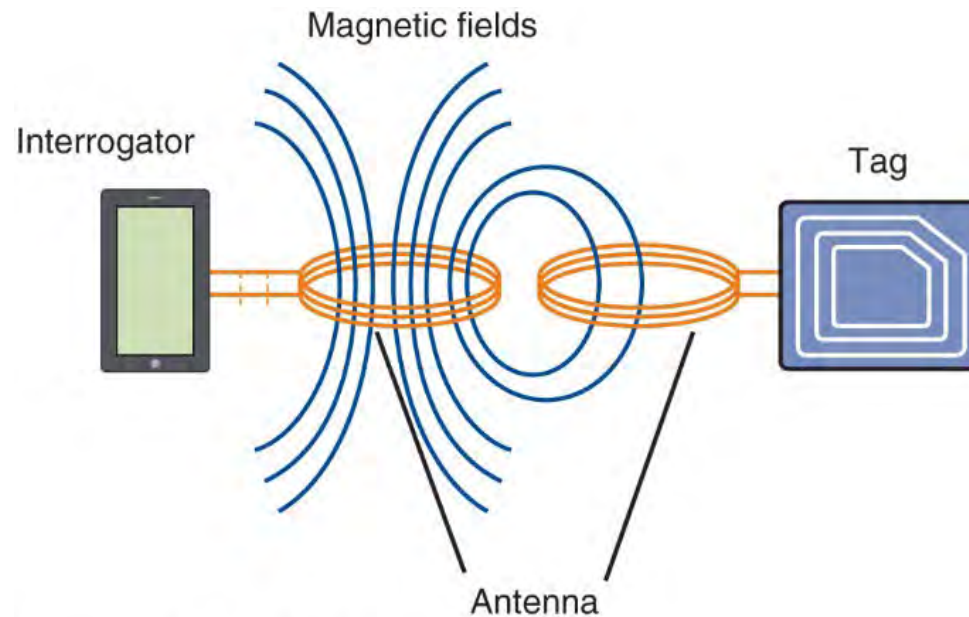


# Near Field Communication (NFC) Attacks (1 of 4)

- Near field communication (NFC)
  - A set of standards used to establish communication between devices in close proximity
  - Once devices are brought within 4 cm of each other or tapped together, two-way communication is established
- Devices using NFC can be active or passive
  - Passive NFC device – contains information that other devices can read but does not read or receive any information (example, NFC tag)
  - Active NFC device – can read information as well as transmit data



# Near Field Communication (NFC) Attacks (2 of 4)



**Figure 8-2** NFC magnetic induction





# Near Field Communication (NFC) Attacks (3 of 4)

- Examples of NFC uses:
  - Automobile
  - Entertainment
  - Office
  - Retail stores
  - Transportation
- NFC devices are used in contactless payment systems
  - A consumer can pay for a purchase by simply tapping a store's payment terminal with their smartphone



# Near Field Communication (NFC) Attacks (4 of 4)

Vulnerability	Explanation	Defense
Eavesdropping	Unencrypted NFC communication between the device and terminal can be intercepted and viewed	Because an attacker must be extremely close to pick up the signal, users should remain aware of their surroundings while making a payment
Data theft	Attackers can “bump” a portable reader to a user’s smartphone in a crowd to make an NFC connection and steal payment information stored on the phone	This can be prevented by turning off NFC while in a large crowd
Man-in-the-middle attack	An attacker can intercept the NFC communications between devices and forge a fictitious response	Devices can be configured in pairing so one device can only send while the other can only receive
Device theft	The theft of a smartphone could allow an attacker to use that phone for purchases	Smartphone should be protected with passwords or strong PINs



# Radio Frequency Identification (RFID)

## Attacks (1 of 2)

- Radio frequency identification (RFID)
  - Commonly used to transmit information between employee identification badges, inventory tags, book labels, and other paper-based tags that can be detected by a proximity reader
- Most RFID tags are passive
  - Do not have their own power supply
  - Because they do not require a power supply, they can be very small
- RFID tags are susceptible to different attacks
- Current version of RFID standards known as Generation 2
  - Contains some security enhancements over the previous version



# Radio Frequency Identification (RFID)

## Attacks (2 of 2)

RFID attack type	Description of attack	Implications of RFID attack
Unauthorized tag access	A rogue RFID reader can determine the inventory on a store shelf to track the sales of specific items	Sales information could be used by a rival product manufacturer to negotiate additional shelf space or better product placement
Fake tags	Authentic RFID tags are replaced with fake tags that contain fictitious data about products that are not in inventory	Fake tags undermine the integrity of the store's inventory system by showing data for items that do not exist
Eavesdropping	Unauthorized users could listen in on communications between RFID tags and readers	Confidential data, such as a politician's purchase of antidepressants, could be sold to a rival candidate in a "smear" campaign



# Wireless Local Area Network Attacks

- A WLAN is designed to replace or supplement a wired LAN
- It is important to know about the:
  - History and specifications of IEEE WLANs
  - Hardware necessary for a wireless network
  - Different types of WLAN attacks directed at enterprise and home users



# IEEE WLANs (1 of 3)

- Institute of Electrical and Electronics Engineers (IEEE) WLANS
  - Most influential organization for computer networking and wireless communications
  - Dates back to 1884
  - Began developing network architecture standards in the 1980s
- 1997: release of IEEE 802.11
  - Standard for wireless local area networks (WLANs)
  - Higher speeds (5.5 Mbps and 11 Mbps) added in 1999: IEEE 802.11b
- IEEE 802.11a
  - Specifies maximum rated speed of 54Mbps using the 5GHz spectrum



