Chapter 7

Securing Wireless LANs

Episode 7.01

Episode title: **Wi-Fi Encryption Standards**

Objective: **3.4 Given a scenario, install and configure wireless security settings.**

Wired Equivalent Privacy (WEP)

- Part of original 802.11 standard
- RC4 streaming
- Began with initialization vector (IV)
- Problem was with IVs

IEEE 802.11i

- AES instead of RC4
- Pre-shared key (PSK) instead of IV
  - Or WPA-Enterprise
    - Authenticate with RADIUS server
- The problem: most WAPs and network cards couldn't handle AES
- Solution: Wi-Fi Protected Access (WPA)
  - RC4 with PSK or RADIUS server

IEEE 802.11i

- WPA2
  - AES
  - Can do RADIUS or PSK
  - Counter-Mode/CBC-MAC Protocol
    - CCMP
  - The problem: can be cracked through the handshake

WPA3

- Disallows outdated protocols
- Protected Management Frames (PMF)
- Simultaneous authentication of equals (SAE)

Wi-Fi Protected Setup (WPS)

- Must have WPS-capable wireless access points (WAPs) and devices
- Press button on both WAP and device
- Creates a WPA2-encrypted connection
- The problem: easy to crack
- The solution: devices no longer include it

Quick Review

- WEP utilized RC4 encryption and is no longer in use
- 802.11i introduced AES encryption, PSKs, and enterprise mode, but many devices couldn't handle the AES encryption process
- WPA solved this problem by allowing RC4, but eventually was hacked
- WPA2 is still in use and utilizes AES with CCMP and can be used in personal (PSK) or enterprise (RADIUS)
- WPA3 is the newest and best authentication protocol and uses PMF and SAE
- WPSes became crackable and have been deprecated

Episode 7.02

Episode title: **RFID, NFC, and Bluetooth**

Objective:

1.4 Given a scenario, analyze potential indicators associated with network attacks.

3.5 Given a scenario, implement secure mobile solutions.

Radio Frequency Identifier (RFID)

- Uses RF communication to track objects with RFID tags
- Range is ~5 meters (16.5 feet)
- Commonly used for inventory control, locating pets, and in some passports
- RFID tags are normally powered by the reading/scanning device

Near Field Communication (NFC)

- Type of RFID
- Close-range wireless communications
  - Approximately 5 cm (1.5 inches)
- Common uses
  - Payment cards
  - Smartphone (data sharing, payments)
  - Read/write NFC tags

Bluetooth

- 802.15.1 standard
  - 2.4 or 5 GHz frequency range
- Wireless networking with shorter range than Wi-Fi
  - Class 1
    - Up to 100 meters (328 feet)
    - Example: USB Wi-Fi dongles
  - Class 2
    - 10 meters (33 feet)
    - Example: Bluetooth headset

Bluetooth

- Devices must be paired together to communicate
  - Car stereo
  - Headset
  - Keyboards

Bluetooth Attacks

- Bluejacking
  - Unauthorized sending of anonymous messages to a Bluetooth device
  - Example: sharing bogus contact information with a message as the contact name
- Bluesnarfing
  - Data theft from remote devices using Bluetooth
- Mitigation
  - Disable Bluetooth when not needed

Quick Review

- RFID uses wireless tags on objects; commonly used for inventory control
- NFC is a short-range wireless technology commonly used for payment cards
- Bluetooth is a wireless technology for pairing devices together such as smartphones, speakers, or headsets
- Bluejacking and bluesnarfing are Bluetooth attacks

Episode 7.03

Episode title: **Wi-Fi Coverage and Performance**

Objective:

3.4 Given a scenario, install and configure wireless security settings.

3.5 Given a scenario, implement secure mobile solutions.

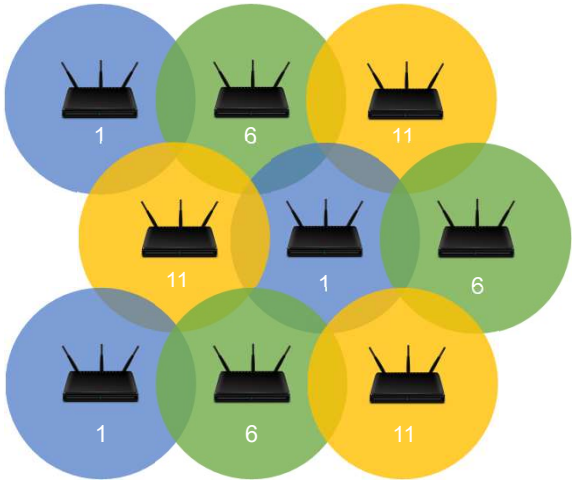
Wi-Fi Coverage and Performance

- Signal strength weakens over distance
  - Transmission power measured in decibel milliwatts (dBm)
  - -30 dBm is great, -80 not so great
- Atmospheric conditions affect wireless connectivity

