Module 6

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

Wi-Fi security relies on three foundational pillars:

- **Authentication:** Ensures that only authorized users and devices can connect to the wireless network. It verifies the identity of the users through credentials such as passwords or digital certificates. In enterprise networks, protocols like 802.1X and EAP (Extensible Authentication Protocol) are used to authenticate users.
- **Encryption:** Protects the confidentiality of data transmitted over the wireless network. It converts readable data into an unreadable format to prevent eavesdropping by unauthorized users. Common encryption standards include WEP (obsolete), WPA, WPA2, and WPA3.
- **Integrity:** Ensures that the data has not been tampered with during transmission. Mechanisms such as Message Integrity Checks (MIC) and the use of cryptographic hashes ensure that data integrity is maintained. This helps prevent man-in-the-middle and replay attacks.

These pillars work together to create a secure wireless environment by preventing unauthorized access, protecting transmitted data, and ensuring the authenticity and integrity of communication.

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

- **Authentication:** This is the process of verifying the identity of a device or user attempting to join a Wi-Fi network. It ensures that only authorized users can access the network. Authentication can be as simple as entering a Wi-Fi password (pre-shared key) or more complex involving 802.1X protocols and RADIUS servers. Once authentication is successful, a session key is often generated for encryption purposes.
- **Encryption:** After successful authentication, encryption ensures that the communication between the device and the access point is secure and unreadable to outsiders. Encryption algorithms scramble the data, making it unintelligible to anyone without the proper decryption key. WPA2 uses AES (Advanced Encryption Standard), while WPA3 uses more advanced encryption mechanisms like Simultaneous Authentication of Equals (SAE).

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

- **WEP (Wired Equivalent Privacy):**
    - Introduced in 1997 as the original Wi-Fi security protocol.
    - Uses RC4 stream cipher and static keys.
    - Vulnerable to several attacks due to poor key management and predictable IVs.

    - Deprecated and considered insecure.
- **WPA (Wi-Fi Protected Access):**
    - Introduced in 2003 as an interim solution to WEP.
    - Uses TKIP (Temporal Key Integrity Protocol) to dynamically change encryption keys.
    - More secure than WEP but still vulnerable to certain attacks.
- **WPA2:**
    - Introduced in 2004 as the official standard.
    - Uses AES for encryption, which is much stronger than TKIP.
    - Introduced CCMP for integrity checking.
    - Widely adopted and still used today.
- **WPA3:**
    - Introduced in 2018.
    - Uses Simultaneous Authentication of Equals (SAE) instead of PSK.
    - Protects against dictionary attacks.
    - Supports forward secrecy.
    - Includes WPA3-Enterprise with 192-bit encryption for enterprise use.

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

WEP is considered insecure due to the following reasons:

- **Weak Encryption:** It uses the RC4 encryption algorithm with static keys and a 24-bit Initialization Vector (IV), which is too short and often reused.
- **Predictable Key Stream:** Attackers can collect enough IVs to determine the encryption key through statistical analysis.
- **No Key Management:** Keys are manually entered and not rotated or changed, making them susceptible to long-term compromise.
- **Lack of Integrity Checking:** WEP uses a weak checksum method that does not adequately prevent tampering.

Compared to WPA2 and WPA3, which use robust encryption (AES) and dynamic key management, WEP offers little to no real protection and is easily cracked using tools available to the public.

5. Why was WPA2 introduced?

WPA2 was introduced to address the vulnerabilities in WPA and to bring Wi-Fi security in line with modern encryption standards. Key reasons include:

- **Stronger Encryption:** WPA2 uses AES (Advanced Encryption Standard), which is a more secure and efficient encryption algorithm than TKIP used in WPA.
- **Improved Integrity:** It introduces CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for message integrity.
- **Compliance with IEEE 802.11i:** WPA2 fully implements the security enhancements defined in the 802.11i standard.
- **Scalability and Enterprise Support:** WPA2 includes features suitable for enterprise environments, such as support for 802.1X and RADIUS servers.

These improvements made WPA2 the gold standard in Wi-Fi security for over a decade.

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

The Pairwise Master Key (PMK) is a fundamental component in the 4-way handshake process. It is derived from the pre-shared key (in WPA/WPA2-Personal) or obtained through an authentication server (in WPA/WPA2-Enterprise).

Role of PMK:

- It serves as the root key for generating the Pairwise Transient Key (PTK).
- Both the access point and the client derive the same PTK independently using the PMK, nonces, and MAC addresses.
- The PTK is used to encrypt and validate unicast communication.

The PMK ensures that only authenticated devices with the correct credentials can generate valid session keys, making it crucial for secure communication.

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

The 4-way handshake confirms that both the access point (AP) and the client possess the same Pairwise Master Key (PMK) without transmitting it over the air. Here is how mutual authentication occurs:

1. **Message 1:** AP sends a random number (ANonce) to the client.
2. **Message 2:** Client uses PMK, ANonce, SNonce (client-generated random number), and both MAC addresses to derive the PTK. It then sends the SNonce to the AP.
3. **Message 3:** AP uses the same inputs to derive the PTK and confirms that both sides match. It sends the Group Temporal Key (GTK) encrypted with the PTK to the client.
4. **Message 4:** Client installs the keys and sends an acknowledgment.

If any step fails (due to incorrect keys or tampering), the handshake will not complete. This ensures both parties have a valid PMK and thus authenticates each other.

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

If a wrong passphrase is entered:

- The client and AP will derive different Pairwise Master Keys (PMKs).
- This results in mismatched Pairwise Transient Keys (PTKs).
- The cryptographic checks during the handshake (such as MIC validation) will fail.
- Consequently, the 4-way handshake will not complete, and the client will not be allowed to connect to the network.

This mechanism protects the network from unauthorized access even if an incorrect but valid-looking passphrase is entered.

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

802.1X addresses the need for **port-based network access control** in both wired and wireless networks. It solves several key problems:

- **Unauthorized Access:** Ensures that only authenticated users or devices can gain network access.
- **Credential Validation:** Integrates with backend authentication systems (e.g., RADIUS) for validating user credentials.
- **Dynamic Key Management:** Supports per-user, per-session key generation for secure communication.
- **Scalability:** Ideal for large enterprise networks with centralized authentication.

By using 802.1X, organizations can enforce security policies at the network edge and prevent rogue devices from joining the network.

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

802.1X significantly strengthens Wi-Fi security in the following ways:

- **Mutual Authentication:** Verifies both the client and the authentication server before granting access.
- **Per-Session Encryption Keys:** Generates unique keys for each session, preventing key reuse and replay attacks.
- **Centralized Access Control:** Uses RADIUS or similar servers for managing user credentials and policies.

- **Reduced Risk of Credential Theft:** Supports secure EAP methods (e.g., EAP-TLS) that use certificates instead of passwords.

This framework makes wireless networks more secure by ensuring only legitimate users gain access, and by protecting data with dynamic encryption.