Wi-Fi Training Program
Assignment Questions -Module 6

Q1: What are the pillars of Wi-Fi security?

Wi-Fi security is fundamentally built upon four key pillars that ensure the safe and reliable operation of wireless networks:

1. **Confidentiality**: This involves the protection of transmitted data from unauthorized access or eavesdropping through encryption techniques. It ensures that sensitive information remains private during wireless communication.
2. **Integrity**: Integrity ensures that the data sent over the network has not been altered or tampered with during transmission. This is achieved through cryptographic hash functions and message integrity codes.
3. **Authentication**: Authentication verifies the identity of devices or users attempting to access the wireless network. It prevents unauthorized access and supports trust between network entities through mechanisms such as passwords, digital certificates, or centralized authentication servers (e.g., RADIUS).
4. **Access Control**: This pillar involves defining and enforcing policies that restrict access to network resources based on user roles, device type, or other criteria. It ensures that only authorized users and devices can utilize the network.

Q2: Explain the difference between authentication and encryption in Wi-Fi security.

In the context of Wi-Fi security, **authentication** and **encryption** serve distinct but complementary roles:

- **Authentication** is the process of verifying the identity of a device or user attempting to connect to a wireless network. It ensures that only authorized entities are granted access. This can be achieved through pre-shared keys (PSK), digital certificates, or enterprise-level solutions like IEEE 802.1X with a RADIUS server. Authentication forms the basis for establishing trust between the client and the access point.
- **Encryption**, on the other hand, is the process of converting data into a secure format that is unreadable to unauthorized parties. It protects the confidentiality of the information transmitted over the wireless medium by preventing eavesdropping and unauthorized data access. Common encryption protocols include TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard).

Q3: Explain the differences between WEP, WPA, WPA2, and WPA3.

1. **WEP (Wired Equivalent Privacy)**:
   - Introduced as part of the original IEEE 802.11 standard.
   - Uses the RC4 stream cipher and a static encryption key.
   - Vulnerable to numerous cryptographic attacks due to weak initialization vector (IV) management and key reuse.
   - Now considered obsolete and insecure.
2. **WPA (Wi-Fi Protected Access)**:
   - Introduced as an interim solution to replace WEP.
   - Implements TKIP (Temporal Key Integrity Protocol), which dynamically changes encryption keys.
   - Improves security over WEP but still relies on the RC4 cipher, making it susceptible to certain attacks.
   - Also considered outdated for modern networks.
3. **WPA2**:
   - Based on the IEEE 802.11i standard and introduced AES (Advanced Encryption Standard) with CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol).
   - Provides strong encryption and integrity protection.
   - Includes support for 802.1X authentication (Enterprise mode) and Pre-Shared Key (PSK) for personal networks.
   - Remains widely used and secure when properly configured.
4. **WPA3**:
   - The most recent and robust Wi-Fi security protocol.
   - Replaces PSK with SAE (Simultaneous Authentication of Equals) for more secure key establishment and protection against offline dictionary attacks.
   - Provides forward secrecy, ensuring that session keys cannot be derived even if long-term credentials are compromised.
   - Offers enhanced protection for public and open networks through Opportunistic Wireless Encryption (OWE).
   - Mandatory use of 192-bit encryption in WPA3-Enterprise mode.

Q4: Why is WEP considered insecure compared to WPA2 or WPA3?

Wired Equivalent Privacy (WEP) is considered highly insecure for several reasons:

- **Weak Encryption**: WEP uses the RC4 stream cipher with a 40-bit or 104-bit key and a 24-bit Initialization Vector (IV). The limited size of the IV leads to frequent key reuse, making it easier for attackers to detect patterns and crack the encryption.
- **IV Vulnerabilities**: The IVs in WEP are transmitted in plaintext and are prone to collisions. This design flaw allows attackers to collect enough packets to analyze and deduce the encryption key.
- **Lack of Strong Key Management**: WEP relies on static, manually configured keys that rarely change. This static nature makes it easier for an attacker to capture enough data and break the key over time.
- **Absence of Robust Authentication**: WEP does not provide strong mutual authentication between the client and the access point, making it susceptible to impersonation and spoofing attacks.

Q5: Why was WPA2 introduced?

WPA2 (Wi-Fi Protected Access 2) was introduced to address the security deficiencies found in earlier Wi-Fi protection protocols, particularly WEP and WPA. Its primary purposes were:

- **Compliance with IEEE 802.11i Standard**: WPA2 fully implements the security specifications outlined in the IEEE 802.11i standard, offering a more formal and comprehensive approach to wireless security.
- **Stronger Encryption**: Unlike WPA, which used the temporary TKIP protocol as a stopgap, WPA2 introduced the use of AES (Advanced Encryption Standard) with CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) to provide robust confidentiality, integrity, and authentication protections.
- **Enhanced Network Authentication**: WPA2 supports both Personal mode (using a Pre-Shared Key, PSK) for home networks and Enterprise mode (using 802.1X authentication and RADIUS servers) for corporate environments, enabling secure user and device validation.
- **Improved Data Integrity and Key Management**: WPA2 significantly enhances data integrity through stronger cryptographic techniques and dynamic session key generation, preventing many attacks that exploited static or weak keys.