## IEEE WLANs (2 of 3)

- IEEE 802.11g
  - Preserves stable and widely accepted features of 802.11b and increases data transfer rates similar to 802.11a
- IEEE 802.11n
  - Ratified in 2009
  - Improvements: speed, coverage area, resistance to interference, and strong security
- IEEE 802.11ac
  - Ratified in early 2014 and has data rates over 7 Gbps



## IEEE WLANs (3 of 3)

	<b>802.11</b>	<b>802.11b</b>	<b>802.11a</b>	<b>802.11g</b>	<b>802.11n</b>	<b>802.11ad</b>	<b>802.11ac</b>
Frequency	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz	2.4 GHz & 5 GHz	60 GHz	5 GHz
Maximum data rate	2 Mbps	11 Mbps	54 Mbps	54 Mbps	600 Mbps	7 Gbps	7.2 Gbps
Indoor range (feet/meters)	65/20	125/38	115/35	115/35	230/70	32/10	115/35
Outdoor range (feet/meters)	328/100	460/140	393/120	460/140	820/250	N/A	460/140
Ratification date	1997	1999	1999	2003	2009	2013	2014



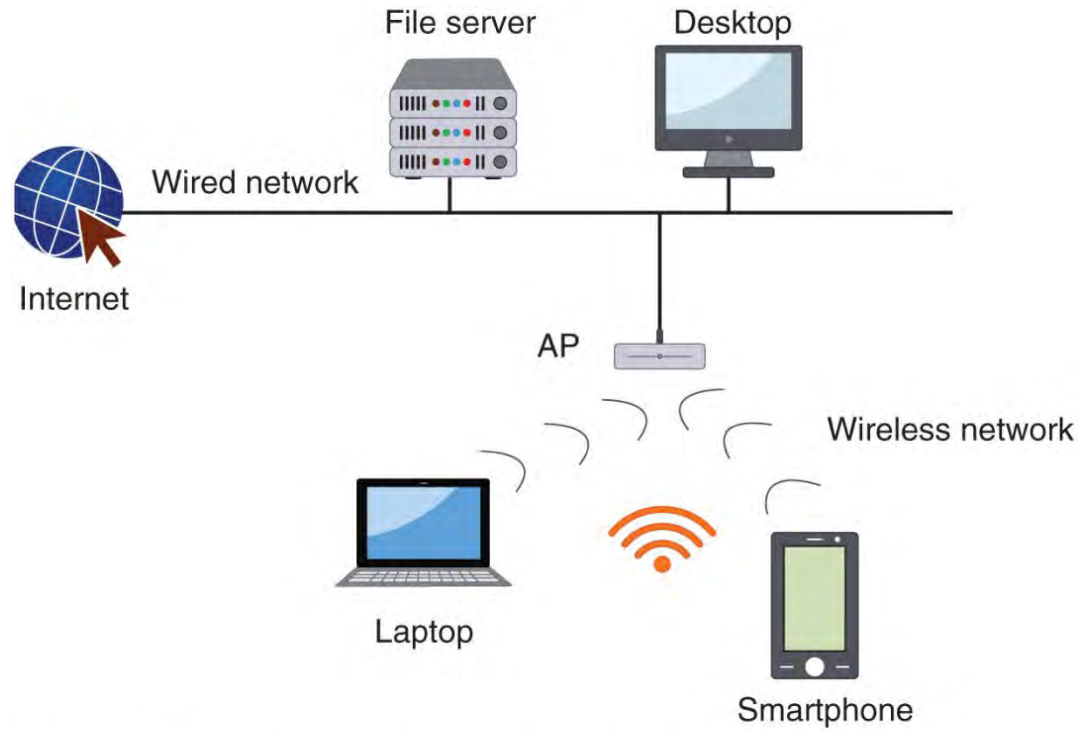


# WLAN Hardware (1 of 3)

- Wireless client network interface card adapter
  - Performs same functions as wired adapter
  - Antenna sends and receives signals through airwaves
- Access point (AP) major parts
  - Antenna and radio transmitter/receiver send and receive wireless signals
  - Bridging software to interface wireless devices to other devices
  - Wired network interface allows it to connect by cable to standard wired network
- Access point (AP) functions
  - Acts as “base station” for wireless network
  - Acts as a bridge between wireless and wired networks
    - Can connect to wired network by a cable



## WLAN Hardware (2 of 3)



**Figure 8-5** Access point (AP) in WLAN



## WLAN Hardware (3 of 3)

- A WLAN using an AP is operating in **infrastructure mode**
- Network that are not using an AP operate in **ad hoc mode**
  - Devices can only communicate between themselves and cannot connect to another network
  - The Wi-Fi Alliance has created a similar technical specification called **Wi-Fi Direct**
- Residential WLAN gateway
  - Used by small offices or home users to connect to the Internet
  - Features included are AP, firewall, router, dynamic host configuration protocol (DHCP) server, and others

