WiFi Training Program

Module 6 assignment

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

The three primary pillars of Wi-Fi security are:

- Authentication: Verifying the identity of devices attempting to connect to the network, ensuring that only authorized users are granted access.
- Encryption: Protecting data in transit by converting it into a coded format, making it unreadable to unauthorized parties.
- Integrity: Ensuring that data is not tampered with during transmission, providing assurances that the data received is exactly what was sent.

2. Explain the difference between authentication and encryption in WiFi security.

- Authentication is the process of verifying the identity of a device or user attempting to access a Wi-Fi network. It ensures that only legitimate users are granted access.
- Encryption, on the other hand, protects the confidentiality of data being transmitted across the network by encoding it, ensuring that even if the data is intercepted, it cannot be read without the decryption key.
- In essence, authentication controls who can access the network, while encryption protects what is being transmitted.

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

- WEP (Wired Equivalent Privacy): Introduced in 1997, WEP used RC4 encryption but had major security flaws, including weak key management, making it vulnerable to attacks.
- WPA (Wi-Fi Protected Access): Introduced as a temporary solution to replace WEP, WPA improved security by introducing TKIP (Temporal Key Integrity Protocol) but still had vulnerabilities.

- WPA2: Standardized in 2004, WPA2 introduced stronger AES (Advanced Encryption Standard) encryption and the CCMP protocol, offering much better security and robustness.
- WPA3: Released in 2018, WPA3 strengthens security further with individualized data encryption, forward secrecy, and more secure handshake protocols (such as SAE – Simultaneous Authentication of Equals), protecting networks even against offline dictionary attacks.

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

WEP is considered insecure because:

- It uses static encryption keys that are reused, making them susceptible to interception and decryption.
- The RC4 encryption algorithm used in WEP is weak and vulnerable to known attacks.
- Initialization Vectors (IVs) are short (24 bits) and predictable, leading to key reuse vulnerabilities.
- Modern attack tools can crack WEP keys within minutes, making it unsuitable for secure communications compared to WPA2's AES encryption and WPA3's advanced authentication protocols.

5. Why was WPA2 introduced?

WPA2 was introduced to:

- Replace the interim WPA standard with a permanent, stronger security protocol.
- Address the shortcomings of WPA by implementing mandatory support for AES encryption and CCMP for data confidentiality and integrity.
- Comply with IEEE 802.11i standard specifications for robust wireless security.
- Provide an enterprise-level security option with 802.1X authentication and improved encryption mechanisms.

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

The Pairwise Master Key (PMK) serves as the foundation for deriving encryption keys during the 4-way handshake process:

- It is generated during the authentication phase (either by a Pre-Shared Key (PSK) or through 802.1X authentication).
- The PMK is used by both the client (supplicant) and the access point (authenticator) to derive the Pairwise Transient Key (PTK), ensuring that encryption keys are securely created and are known only to the authenticated parties.
- Thus, it plays a critical role in establishing a secure communication session.

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

The 4-way handshake ensures mutual authentication by:

- Using a challenge-response mechanism where both the client and access point prove they possess the same PMK without transmitting it.
- Generating and exchanging nonces (random numbers) and deriving session keys (PTK) independently.
- Verifying that both sides have calculated the same keys by exchanging message authentication codes (MICs).
- This mutual proof process confirms that both parties are legitimate and share the correct credentials.

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

If the passphrase is incorrect:

- The derived Pairwise Master Key (PMK) will not match between the client and the access point.

- As a result, the calculated message authentication codes (MICs) during the handshake will differ.
- The access point will detect the mismatch and reject the connection attempt.
- The client will also fail to establish a secured session, and reauthentication would be required.

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

802.1X solves the problem of unauthorized access to a network by:

- Enabling port-based network access control (PNAC).
- Requiring devices to authenticate themselves before gaining network access.
- Supporting dynamic key management and integration with centralized authentication servers (such as RADIUS).
- Thus, it enhances security, particularly in enterprise environments, by preventing rogue devices from connecting without proper credentials.

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

802.1X enhances wireless network security by:

- Providing strong authentication mechanisms through support for multiple EAP (Extensible Authentication Protocol) types.
- Ensuring that users or devices are authenticated before being granted any network access.
- Allowing for dynamic generation and distribution of encryption keys, which are unique per session, thereby reducing the risk of key reuse attacks.
- Integrating with centralized authentication systems (e.g., RADIUS servers), enabling detailed access control policies and accounting.