MODULE 6

1. What are the pillars of Wi-Fi Security?

   The pillars of Wi-Fi security are the core principles and technologies that ensure confidentiality, integrity, and availability of wireless communication. These pillars protect networks from unauthorized access, eavesdropping, and data tampering. The four main pillars are:

   I. Authentication
      - Purpose: Confirms that only authorized users and devices can access the network.
      - Common methods: Pre-Shared Key (PSK) for home networks, 802.1X with RADIUS for enterprise networks, Open or captive portals for guest access.
      - Protocols: WPA2/WPA3-Personal and WPA2/WPA3-Enterprise.

   II. Encryption
      - Purpose: Protects data from being read by unauthorized parties during transmission.
      - Techniques: AES (Advanced Encryption Standard) – Strong encryption used in WPA2/WPA3, GCMP (Galois/Counter Mode Protocol) – Used in WPA3 for improved speed and security.
      - Benefit: Ensures confidentiality of user data on the network.

   III. Integrity Protection
      - Purpose: Ensures data is not altered or tampered with in transit.
      - Uses Message Integrity Check (MIC) in WPA2/WPA3 to detect forged packets.
      - Prevents man-in-the-middle attacks and packet injection.
      - Protocols: TKIP (older), replaced by AES/CCMP and GCMP in WPA2/WPA3.

   IV. Access Control
      - Purpose: Defines and enforces who can access what on the network.
      - Mechanisms:
         - MAC filtering (basic).
         - VLAN assignment, ACLs, and firewall rules (advanced).
         - Network segmentation for IoT, guest, and employee traffic.

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

   Authentication
   - Purpose: Verifies the identity of the user or device trying to connect to the Wi-Fi network.
   - When It Happens: During the initial connection phase.
   - Ensures only authorized users/devices gain access to the network.
   - Examples: WPA2/WPA3-PSK-Requires a shared password, WPA2/WPA3-Enterprise (802.1X)- Uses usernames/passwords or certificates via a RADIUS server.
   - Outcome: If authentication fails, the device is denied access.

Encryption

- Purpose: Protects the data transmitted over the network from being intercepted or read by unauthorized parties.
- When It Happens: After authentication, once a secure connection is established.
- Converts readable data into an unreadable format using cryptographic algorithms.
- Examples: AES (Advanced Encryption Standard) used in WPA2/WPA3, GCMP for improved performance in WPA3.
- Outcome: Prevents eavesdropping and data theft.

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

Feature	WEP 1997	WPA 2003	WPA2 2004	WPA3 2018
Security level	Weak (easily cracked)	Improved, but still vulnerable	Strong	Very Strong
Encryption Algorithm	RC4 (weak)	TKIP (Temporal Key Integrity Protocol)	AES (Advanced Encryption Standard)	AES-GCMP (stronger than AES-CCMP)
Key Management	Static keys	Dynamic session keys	Dynamic session keys	SAE (Simultaneous Authentication of Equals)
Authentication	Open or shared key	Pre-shared or 802.1X	Pre-shared or 802.1X	SAE (for personal), 192-bit security (enterprise)
Vulnerabilities	Easily hacked	TKIP flaws, dictionary attacks	Vulnerable to KRACK attack (patched)	Resistant to offline and dictionary attacks
Status	Deprecated	Deprecated	Widely used	Emerging Standard

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

Weak Encryption (RC4)

- WEP uses the RC4 stream cipher with a static key, which is vulnerable to key reuse attacks.
- RC4 itself is outdated and prone to statistical analysis.

Short Initialization Vector (IV)

- WEP uses a 24-bit IV, which results in frequent IV collisions.
- This allows attackers to capture enough packets and perform key recovery attacks.

No Strong Key Management

- WEP uses static, manually configured keys (usually shared among users).
- These keys do not change dynamically, making them easy to capture and reuse.

Lack of Integrity Protection

- WEP's Integrity Check Value (ICV) is weak and based on the CRC-32 algorithm.
- It can be manipulated, allowing packet modification without detection

Easily Crackable

- Tools like Aircrack-ng can crack WEP keys in minutes using a few thousand captured packets.

5. Why was WPA2 introduced?

WPA2 (Wi-Fi Protected Access 2) was introduced in 2004 to replace WPA and provide a stronger, more secure standard for wireless communication.
To Strengthen Encryption

- WPA used TKIP (Temporal Key Integrity Protocol), which was only a temporary fix over WEP.
- WPA2 introduced AES (Advanced Encryption Standard) with CCMP (Counter Mode CBC-MAC Protocol), offering robust encryption that meets government-grade security standards.

