WiFi Assessment 6 - Module 6

Name	T K Gowtham
Email ID	gowthamkamalasekar@gmail.com
College	VIT Chennai

1. **What are the pillars of Wi-Fi security?**

- The three pillars of WiFi security are :
  - Authentication : Keeps data private and inaccessible to unauthorized users.
  - Integrity : Ensures that the data sent over WiFi isn't tampered with.
  - Availability : Ensures the WiFi network is reliable and accessible to authorized users when needed.

2. **Explain the difference between authentication and encryption in Wi-Fi security.**

Authentication	**Encryption**
Verifies who is trying to access the network	Protects what data is being transmitted.
Main focus is to Check Identity	Main focus is to protect data
Happens when before allowing a device to join the network	Happens after the connection is established.
It's done using Password, username and digital certificate	It's done using algorithms like AES, DES, and Blowfish.
Finally, either access will be granted or denied	Finally, data is encrypted during transmission.

3. **Explain the differences between WEP, WPA, WPA2, and WPA3.**

	WEP	**WPA**	**WPA2**	**WPA3**
Release Year	1999	2003	2004	2018
Encryption Method	RC4	TKIP with RC4	CCMP and AES	AES
Session Key size	40 Bit	128 Bit	128 Bit	128 Bit in Personal 192 Bit in Enterprise
Cipher Text	Stream	Stream	Block	Block
Data Integrity	CRC-32	MIC	CBC-MAC	Secure Hash Algorithm
Key Management	Not provided	4 way handshaking mechanism	4 way handshaking mechanism	Simultaneous Authentication of Equals Handshake
Authentication	WPE-Open WPE-Shared	PSK & 802.1x with EAP variant	PSK & 802.1x with EAP variant	SAE & 802.1x with EAP variant

4. **Why is WEP considered insecure compared to WPA2 or WPA3?**

- Weak Encryption : WEP uses RC4 stream cipher with a small 40 bit key which is easy to crack and attackers can break WEP in minutes.
- Poor Key Management : The same encryption key is used again and again and it is not rotated so hackers can capture packets and analyze repeated patterns to discover the key.
- Weak Integrity Check : WEP uses CRC-32 to check data integrity which doesn’t provide real protection against attackers, as they can modify packets without being detected.
- IV resume and collision : WEP uses a 24 bit Initialization vector (IV) which is too small. IVs repeat allowing attackers to detect and exploit patterns.
- Weak Authentication : WEP uses weak shared key authentication, which can be bypassed by replaying captured packets.

5. **Why was WPA2 introduced?**

- WPA2 was introduced in 2004 to fix the security weakness in WPA and WEP.
- Stronger Encryption : WEP and WPA uses RC4 but WPA2 uses AES with CCMP which is a robust encryption technique.
- Better Data Integrity : WPA2 uses CCMP, which ensures that data isn't tampered with during transmission. It is replaced with Message Integrity Code (MIC) used in WPA, which is vulnerable.
- More secure key management : WPA2 has the 4 way handshake from WPA but it used with stronger encryption reducing the risk of key cracking.
- Mandatory for WiFi certification : From 2006 onwards, the WiFi alliance required all certified devices to support WPA2 and it helped standardize strong security across the WiFi industry.
- Actually, WPA was a temporary fix to address WEP flaws while WPA2 was being finalized and WPA2 is the real long term solution.

6. **What is the role of the Pairwise Master Key (PMK) in the 4-way handshake?**

- PMK plays a central role in securing 4 way handshake in WiFi WPA, WPA2 and WPA3.
- PMK is a secret key shared between the client (device) and the access point (AP).
- It is derived from a pre-shared key(PSK) in WPA/WPA-2 personal or via 802.1x/EAP authentication (in WPA/WPA2/WPA3-Enterprise).
- The 4 way handshake uses the PMK to :
    - ○ Generate Session Key : PMK is used to derive the Pairwise Transient Key (PTK). It is then split into multiple keys like for encryption as TK and for message integrity as MIC key.
    - ○ Mutual Authentication : Ensures that both client and AP prove they know the PMK without sending it over the air and this prevents eavesdroppers from stealing the PMK.
    - ○ Secure Key Exchange : It allows safe generation of fresh encryption keys for each session and it prevents replay attacks and protects against tampering.

