# ECCS-3631
# Networks and Data Communications

## Module 8-2
## Wi-Fi Security

Dr. Ajmal Khan

# Your Internet and Wi-Fi Service

- All you need Wi-Fi from your Internet Connection.
- How much do you pay for your Internet?

- What are your thoughts if someone offers to install a Free Open Wi-Fi in your neighborhood, you can save money to pay for your Internet connection.

# Wireless Security

**Authentication**

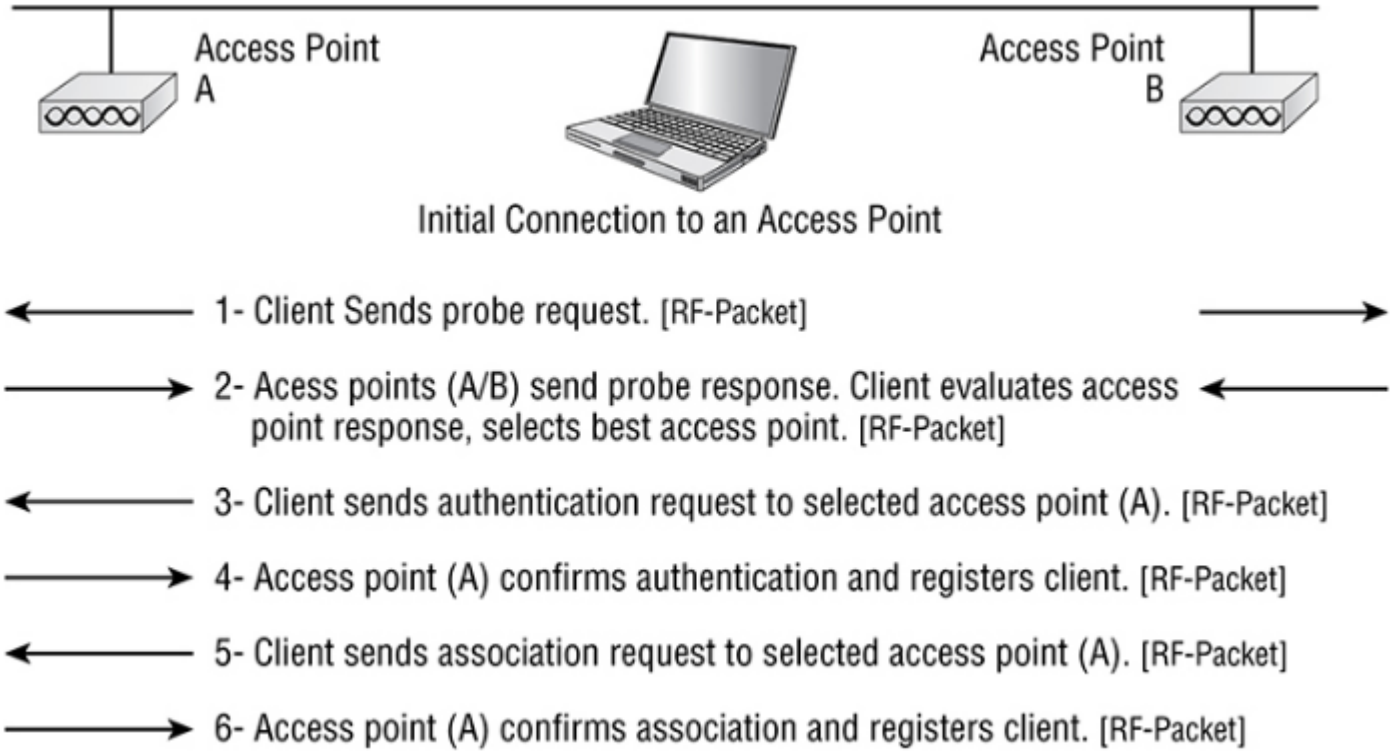
- At the foundational level, authentication uniquely identifies the user and/or machine.

**Encryption**

- The encryption process protects the data or the authentication process by scrambling the information enough that it becomes unreadable by anyone trying to capture the raw frames.

# WEP Shared-Key Authentication

- With shared-key authentication, the access point sends the client device a challenge-text packet that the client must then encrypt with the correct Wired Equivalent Privacy (WEP) key and return to the access point.
- Without the correct key, authentication will fail and the client won't be allowed to associate with the access point.