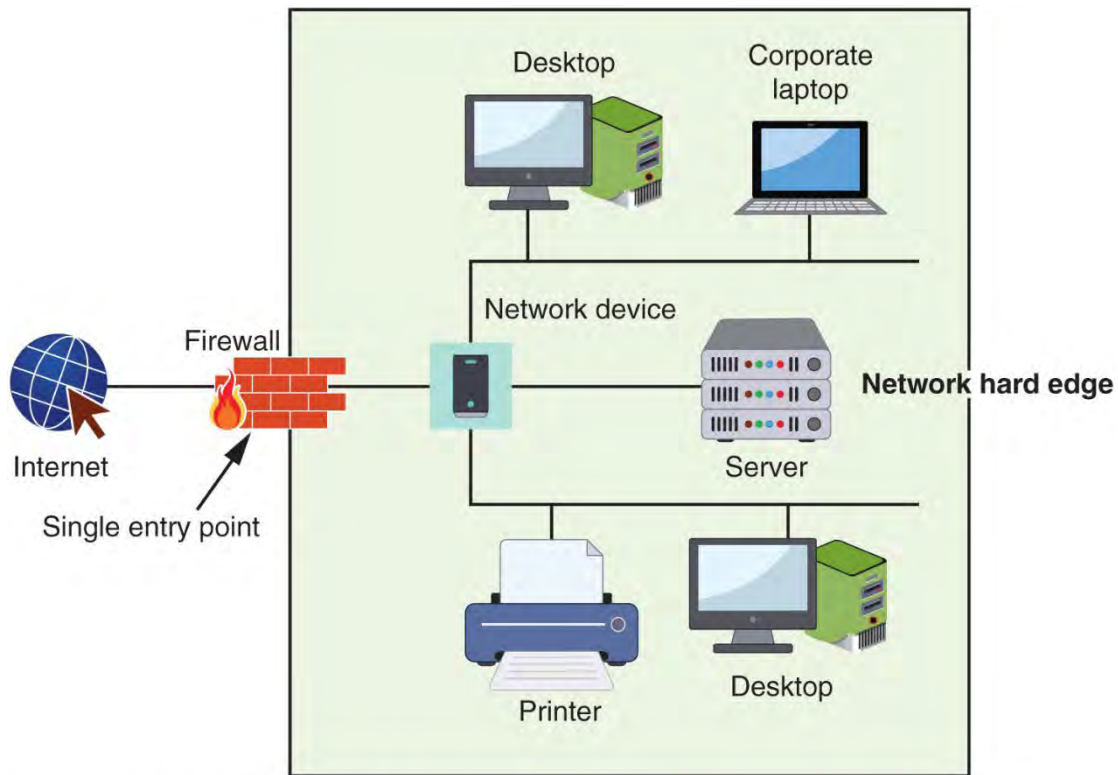


# WLAN Enterprise Attacks (1 of 7)

- In a network, a well-defined boundary protects data and resources
  - Boundary is known as a “hard edge”
- The introduction of WLANs in enterprises has changed hard edges to “blurred edges”
- Types of wireless attacks
  - Rogue access points
  - Evil twins
  - Intercepting wireless data
  - Wireless replay attacks
  - Denial of service attacks



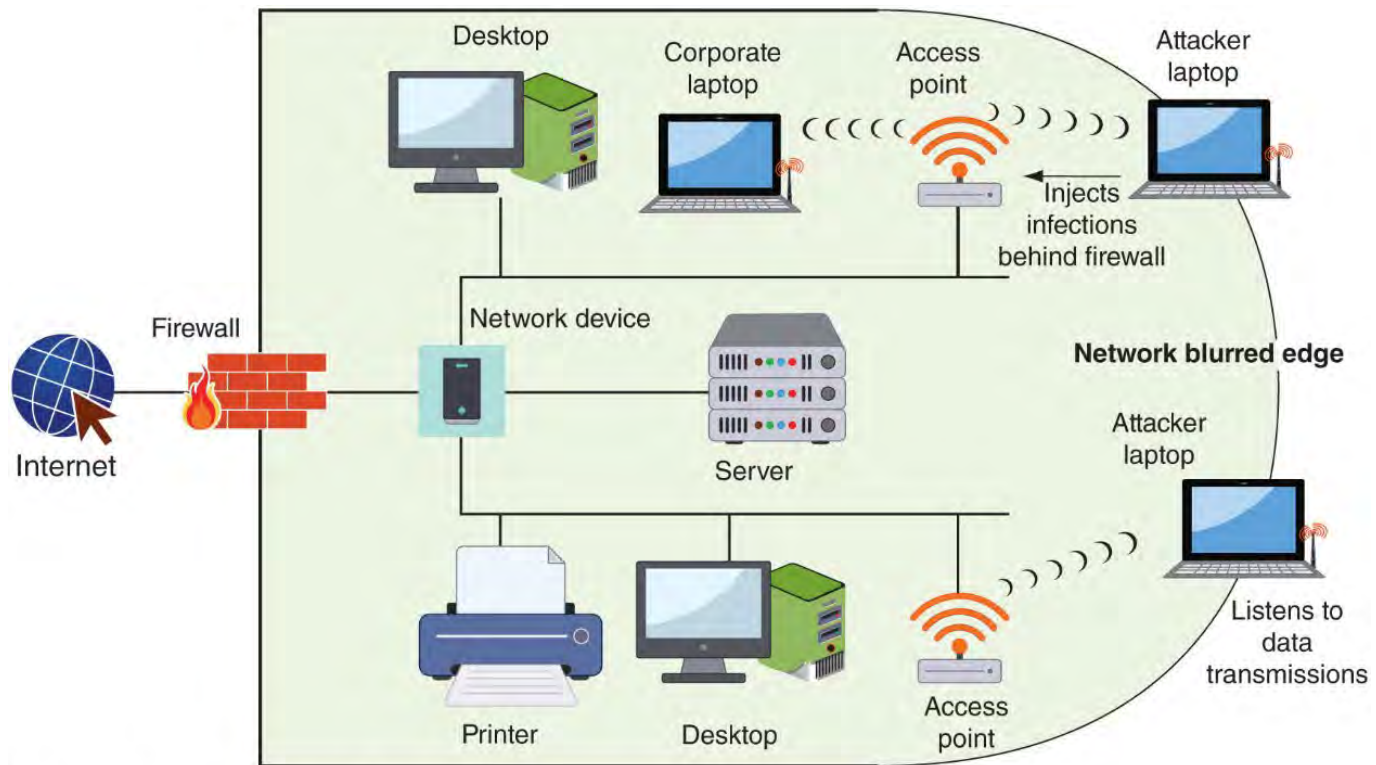
# WLAN Enterprise Attacks (2 of 7)



