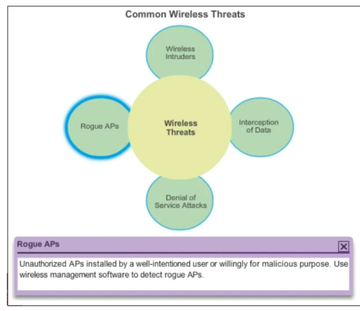
Lecture 9d - Wireless Security

Type	Lecture
Materials	Empty
Reviewed	☑

1. WLAN Threats

Securing Wireless



DoS Attack

- **Wireless DoS attacks can be the result of:**
  - **Improperly configured** devices
  - **Configuration errors** can **disable the WLAN**
  - A **malicious user** intentionally **interfering** with the **wireless communication. Disable** the wireless network where **no legitimate** device can **access** the medium
- **Accidental interference**
  - WLANs **operate** in the **unlicensed frequency** bands and are **prone** to **interference** from other wireless devices such as microwave ovens, cordless phones, baby monitors…
  - **2.4 GHz band** is **more prone** to interference than the **5 GHz band**

Management Frame DoS Attacks

- **A spoofed disconnect attack**
  - Occurs when an attacker **sends a series** of "**disassociate**" **commands** to all wireless clients.
  - **Cause** all clients to **disconnect.**
  - The wireless clients immediately try to re-associate, which creates a burst of traffic.
- **A CTS flood**
  - An attacker takes advantage of the **CSMA/CA** contention method to **monopolize the bandwidth**
  - The attacker **repeatedly** floods **Clear to Send (CTS)** frames to a bogus **Station**.
  - All wireless clients sharing the **RF medium** receive the CTS and **withhold transmissions** until the attacker **stops transmitting** the **CTS** frames

Rogue Access Points

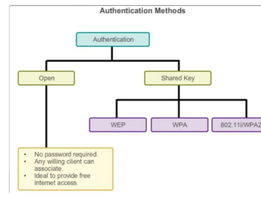
- A **rogue AP** is an **AP** or **wireless router** that has been:
  - **Connected** to a corporate network **without explicit authorization** and **against corporate policy**
  - **Connected** or **enabled** by an attacker to **capture client data**, such as the **MAC addresses** of clients (both wireless and wired), or to **capture and disguise data packets**, to **gain access** to network **resources**, or to launch **man-in-the-middle (MITM) attacks**
  - To **prevent** the installation of **rogue APs**, **organizations** should actively **monitor** the radio **spectrum** for **unauthorized APs**

Man-in-the-Middle Attack

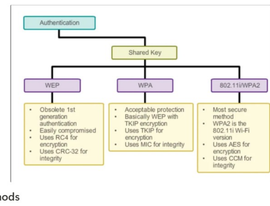
- **"Evil twin AP" attack:**
  - A popular wireless **MITM** attack where an attacker introduces a **rogue AP** and **configures** it with the **same SSID as a legitimate AP**
  - **Locations offering free Wi-Fi**, such as airports, cafes, and restaurants, are **common MITM targets** due to **open authentication**
  - Connecting **wireless clients** would see **two APs offering wireless access.** Those **near the rogue AP** find a stronger signal and will likely **associate** with the **evil twin AP**. **User traffic** is now **sent** to the **rogue AP**, which in turn **captures** the data and forwards it to the legitimate AP
  - Return **traffic** from the **legitimate AP** is **sent** to the **rogue AP**, captured, and then forwarded to the **unsuspecting STA**

2. Securing WLANs

- **Wireless Security Overview**
  - Use **authentication** and **encryption** to secure a wireless network.



- **Shared Key Authentication Methods**



- **Encryption Methods**

  IEEE 802.11i and the Wi-Fi Alliance WPA and WPA2 standards use the following encryption protocols:

  - **Temporal Key Integrity Protocol (TKIP)**
    - Used by **WPA**
    - Makes use of **WEP**, but **encrypts** the **Layer 2 payload** using TKIP, and carries out a **Cisco Message Integrity Check (MIC)**
  - **Advanced Encryption Standard (AES)**
    - Encryption method used by **WPA2**
    - **Stronger** method of encryption.
    - **Always** choose **WPA2** with **AES** when possible
- **Authenticating a Home User**

  WPA and WPA2 support two types of authentication:

  - **Personal**
    - Intended for **home** or **small office networks**, or authenticated users who use a **pre-shared key (PSK)**
    - **No special authentication** server is required
  - **Enterprise**
    - Requires a **Remote Authentication Dial-In User Service (RADIUS)** authentication server
    - Provides additional security
    - Users **authenticate** using **802.1X standard**, which uses the **Extensible Authentication Protocol (EAP)** for authentication
    - Allows **per-user security**