Wi-Fi Site Survey

- Conduct during Wi-Fi deployment and troubleshooting
- Collect wireless stats
  - Signal strength
  - Noise
  - Channel overlapping
  - Transmission speeds

Wi-Fi Coverage and Channels



Quick Review

- A Wi-Fi site survey shows existing WLANs, signal strength, channel usages, and security settings
- Extended WLAN coverage is possible, but ensure channels do not overlap in adjacent cells
- Wi-Fi heat maps use colors to indicate areas with strong signal strength as well as dead zones

Episode 7.04

Episode title: **Wi-Fi Discovery and Attacks**

Objective: **1.4 Given a scenario, analyze potential indicators associated with network attacks.**

1.8 Explain the techniques used in penetration testing.

Wi-Fi Discovery and Mapping

- War-chalking
  - Sidewalk marking
- War-driving
  - Scan from within vehicle
- War-flying
  - Scan using a drone

Malicious WAP Targeting

- Rogue access point
  - Unauthorized wireless AP
- Evil twin
  - Unauthorized wireless AP mimicking valid AP name

Wi-Fi AP Beacon Frames

- Sent every ~100ms
- Clients cannot verify beacons
  - Key not established yet
  - Beacon frames are easily forged
- Contains
  - SSID (WLAN name)
  - Maximum transmit power (dBm)

Wi-Fi Attacks

- Connecting to open WLANs
- Cracking WEP passphrase
- RF signal jamming
  - Interference
  - Wi-Fi channel overlap
  - Flood AP with deauthentication (disassociation) packets
  - Denial of Service (DoS) attack

Quick Review

- WLANs can be discovered in proximity due to beacon frames
- Jamming attacks are interference attacks
- WEP passphrases are easily cracked
- Deauthentication/disassociation severs Wi-Fi client connections
- Client to AP handshakes can be captured to perform offline PSK attacks

Episode 7.05

Episode title: **Cracking WPA2**

Objective: **1.4 Given a scenario, analyze potential indicators associated with network attacks.**

Disassociation/ Deauthentication Attacks

- Discover APs
- Discover connected clients
- Disconnect active client from AP
  - sudo aireplay-ng -0 1 -a <AP MAC> -c <Client MAC>
- Monitor client-AP handshake
- Perform online or offline dictionary or brute-force to determine PSK

Quick Review

- The WLAN BSSID must be known when attacking a WLAN
- Client MAC address is required for some WLAN attacks
- Online or offline dictionary and brute-force attacks can crack WPA PSKs

Episode 7.06

Episode title: **Wi-Fi Hardening**

Objective: **3.4 Given a scenario, install and configure wireless security settings.**

Extensible Authentication Protocol (EAP)

- IEEE 802.1x RADIUS authentication
  - Supports identity federation
- EAP-FAST (Flexible Authentication via Secure Tunneling)
  - No certificates
  - Shared secret must be configured on both devices
- EAP-TLS
  - Server- and client-side certificates

Extensible Authentication Protocol (EAP)

- EAP-TTLS
  - Requires a server certificate
  - Encapsulates RADIUS messages
- Protected EAP
  - Requires a server certificate
  - Encapsulates EAP messages

Hardening Wi-Fi

- Change default AP credentials
- Hide the SSID
  - WLAN name is removed from AP beacon frames
  - Clients must know the SSID to connect
  - Clients must know PSK or credentials

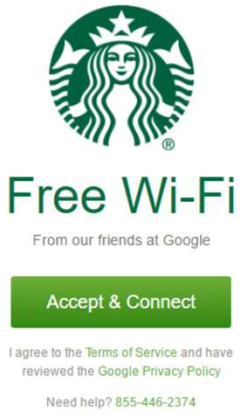
Wi-Fi Hardening

- Enable MAC filtering
- Use WPA3 Enterprise
  - RADIUS server authentication
- Limit signal emanation
  - Transmit power levels

Wi-Fi Hardening

- Captive portal
  - Landing page (Web site)
  - May require user authentication
    - Until authenticated, all HTTP requests show the landing page
  - User may only need to agree to terms of use

Wi-Fi Captive Portal



Quick Review

- Use RADIUS authentication for enterprise Wi-Fi networks
- EAP variants can be used to harden Wi-Fi authentication
- Hardening Wi-Fi includes changing default settings, hiding the SSID, using WPA3, and enabling MAC filtering
- Captive portals are initial landing pages when users connect to public Wi-Fi networks