WIFI TRANING MODULE 6 ASSESSMENT SOLUTION

-BY SAKTHI KUMAR S

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

The pillars of Wi-Fi security are essential components that ensure secure and reliable wireless communication. The main pillars include:

1. Authentication
   Ensures that only authorized users and devices can access the Wi-Fi network. Examples include:
   - Pre-Shared Key (PSK) for personal networks (WPA2/WPA3-Personal)
   - 802.1X with EAP (Extensible Authentication Protocol) for enterprise networks (WPA2/WPA3-Enterprise)
2. Encryption
   Protects the confidentiality of data transmitted over the network. It scrambles data to make it unreadable to unauthorized parties. Common encryption methods:
   - AES (Advanced Encryption Standard) in WPA2/WPA3
   - GCMP (Galois/Counter Mode Protocol) in WPA3
3. Integrity
   Ensures that the transmitted data has not been tampered with during transmission. It detects and prevents data modification attacks using:
   - Message Integrity Check (MIC)
   - CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)
4. Key Management
   Ensures secure generation, exchange, and renewal of encryption keys. Includes processes such as:
   - 4-Way Handshake (WPA2)
   - Simultaneous Authentication of Equals (SAE) in WPA3

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

1. Authentication
    - Purpose: Verifies the identity of the user or device trying to access the network.
    - When it happens: Before the user is allowed to connect to the Wi-Fi network.
        1. WPA2-PSK (uses a shared password)
        2. WPA2/WPA3-Enterprise (uses 802.1X with EAP methods and RADIUS servers)
2. Encryption
    - Purpose: Protects the data transmitted over the air by making it unreadable to unauthorized parties.
    - When it happens: After a successful authentication, when data is being transmitted between devices and access points.
        1. AES (used in WPA2/WPA3)
        2. GCMP (used in WPA3 for better performance and security)

Feature	Authentication	Encryption
Purpose	Verifies the identity of the user or device	Protects data from being read by unauthorized parties
When It Occurs	Before establishing a secure connection	After authentication, during data transmission
What It Protects	Network access	Data confidentiality and privacy
Key Examples	WPA2-PSK, WPA3-SAE, 802.1X with EAP methods	AES (WPA2/WPA3), TKIP (WPA), GCMP (WPA3)
Mechanism	Identity verification using passwords, certificates, or EAP methods	Mathematical algorithms to scramble and unscramble data
Used In	WiFi login and access control	Wireless data transmission security
Technology Used	PSK, EAP, RADIUS, SAE	AES, TKIP, CCMP, GCMP

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

Feature	WEP	WPA	WPA2	WPA3
Full Form	Wired Equivalent Privacy	Wi-Fi Protected Access	Wi-Fi Protected Access 2	Wi-Fi Protected Access 3
Encryption	RC4 (weak & outdated)	TKIP (Temporal Key Integrity Protocol)	AES (Advanced Encryption Standard)	AES-GCMP (Galois Counter Mode Protocol)
Key Management	Static keys	Dynamic keys (via TKIP)	4-Way Handshake with AES	SAE (Simultaneous Authentication of Equals)
Vulnerability	Easily cracked in minutes	Improved but still weak (TKIP)	Stronger encryption, secure for most use	Strongest security, resistant to offline attacks
Security Status	Obsolete/Insecure	Deprecated	Secure (widely used)	Most secure (recommended for new networks)
Compatibility	Legacy devices only	Transitional (no longer used)	Broad device support	Modern devices (2018 onward)

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

WEP (Wired Equivalent Privacy) is considered insecure due to several critical weaknesses:

1. Weak Encryption Algorithm (RC4)
   WEP uses RC4, which has known vulnerabilities. The initialization vector (IV) used in WEP is only 24 bits long, leading to IV reuse a major flaw that allows attackers to collect enough packets to crack the key easily.
2. Static Key Usage
   WEP relies on a single static key that doesn't change unless manually updated. This makes it easier for attackers to perform key recovery attacks.
3. No Robust Key Management
   WEP lacks proper mechanisms for key exchange or renewal, unlike the 4-way handshake in WPA2 or SAE in WPA3, which provide dynamic and secure key management.
4. Susceptibility to Packet Injection and Replay Attacks
   Due to weak data integrity mechanisms, WEP is vulnerable to attackers injecting malicious packets or replaying captured ones.
5. Cracked in Minutes with Readily Available Tools
   Tools like Air crack-ng can crack WEP in a few minutes using packet sniffing and dictionary attacks, making it completely unsuitable for any secure communication today.

5. Why was WPA2 introduced?

WPA2 was introduced in 2004 as an upgrade to WPA to address the growing need for stronger wireless security. The key reasons for introducing WPA2 include:

1. Replacement of TKIP with AES:
   WPA used TKIP, which had limitations and vulnerabilities. WPA2 introduced AES-based encryption through CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), which is far more secure and compliant with modern cryptographic standards.
2. Stronger Data Integrity and Confidentiality:
   WPA2 provides robust data protection and integrity checks, making it more resilient against replay attacks and tampering.
3. Mandatory Support for Enterprise Authentication:
   WPA2 formalized support for 802.1X-based authentication (used in WPA2-Enterprise), enabling the use of RADIUS servers and EAP methods for enterprise-grade security.
4. Wi-Fi Alliance Compliance:
   WPA2 became a mandatory certification for Wi-Fi devices by the Wi-Fi Alliance, ensuring a baseline of security across vendors and devices.