**Figure 8-6** Network hard edge



# WLAN Enterprise Attacks (3 of 7)



**Figure 8-7** Network blurred edge

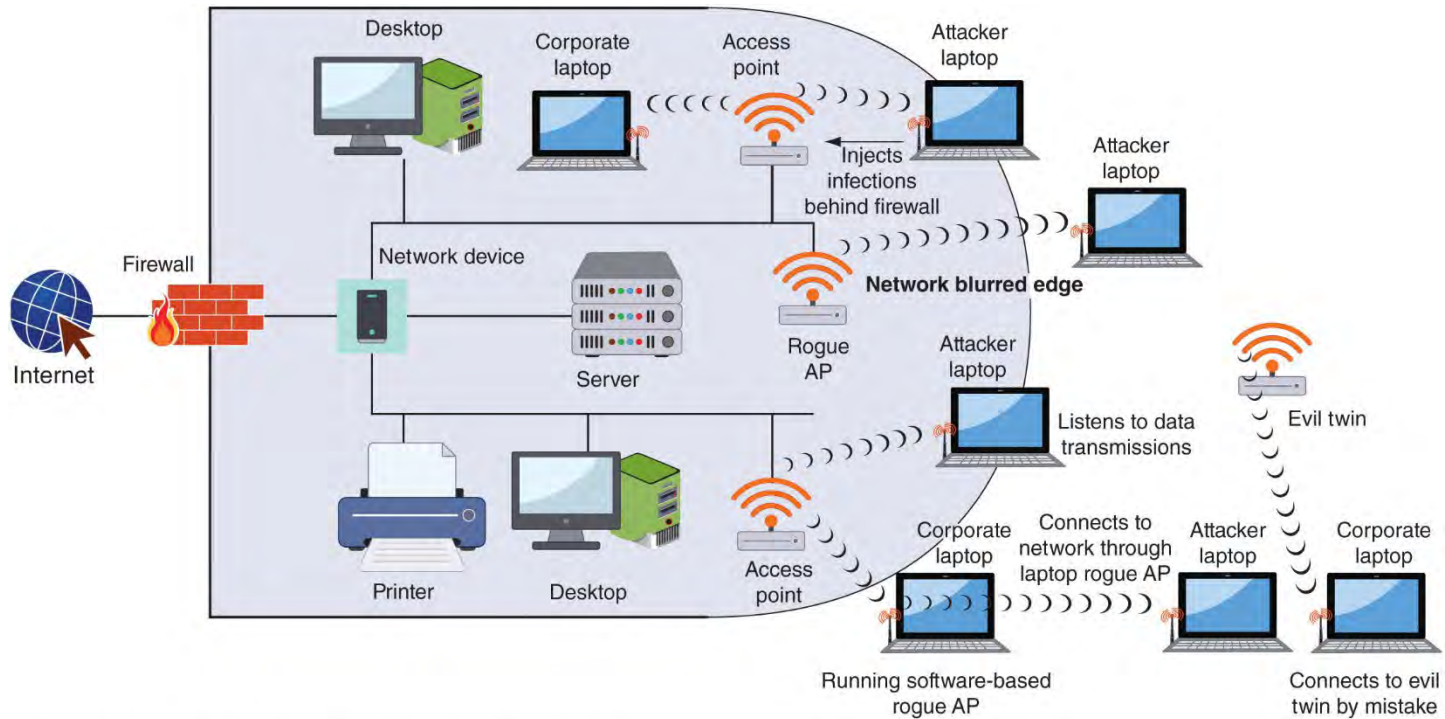


## WLAN Enterprise Attacks (4 of 7)

- Rogue access point
  - An unauthorized access point that allows an attacker to bypass network security configurations
  - Usually set up by an insider (employee)
  - May be set up behind a firewall, opening the network to attacks
- Evil twin
  - AP set up by an attacker
  - Attempts to mimic an authorized AP
  - Attackers capture transmissions from users to evil twin AP



# WLAN Enterprise Attacks (5 of 7)



**Figure 8-8** Rogue access point and evil twin attacks





## WLAN Enterprise Attacks (6 of 7)

- Intercepting Wireless Data
  - An attacker can pick up the RF signal from an open or misconfigured AP
  - Using a WLAN to read this data could yield significant information to an attacker regarding the wired enterprise network
- Wireless Replay Attack
  - Also known as “hijacking”
  - The attacker captures transmitted wireless data, records it, and then sends it on to the original recipient without the attacker’s presence being detected
  - Can be accomplished using an evil twin AP
  - Known as a man-in-the-middle attack



# WLAN Enterprise Attacks (7 of 7)

- Wireless Denial of Service Attack
  - RF jamming - attackers use intentional RF interference to flood the RF spectrum with enough interference to prevent a device from communicating with the AP
  - Spoofing - attackers craft a fictitious frame that pretends to come from a trusted client when it actually comes from the attacker
  - Manipulating duration field values - attackers send a frame with the duration field set to a high value, preventing other devices from transmitting for that period of time
- Wireless Home Attacks - most home users fail to configure any security on their home networks
  - Attackers can:
    - Steal data
    - Read wireless transmissions
    - Inject malware
    - Download harmful content



# Vulnerabilities of IEEE Wireless Security

- Original IEEE 802.11 committee recognized wireless transmissions could be vulnerable
  - Implemented several wireless security protections in the standard
  - Left others to WLAN vendor's discretion
  - Protections were vulnerable and led to multiple attacks