Q6: 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 Wi-Fi 4-Way Handshake process by serving as the foundational key material from which further encryption keys are derived. Specifically:

- The PMK is a long-term secret shared between the client (supplicant) and the access point (authenticator). It is either generated from a pre-shared key (PSK) in personal networks or obtained from an authentication server (such as RADIUS) in enterprise networks.
- During the 4-Way Handshake, both the client and the access point use the PMK, along with nonces (random numbers) and MAC addresses, to derive a **Pairwise Transient Key (PTK)**. The PTK is then used to encrypt unicast traffic between the client and the access point.
- The PMK itself is **never transmitted over the air**. Instead, it remains securely stored and is used internally to verify that both parties possess the same key, thereby ensuring mutual authentication.
- Through this process, the PMK ensures **confidentiality, integrity, and authenticity** of the communication without exposing sensitive key material.

Q7: How does the 4-Way Handshake ensure mutual authentication between the client and the access point?

The **4-Way Handshake** ensures **mutual authentication** between the client (supplicant) and the access point (authenticator) by using a secure challenge-response mechanism based on the Pairwise Master Key (PMK). The process works as follows:

- Both the client and the access point independently derive the **Pairwise Transient Key (PTK)** using the PMK, nonces (random numbers generated by both sides), and their respective MAC addresses.
- The access point initiates the handshake by sending a nonce (ANonce) to the client. The client responds with its own nonce (SNonce) and a Message Integrity Code (MIC) calculated using the PTK.
- Each party verifies that the other has correctly derived the PTK by validating the MIC attached to the handshake messages. Since deriving the PTK correctly depends on having the same PMK, a correct MIC confirms possession of the PMK.
- If either side detects that the MIC does not match, the handshake fails, preventing network access.

Q8: What will happen if we put a wrong passphrase during a 4-Way Handshake?

If an incorrect passphrase is used during the 4-Way Handshake process, the authentication will fail. This happens because:

- The wrong passphrase leads to the derivation of an incorrect **Pairwise Master Key (PMK)** on the client side.
- As a result, the **Pairwise Transient Key (PTK)** generated from the PMK and the exchanged nonces will also be incorrect.
- During the handshake, when the client sends a message protected with a **Message Integrity Code (MIC)** based on the wrong PTK, the access point will not be able to validate it successfully.
- The mismatch in MIC validation signals that the client does not possess the correct cryptographic credentials, causing the access point to terminate the handshake and deny network access.

Q9: What problem does 802.1X solve in a network?

802.1X is a network access control protocol that addresses the problem of securing network access by enforcing authentication before granting devices access to a network. It is commonly used in Ethernet and Wi-Fi networks.

The main problem it solves is ensuring that only authorized devices or users can connect to the network, preventing unauthorized access and potential security breaches. This is achieved through a process of:

1. **Authentication**: Before a device is allowed to join the network, it must provide credentials (e.g., username, password, or certificates) that are validated by a central authentication server (usually RADIUS).
2. **Authorization**: Once authenticated, the device is authorized with specific network privileges based on its identity, ensuring it can only access appropriate resources.
3. **Dynamic VLAN Assignment**: Depending on the outcome of the authentication, 802.1X can assign devices to specific VLANs or networks, ensuring that devices only have access to the parts of the network they are permitted to.

Q10: How does 802.1X enhance security over wireless networks?

802.1X significantly enhances security in wireless networks by providing robust authentication and access control mechanisms. Here's how it strengthens security:

1. **Prevents Unauthorized Access**:
    - **Authentication before Access**: With 802.1X, devices must authenticate before they can join the network. This ensures that only authorized devices, typically identified by credentials like usernames, passwords, or digital certificates, are allowed to connect.
2. **Mutual Authentication**:
    - **Server and Client Authentication**: 802.1X allows both the client (device) and the server (typically a RADIUS server) to authenticate each other. This mutual authentication ensures that the client is connecting to a legitimate network and that the network can trust the device.
3. **Dynamic Encryption Key Generation**:
    - **Stronger Encryption**: Once authenticated, 802.1X supports the negotiation of encryption keys (like WPA2-Enterprise or WPA3-Enterprise). This means that each device gets a unique session key, providing stronger encryption and protecting against eavesdropping and man-in-the-middle attacks.
4. **No Open Authentication**:
    - **No Open Networks**: Unlike open Wi-Fi networks, where anyone can join without credentials, 802.1X requires a valid authentication exchange. This eliminates the risk of unauthorized users simply connecting to the network.
5. **Role-Based Access Control**:
    - **Granular Control**: Depending on the result of the authentication, 802.1X can assign the user or device to a specific VLAN or segment of the network. This enables policies that limit access to sensitive resources or restrict network privileges based on user roles or device types.
6. **Improved Protection against Rogue Devices**:
    - **Port-Based Access Control**: With 802.1X, if a rogue device tries to connect to a wired or wireless port, it is denied access until it successfully authenticates. This helps in preventing unauthorized devices from connecting and potentially attacking the network.