In short: WPA2 was introduced to overcome the security weaknesses of WPA and WEP, and to align with modern encryption standards like AES for better wireless protection.

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 security protocols. Here's how it fits in:

Role of PMK:

1. For Deriving Session Keys:
   The PMK is used to derive a Pairwise Transient Key (PTK), which is then split into:
   - Encryption keys (to encrypt user data)
   - Message Integrity Code (MIC) keys (to ensure message authenticity)
2. Ensures Secure Key Exchange Without Transmitting Keys Over the Air:
   During the 4-way handshake, both the client (STA) and the access point (AP) independently generate the same PTK using the shared PMK, without ever sending it across the air, ensuring secrecy.
3. Depends on Authentication Type:
   - In WPA/WPA2-Personal, the PMK is derived from the Pre-Shared Key (PSK).
   - In WPA2-Enterprise, the PMK is generated during 802.1X/EAP authentication.
4. Protects Against Replay and Spoofing Attacks:
   It ensures that only legitimate clients that possess the correct PMK (from a valid PSK or EAP exchange) can derive the correct session keys.

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

The 4-way handshake ensures mutual authentication through a secure key exchange process based on the Pairwise Master Key (PMK).

Process flow:

1. Both the Client (STA) and Access Point (AP) start with the same PMK, derived from a pre-shared key (PSK) or from an 802.1X/EAP authentication exchange.
2. The AP sends a random nonce (ANonce) to the client.
3. The client generates its own nonce (SNonce) and computes the Pairwise Transient Key (PTK) using:
    - PMK
    - ANonce
    - SNonce
    - MAC addresses of both client and AP
4. The client sends the SNonce and a Message Integrity Code (MIC) to the AP.
5. The AP uses the same parameters to derive the PTK and checks the MIC.
6. If valid, the AP sends a confirmation message with its own MIC.

Mutual Authentication Ensured Because:

- Both parties must possess the correct PMK to derive the same PTK and correctly generate/verify the MICs.
- If either side has the wrong PMK (e.g., wrong password), MIC verification fails, and the handshake is terminated.

So, even though the 4-way handshake doesn't directly send credentials, it proves possession of the correct PMK, ensuring both sides are legitimate.

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

If a wrong passphrase is entered:

1. The client derives an incorrect PMK from the wrong passphrase.
2. It uses that PMK to compute the PTK and generate a MIC for Message 2 of the 4-way handshake.
3. The access point, having the correct PMK, derives its own PTK and attempts to verify the MIC from the client.
4. MIC mismatch occurs because the keys are different.
5. The AP terminates the handshake, and the client fails to connect to the Wi-Fi network.

Result:

- Incorrect PMK Derivation.
- Handshake Termination.
- MIC Failure
- Authentication fails
- No IP address is assigned
- Client sees a “Wrong Password” or “Cannot Connect” error

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

802.1X solves the problem of unauthorized access to a network by providing port-based network access control. It ensures that only authenticated users/devices can access the network, whether it's wired or wireless.

Problems Solved by 802.1X:

1. Unauthorized Access Prevention:
   It ensures that users must be authenticated before gaining access to any network resources.
2. Dynamic Access Control:
   Access can be granted, denied, or restricted based on user credentials, time, location, or security policies.
3. Centralized Authentication:
   Uses a RADIUS server for centralized user authentication, accounting, and authorization (AAA).
4. No Shared Passwords (unlike WPA-PSK):
   Credentials are managed per-user, making it scalable and secure for large enterprise networks.

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

802.1X enhances wireless security by integrating with WPA2-Enterprise or WPA3-Enterprise, creating a robust authentication framework that verifies users before allowing any access to the network.

Key Security Enhancements by 802.1X:

1. User-Based Authentication with EAP:
   Uses EAP (Extensible Authentication Protocol) to support multiple secure authentication methods (e.g., EAP-TLS, PEAP, EAP-TTLS).
2. Per-Session Unique Keys:
   After successful authentication, the RADIUS server and client derive a unique Pairwise Master Key (PMK), ensuring encrypted and isolated sessions per user.
3. Protection Against Credential Theft:
   When using methods like EAP-TLS, credentials are never sent in plaintext. Certificates are used instead of passwords, preventing interception or phishing.
4. Dynamic VLAN Assignment:
   Based on user role or profile, 802.1X can place users into different VLANs, enhancing network segmentation and access control.
5. Scalability and Centralized Management:
   Perfect for large organizations, universities, and enterprises that require user-level accountability and audit logs.
6. 802.1X solves the problem of network access by ensuring users are authenticated before they connect.
7. 802.1X enhances wireless security by enabling strong, per-user authentication and encryption, far more secure than pre-shared keys.