# Wired Equivalent Privacy

- WEP – an IEEE 802.11 security protocol designed to ensure that only authorized parties can view transmissions
  - Encrypts plaintext into ciphertext
- Secret key is shared between wireless client device and AP
- WEP vulnerabilities
  - WEP can only use 64-bit or 128-bit number to encrypt
    - **Initialization vector (IV)** is only 24 of those bits
    - Short length makes it easier to break
  - Violates cardinal rule of cryptography: avoid a detectable pattern
    - Attackers can see duplication when IVs start repeating



# Wi-Fi Protected Setup

- WPS is an optional means of configuring security on WLANS
  - Two common WPS methods:
    - PIN method - utilizes a PIN printed on a sticker of the wireless router or displayed through a software wizard
      - User enters Pin and security configuration automatically occurs
    - Push-button method - user pushes buttons and security configuration takes place
  - Design and implementation flaws:
    - There is no lockout limit for entering PINs
    - The last PIN character is only a checksum
    - The wireless router reports the validity of the first and second halves of the PIN separately
-



# MAC Address Filtering (1 of 3)

- Method of controlling WLAN access
  - Limit a device's access to AP
- Media Access Control (MAC) address filtering
  - Used by nearly all wireless AP vendors
  - Permits or blocks device based on MAC address
- Vulnerabilities of MAC address filtering
  - Addresses exchanged in unencrypted format
    - Attacker can see address of approved device and substitute it on his own device
  - Managing large number of addresses is challenging



## MAC Address Filtering (2 of 3)

Organizational Unique Identifier (OUI)      Individual Address Block (IAB)

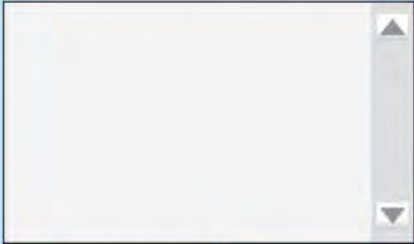
00-50-F2-7C-62-E1

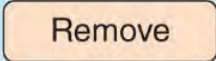
**Figure 8-9**    MAC address

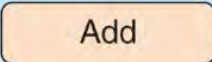


# MAC Address Filtering (3 of 3)

Filter: ☒ Allow only stations in list  
☐ Block all stations in list

Stations List: 

 Remove

MAC Address:  :  :  :  :  :   Add

**Figure 8-10** MAC address filtering





# SSID Broadcasting

- Service Set Identifier (SSID)
  - The user-supplied network name of a wireless network; usually broadcast so that any device can see it
    - The broadcast can be restricted
- Some wireless security sources encourage users to configure their APs to prevent the broadcast of the SSID
- Not advertising the SSID only provides a weak degree of security and has limitations:
  - SSID can be discovered when transmitted in other frames
  - May prevent users from being able to freely roam from one AP coverage area to another
  - It's not always possible to turn off SSID beaconing



# Wireless Security Solutions

- A unified approach to WLAN security was needed
  - IEEE and Wi-Fi Alliance began developing security solutions
- Resulting standards used today
  - IEEE 802.11i
  - WPA and WPA2



# Wi-Fi Protected Access (WPA)

- Introduced in 2003 by the Wi-Fi Alliance
- A subset of IEEE 802.11i
- Two modes of WPA:
  - WPA Personal
  - WPA Enterprise
- WPA addresses both encryption and authentication



# Temporal Key Integrity Protocol (TKIP) Encryption

- Temporal Key Integrity Protocol (TKIP) Encryption
  - Used in WPA
  - Uses a longer 128 bit key than WEP
  - Dynamically generated for each new packet
  - Includes a **Message Integrity Check (MIC)**, designed to prevent man-in-the-middle attacks



# Preshared Key (PSK) Authentication

- Authentication for WPA Personal is accomplished by using a preshared key (PSK)
- After AP configured, client device must have same key value entered
- Key is shared prior to communication taking place
- Uses a passphrase to generate encryption key
  - Must be entered on each AP and wireless device in advance
- Devices that have the secret key are automatically authenticated by the AP



# WPA Vulnerabilities

- Key management
  - Key sharing is done manually without security protection
  - Keys must be changed on a regular basis
  - Key must be disclosed to guest users
- Passphrases
  - PSK passphrases of fewer than 20 characters subject to cracking



# Wi-Fi Protected Access 2 (WPA2)

- Second generation of WPA is known as WPA2
  - Introduced in 2004
  - Based on final IEEE 802.11i standard
- Two modes of WPA2:
  - WPA2 Personal
  - WPA2 Enterprise
- Addresses to major security areas of WLANs:
  - Encryption
  - Authentication