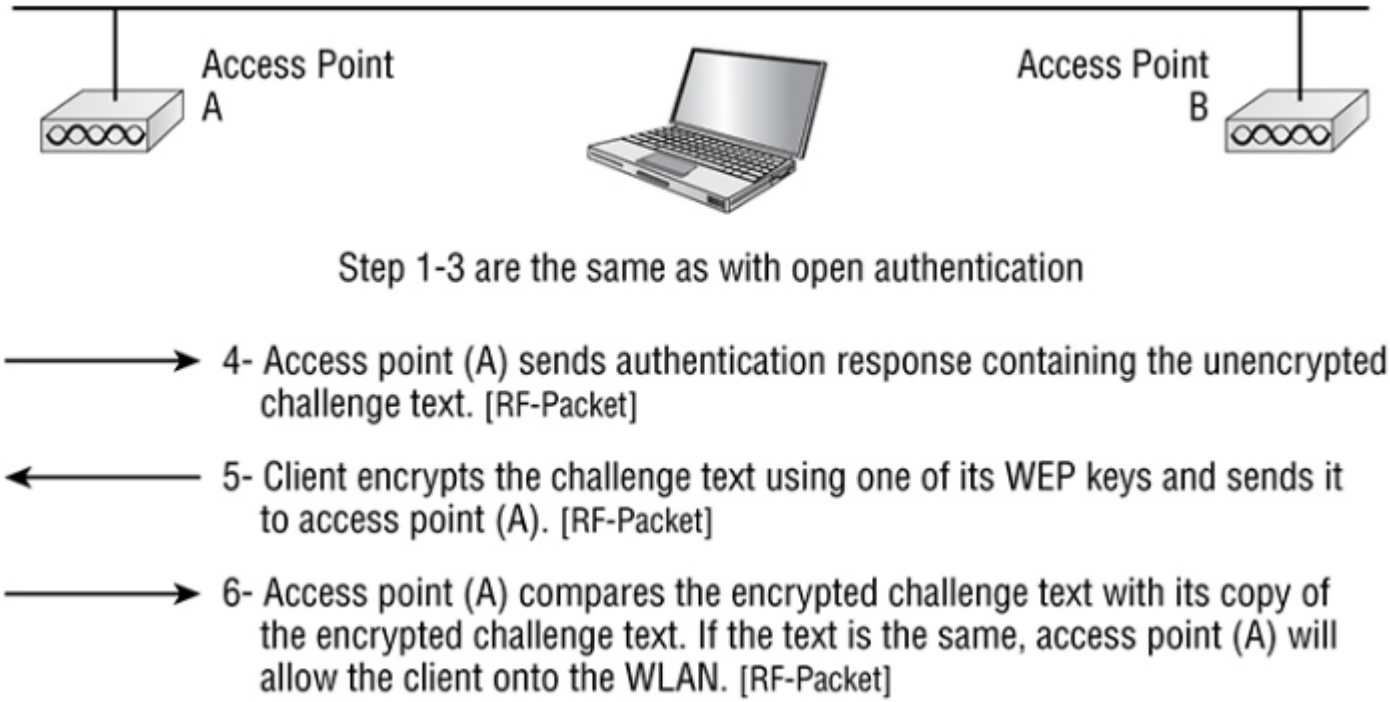


# Shared-Key Downside

- Shared-key authentication is still not considered secure because all a bad guy has to do to get around it is to detect both the clear-text challenge, the same challenge encrypted with a WEP key, and then decipher the WEP key. So it's no surprise that shared key isn't used in today's WLANs.

# Open Access Process

- an authentication request has been sent and "validated" by the AP. But when open authentication is used or set to "none" in the wireless controller, the request is pretty much guaranteed not to be denied.



# WEP Encryption

- With open authentication, even if a client can complete authentication and associate with an access point, the use of WEP prevents the client from sending and receiving data from an access point unless the client has the correct WEP key.

- A WEP key is composed of either 40 or 128 bits, and in its basic form, it's usually statically defined by the network administrator on the access point, and on all clients that communicate with that access point. When static WEP keys are used, a network administrator must perform the tedious task of entering the same keys on every device in the WLAN.

- From a cryptographic point of view using master keys directly is not at all recommended. Master keys should only be used to generate other temporary keys. WEP is seriously flawed in this respect.

# WPA and WPA2

- Wi-Fi Protected Access (WPA) and WPA2 were created in response to the shortcomings of WEP.
- WPA is a standard developed by the Wi-Fi Alliance and provides a standard for authentication and encryption of WLANs that's intended to solve known security problems.
- The benefit of WPA keys over static WEP keys is that the WPA keys can change dynamically while the system is used
- We use WPA2 to help us with today's security issues because we can use AES encryption.
- Pre-Shared Key (PSK) verifies users via a password or identifying code, often called a passphrase, on both the client machine and the access point. A client gains access to the network only if its password matches the access point's password. The PSK also provides keying material that TKIP or AES uses to generate an encryption key for each packet of transmitted data.
- WPA2 uses AES-CCMP for encryption, and WPA uses TKIP.