To Address Vulnerabilities in WEP and WPA

- WEP had critical flaws like static keys and weak IVs.
- WPA still used RC4 cipher (via TKIP), which was vulnerable to several attacks.
- WPA2 eliminated these by mandating AES-based encryption, which is much harder to crack.

To Meet IEEE 802.11i Standard

- WPA2 complies fully with the IEEE 802.11i security amendment, which defines strong authentication, encryption, and integrity protocols for Wi-Fi.

Resistance to Attacks

- WPA2 was designed to prevent key recovery, packet injection, and replay attacks that were possible in WEP and partially in WPA.

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

The Pairwise Master Key (PMK) plays a central role in the 4-way handshake used in WPA/WPA2/WPA3 Wi-Fi security protocols. It is the base key from which encryption keys are derived to securely protect communication between a client (STA) and an access point (AP). The PMK is a pre-shared key (PSK) in personal networks or generated via 802.1X authentication in enterprise networks. It acts as the root key for generating other session keys.

It is used to derive session-specific keys, including: Pairwise Transient Key (PTK) – used to encrypt unicast traffic and Message Integrity Code (MIC) key – for ensuring data integrity.

In the 4-Way Handshake Process:

- PMK is known to both client and AP after authentication (via PSK or 802.1X).
- It is used along with nonces and MAC addresses to derive the PTK.
- The handshake validates both parties know the PMK, preventing spoofing.
- It ensures the session is encrypted, authenticated, and tamper-proof.

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 ensures mutual authentication between the client (station) and the access point (AP) by proving that both parties possess the correct Pairwise Master Key (PMK) without actually transmitting the key. This process also establishes fresh encryption keys for secure communication.

   Step 1: AP → Client

- The Access Point (AP) sends a random number (ANonce) to the client.
- Purpose: Start the handshake with a fresh value.

   Step 2: Client → AP

- The Client creates its own random number (SNonce).
- It uses both nonces (ANonce and SNonce), its MAC address, the AP's MAC address, and the Pairwise Master Key (PMK) to generate a secret key called PTK.
- The client sends:
  - SNonce
  - A Message Integrity Code (MIC) (proves it knows the PMK)

   This lets the AP verify that the client is legitimate.

   Step 3: AP → Client

- The AP also creates the same PTK using the known inputs.
- It checks the MIC from the client.
- Then, the AP sends:
  - Its own MIC (proves it also knows the PMK)
  - The Group Key (GTK) encrypted using the PTK

   This lets the client verify the AP is legitimate.

   Step 4: Client → AP

- The Client confirms it has installed the keys by sending an acknowledgment.

   Result:

- Client authenticates AP.
- AP authenticates client.
- A secure session is now established using the derived PTK.

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

   If a wrong passphrase is used during the 4-way handshake, the process will fail, and the client will not be allowed to connect to the Wi-Fi network.

Client uses wrong passphrase to generate the PMK

- The client derives a Pairwise Master Key (PMK) from the incorrect passphrase.

AP and Client derive different PTKs

- Since the AP has the correct PMK (from the correct passphrase), and the client does not, they each compute different PTKs (session keys).

MIC (Message Integrity Code) fails

- The client sends a MIC (in message 2), but the AP, using a different PTK, cannot verify it.
- Or the AP sends a MIC (in message 3), and the client cannot verify it.

Handshake breaks

- As soon as MIC verification fails, the AP aborts the handshake.

No connection is established

- The client is denied access, and the connection attempt is dropped.
- Some systems may retry a few times before giving up.

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

   802.1X solves the problem of unauthorized access to a network by providing a secure method for network authentication. It ensures that only authenticated users or devices can connect to and use the network resources.

   Problems solved

   - In traditional open or pre-shared key (PSK) networks, anyone with the password can connect.
   - There's no per-user control, no individual authentication, and no identity tracking.
   - Especially in enterprise or campus environments, this can lead to:
     - Unauthorized access
     - Security breaches
     - Lack of user accountability

   Roles:

   - Supplicant: Client device (e.g., laptop)
   - Authenticator: Network switch or wireless access point
   - Authentication Server: Usually a RADIUS server (validates credentials)

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

    - Per-User Authentication: Authenticates each user individually using credentials (e.g., username/password or certificates).
    - Dynamic Key Generation: After successful authentication, unique encryption keys (like PMK) are generated for each session — not shared like in WPA2-PSK.
    - Access Control Before IP Assignment: Devices cannot send/receive network traffic until authenticated — reducing risk of unauthorized access or man-in-the-middle attacks.
    - Integration with RADIUS: Works with RADIUS servers for centralized user management and logging — ideal for enterprises.
    - Supports EAP Methods: Enables secure authentication using various EAP (Extensible Authentication Protocol) types (like EAP-TLS, PEAP, etc.).