# AES-CCMP Encryption

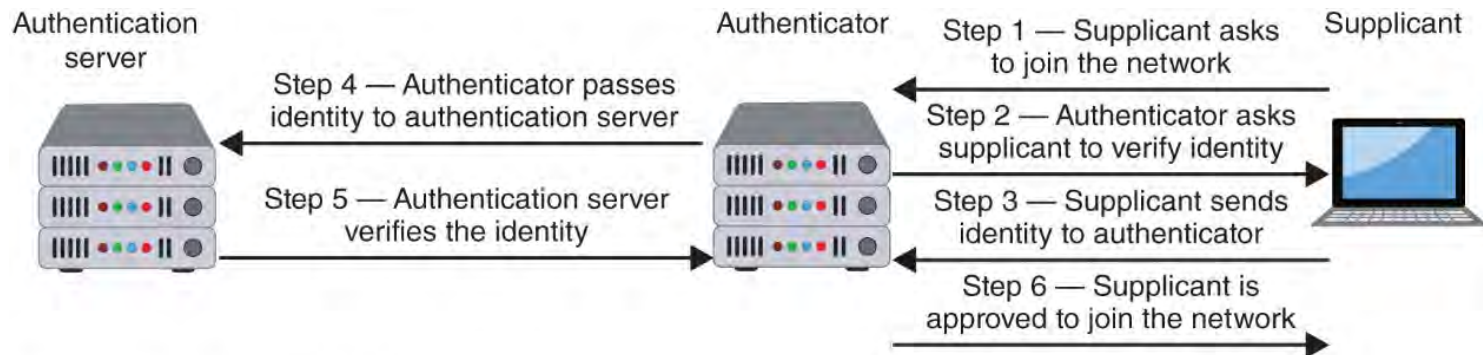
- Advanced Encryption Standard (AES) block cipher
- AES performs three steps on every block (128 bits) of plaintext
  - Within second step, multiple iterations are performed
  - Bytes are substituted and rearranged
- **Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)** is the encryption protocol used for WPA2
  - Specifies the use of CCM with AES
- The Cipher Block Chaining Message Authentication Code (CBC-MAC) component of CCMP provides data integrity and authentication
- Both CCMP and TKIP use a 128-bit key for encryption
  - Both methods use a 64-bit MIC value





# IEEE 802.1x Authentication (1 of 3)

- Originally developed for wired networks
- Provides greater degree of security by implementing port-based authentication
- Blocks all traffic on a port-by-port basis until client is authenticated



**Figure 8-11** IEEE 802.1x process



# IEEE 802.1x Authentication (2 of 3)

- Extensible Authentication Protocol (EAP)
    - A framework for transporting authentication protocols
    - Defines message format
    - Uses four types of packets
      - Request
      - Response
      - Success
      - Failure
  - A common EAP protocol is Protected EAP (PEAP)
    - Simplifies deployment of 802.1x by using Microsoft Windows logins and passwords
    - Creates encrypted channel between client and authentication server
-



# IEEE 802.1x Authentication (3 of 3)

EAP name	Description
EAP-TLS	This protocol uses digital certificates for authentication
DAP-TTLS	This protocol securely tunnels client password authentication within Transport Layer Security (TLS) records
EAP-FAST	This protocol securely tunnels any credential form for authentication (such as a password or a token) using TLS



# Additional Wireless Security Protections

- Other security steps can be taken:
  - Rogue AP system detection
  - Using the correct type of AP
  - AP configuration settings
  - Wireless peripheral protection



# Rogue AP System Detection

- Rogue AP Discovery Tools - 4 types of wireless probes can monitor airwaves for traffic:
  - **Wireless device probe**
  - **Desktop probe**
  - **Access point probe**
  - **Dedicated probe**
- Once a suspicious signal is detected by a wireless probe
  - The information is sent to a centralized database where WLAN management system software compares it to a list of approved APs
  - Any device not on the list is considered a rogue AP



## AP Type (1 of 4)

- AP types can be divided into:
  - Fat vs. thin
  - Controller vs. standalone
  - Captive portal APs
- Fat vs. Thin APs
  - Autonomous APs have the intelligence required to manage wireless authentication, encryption, and other functions for the wireless devices they serve (called fat APs)
  - “Lightweight” APs do not contain all the management and configuration functions found in fat APs (called thin APs)

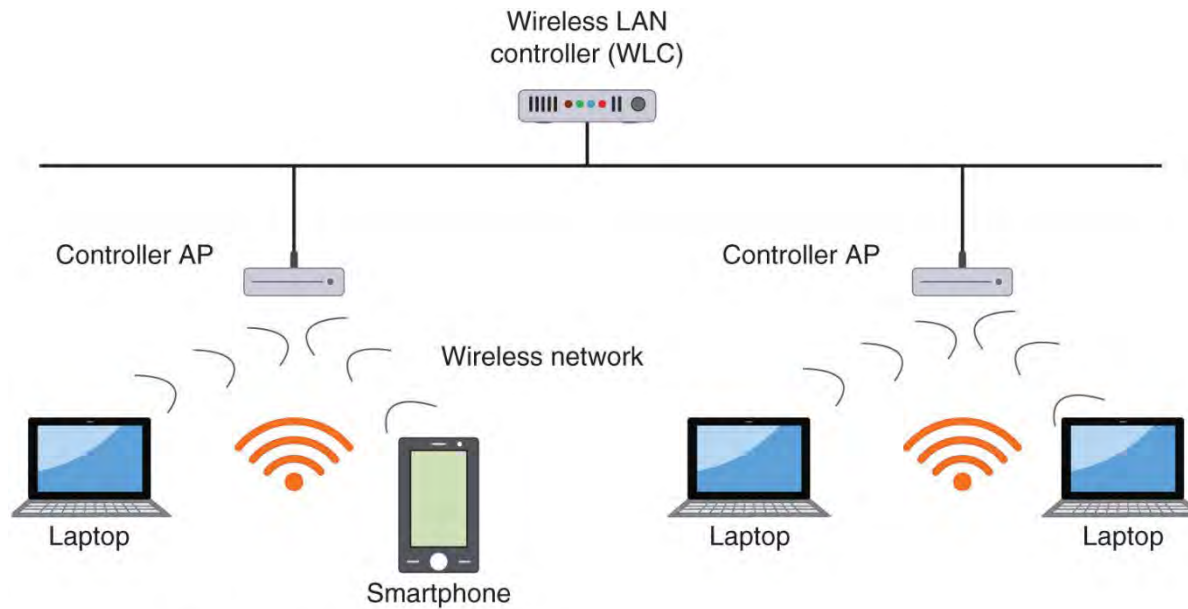


## AP Type (2 of 4)

- Standalone vs. Controller APs
  - Controller APs can be managed through a dedicated wireless LAN controller (WLC)
  - The WLC is the single device that can be configured and settings are automatically distributed to all controller APs
  - Other advantages of controller APs:
    - Handoff procedure is eliminated because all authentications are performed in the WLC
    - Offers tools that provide for monitoring the environment and providing information regarding the best locations for APs, wireless AP configuration settings, and power settings