7. **How does the 4-way handshake ensure mutual authentication between the client and the access point?**

- The 4 way handshake in WPA/WPA2/WPA3 enures mutual authentication between the client and the AP using cryptographic proof that both sides know the PMK without ever transmitting the PMK itself.
- Message 1 (AP → Client) : AP sends a random nonce (ANonce) to the client. This is just a random number used once to ensure freshness.
- Message 2 (Client → AP) : Client generates its own nonce (SNonce), then we derive PTK = PRF(PMK + ANonce + SNonce + MAC(AA) + MAC(SA)). It sends back the SNonce plus a Message Integrity Code (MIC) calculated with the PTK.

- Message 3 (AP → Client) : AP now has ANonce + received SNonce + PMK and derives the same PTK. AP verifies the MIC sent by the client. If valid, AP sends Group Temporal Key (GTK) encrypted with the PTK with its own MIC.
- Message 4 (Client → AP) : Client decrypts and verifies the GTK and MIC. It sends a final acknowledgment to the AP.
- Process of Mutual Authentication :
  - Client proves knowledge of PMK by sending a correct MIC in message 2.
  - AP proves knowledge of PMK by generating a valid MIC in message 3.
  - If either side doesn;t know the PMK, MIC verification will fail, and the handshake is terminated.
- Finally both parties know the PMK, both verified each other's identity without exposing any keys and they now share a fresh session key (PTK) for secure encrypted communication.

8. What will happen if we put a wrong passphrase during a 4-way handshake?

- The client and AP generates different PMK because PMK is derived from the passphrase + SSID. If the passphrase is wrong, then the client's PMK will not be the same as AP's PMK.
- When the handshake starts the client uses its wrong PMK to compute the PTK and sends a MIC as message 2. Then AP tries to verify the MIC using its own PMK (based on the correct PMK).
- Verification fails, because the MIC is invalid.
- As a result, the AP drops the connection, no data encryption keys (PTK) are successfully agreed upon. Clients may retry a few times, but authentication never succeeds.

9. What problem does 802.1X solve in a network?

- 802.1X solves the problem of unauthorized network access by providing port based network access control (PNAC).
- Without 802.1X, anyone who plugs into a network port or connects to WiFi can access the network, even if they are not supposed to. This is a major security risk in enterprise environments.
- 802.1X ensures that only authenticated users/devices can access the network. It acts like a gatekeeper at the switch port or wireless AP.
- So how it works is like the supplicant (client) your device trying to connect, authenticator (switch or access point) which controls the network port and Authentication server (like RADIUS) which verifies your credentials.
- So, what 802.1X does is
  - Device will connect but the authenticator blocks access.
  - Authenticator will ask for identity.
  - Devices send credentials (e.g., username/password or certificate).
  - Server checks them → if valid, access is granted else denied.
- Key benefits are access control and it supports dynamic VLANs and works with WiFi.

10. How does 802.1X enhance security over wireless networks?

- **Strong Authentication before access :** It uses EAP (extensible authentication protocol) to authenticate users. Users must prove their identity using passwords, certificates or smart cards before they can access the network. It prevents unauthorized users from even getting a DHCP IP address.
- **Dynamic Key Management :** After successful authentication, a unique Pairwise Master Key (PMK) is derived. This key is used in the 4 way handshake to generate fresh encryption keys. This prevents key reuse and protects against sniffing or replay attacks.
- **Device Level Security :** Supports machine authentication (before login) and user authentication (after login). This is useful in enterprise networks with corporate laptops and other IOT devices.
- **Role Based Network access :** It can assign users to specific VLANs based on identity, like for example, employees go to secure VLAN while guests go to internet only VLAN.
- So, 802.1X ensures that only trusted users or devices can connect, data is encrypted uniquely per session and network access is tightly controlled.