7.1.5 Wireless Security Facts

This lesson covers the following topics:

- Authentication methods
- Wireless security standards

Authentication Methods

Authentication to wireless networks is implemented using the following methods:

Method	Description
Open	Open authentication requires that clients provide a MAC address in order to connect to the wireless network. ▪ You can use open authentication to allow any wireless client to connect to the AP. Open authentication is typically used on public networks. ▪ You can implement MAC address filtering to restrict access to the AP to only known (or allowed) MAC addresses. Because MAC addresses are easily spoofed, this provides little practical security.
Shared Key	With shared key authentication, clients and APs are configured with a shared key (called a *secret* or a *passphrase*). Only devices with the correct shared key can connect to the wireless network. ▪ All APs and all clients use the same authentication key. ▪ Shared key authentication should be used only on small, private networks. ▪ Shared key authentication is relatively insecure, as hashing methods used to protect the key can be easily broken.
802.1x	802.1x authentication uses usernames and passwords, certificates, or devices such as smart cards to authenticate wireless clients. Originally designed for Ethernet networks, the 802.1x standards have been adapted for use in wireless networks to provide secure authentication. 802.1x authentication requires the following components: ▪ A RADIUS or TACACS+ server to centralize user account and authentication information. A centralized database for user authentication is required to allow wireless clients to roam between cells but authenticate using the same account information ▪ A PKI for issuing certificates. At a minimum, the RADIUS server must have a server certificate. To support mutual authentication, each client must also have a certificate Use 802.1x authentication on large, private networks. Users authenticate with unique usernames and passwords.

Wireless Security Standards

Security for wireless networking is provided from the following standards:

Method	Description
Wired Equivalent Privacy (WEP)	WEP is an optional component of the 802.11 specifications that were deployed in 1997. WEP has the following weaknesses: ▪ A static pre-shared key (PSK) is configured on the AP and the client. It cannot be dynamically changed or exchanged without administration. As a result, every host on large networks usually uses the same key. ▪ Because key values are short and don't change, the key can be captured and easily broken. Because of the inherent security flaws, avoid using WEP whenever possible. If using WEP cannot be avoided, implement it only using open authentication. Shared key authentication with WEP uses the same key for both encryption and authentication, exposing the key to additional attacks.
Wi-Fi Protected Access (WPA)	WPA is the implementation name for wireless security based on initial 802.11i drafts that was deployed in 2003. It was intended to be an intermediate measure to take the place of WEP while a fully secured system (802.11i) was prepared. WPA: ▪ Uses Temporal Key Integrity Protocol (TKIP) for encryption ▪ Supports both pre-shared key (WPA-PSK or WPA Personal) and 802.1x (WPA Enterprise) authentication ▪ Can use dynamic keys or pre-shared keys ▪ Can typically be implemented in WEP-capable devices through a software/firmware update

	WPA keys can also be predicted by reconstructing the Message Integrity Check (MIC) of an intercepted packet, sending the packet to an AP, and observing whether the packet is accepted by the AP.
Wi-Fi Protected Access 2 (WPA2) or 802.11i	WPA2 is the implementation name for wireless security that adheres to the 802.11i specifications. It was deployed in 2005. It is built upon the idea of Robust Secure Networks (RSN). Like WPA, it resolves the weaknesses inherent in WEP. It is intended to eventually replace both WEP and WPA. WPA2: ▪ Uses Advanced Encryption Standard (AES) as the encryption method ▪ Supports both pre-shared key (WPA2-PSK or WPA2 Personal) and 802.1x (WPA2 Enterprise) authentication ▪ Can use dynamic keys or pre-shared keys
Wi-Fi Protected Access 3 (WPA3)	WPA3 is a new authentication launched in 2018. It is a more resilient version of WPA2. WPA3: ▪ Uses password-based authentication ▪ Provides better protection against password guessing attempts by using Simultaneous Authentication of Equals (SAE) ▪ Offers 192-bit cryptographic strength, giving additional protection for networks dealing with sensitive data

When transmitting data on a wireless network, it's important to know if the channel you are using is encrypted. Information sent on unencrypted channels, where no security is being used, can be easily intercepted and viewed. If needed, IPsec can be used to provide security when sending information on an unencrypted channel.