## AP Type (3 of 4)



**Figure 8-12** Controller APs with WLC





## AP Type (4 of 4)

- Captive Portal APs
  - Uses a standard web browser to provide information
  - Gives the wireless user the opportunity to agree to a policy or present valid login credentials



# AP Configuration and Device Options (1 of 3)

- Other AP configuration settings are designed to limit the spread of the wireless RF signal
  - So that a minimum amount of signal extends past the physical boundaries of the enterprise to be accessible to outsiders
- Site Surveys
  - An in-depth examination and analysis of a wireless LAN site



## AP Configuration and Device Options (2 of 3)

- Signal Strength Settings
  - Some APs allow adjustment of the power level at which the LAN transmits
  - Reducing power allows less signal to reach outsiders
- Spectrum Selection
  - Some APs provide the ability to adjust frequency spectrum settings, including:
    - Frequency band
    - Channel selection
    - Channel width

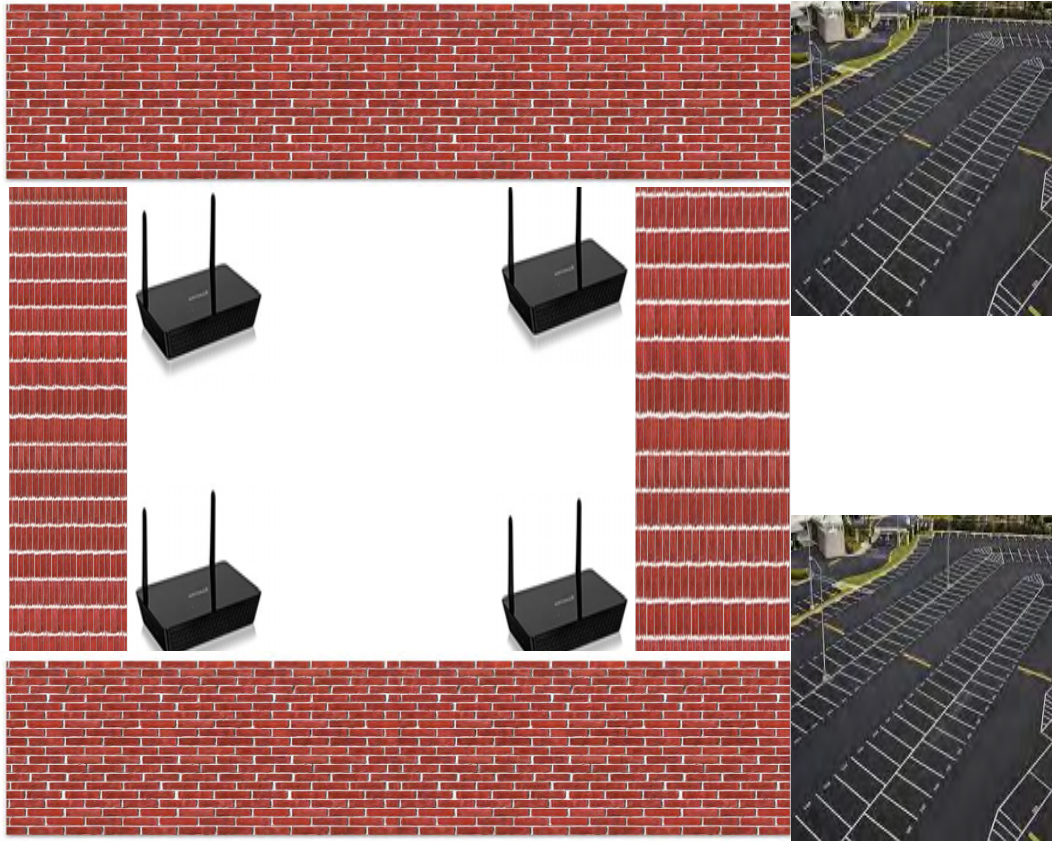


# AP Configuration and Device Options (3 of 3)

- Antennas
  - AP should be located near the center of coverage area
  - Place high on a wall to reduce signal obstructions and deter theft
  - If possible, the AP and antenna should be positioned so that a minimal amount of signal reaches beyond the security perimeter of the building
- Wireless Peripheral Protection
  - Vulnerabilities in wireless mice and keyboards are common
  - One attack could let a threat actor inject mouse movements or keystrokes from a nearby antenna up to 100 yards away
  - Protections include:
    - Updating or replacing any vulnerable devices
    - Switching to more fully tested Bluetooth mice and keyboards
    - Substitute with a wired mouse or keyboard



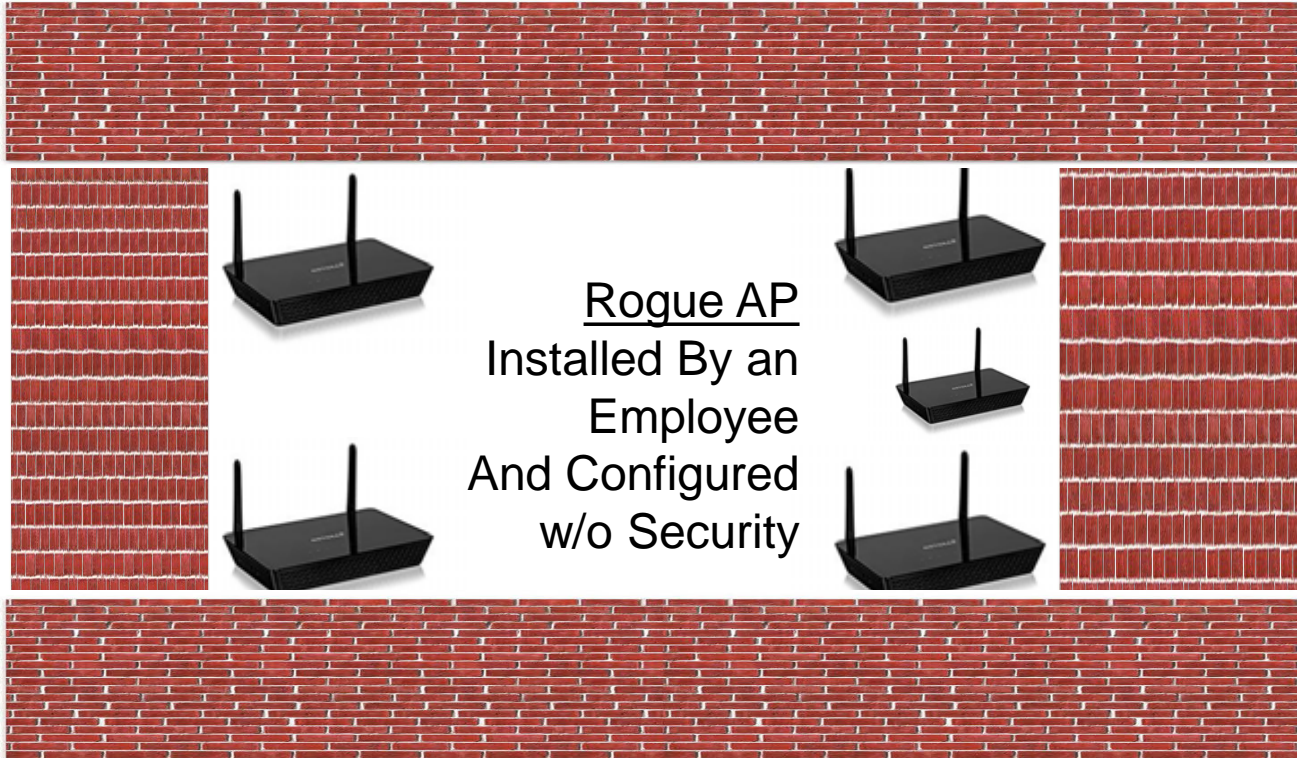
# COMPLETE THE DIAGRAM



- Where would you find...
  - A Rogue Access Point
    - Who installed it?
    - What is special about the config?
- Where would you find...
- An Evil Twin
  - Who installed it?
  - What is special about the config?



# COMPLETE THE DIAGRAM



Rogue AP  
Installed By an  
Employee  
And Configured  
w/o Security



Evil Twin  
Installed By  
Hacker  
Configured  
w/ Matching  
SSID





## Review Questions

Which technology is predominately used for contactless payment systems?

- A. near field communication (NFC)
- B. wireless local area network (WLAN)
- C. Bluetooth
- D. Radio Frequency ID (RFID)



## Review Questions

Which technology is predominately used for contactless payment systems?

- A. near field communication (NFC)
- B. wireless local area network (WLAN)
- C. Bluetooth
- D. Radio Frequency ID (RFID)





## Review Questions

Why is a rogue AP a security vulnerability?

- A. It uses the weaker IEEE 80211i protocol.
- B. It conflicts with other network firewalls and can cause them to become disabled.
- C. It allows an attacker to bypass network security configurations.
- D. It requires the use of vulnerable wireless probes on all mobile devices.



# Review Questions

Why is a rogue AP a security vulnerability?

- A. It uses the weaker IEEE 80211i protocol.
- B. It conflicts with other network firewalls and can cause them to become disabled.
- C. **It allows an attacker to bypass network security configurations.**
- D. It requires the use of vulnerable wireless probes on all mobile devices.



## Review Questions

Vito visits a local coffee shop on his way to school and accesses its free Wi-Fi. When he first connects, a screen appears that requires him to first agree to an Acceptable Use Policy (AUP) before continuing. What type of AP has he encountered?

- A. captive portal
- B. web-based portal
- C. rogue portal
- D. authenticated portal



## Review Questions

Vito visits a local coffee shop on his way to school and accesses its free Wi-Fi. When he first connects, a screen appears that requires him to first agree to an Acceptable Use Policy (AUP) before continuing. What type of AP has he encountered?

- A. **captive portal**
- B. web-based portal
- C. rogue portal
- D. authenticated portal



# Review Questions

The primary design of a(n) \_\_\_\_\_ is to capture the transmissions from legitimate users.

- A. rogue access point
- B. WEP
- C. evil twin
- D. Bluetooth grabber



## Review Questions

The primary design of a(n) \_\_\_\_\_ is to capture the transmissions from legitimate users.

- A. rogue access point
- B. WEP
- C. evil twin
- D. Bluetooth grabber



## Review Questions

AES-CCMP is the encryption protocol standard used in \_\_\_\_\_.

- A. WPA
- B. WPA2
- C. IEEE 802.11
- D. NFC



# Review Questions

AES-CCMP is the encryption protocol standard used in \_\_\_\_\_.

- A. WPA
- B. **WPA2**
- C. IEEE 802.11
- D. NFC



# Coming Up Next...

## CompTIA Security+

### Chapter 9

#### Client and Application Security

