Name: Afreen S

University: Vellore Institute of Technology (VIT)

WiFi Training Program

Assignment – Module 6

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

Wi-Fi security is built on **four main pillars** that ensure safe and reliable wireless communication:

1. Authentication

- Verifies that users or devices are **authorized** to connect to the network.
- Common methods:
  - **Pre-shared Key (PSK)** – used in WPA2/WPA3-Personal
  - **802.1X with EAP** – used in WPA2/WPA3-Enterprise

2. Encryption

- Ensures that transmitted data is **confidential and unreadable** to unauthorized users.
- Protocols used:
  - **WPA2** – uses AES (CCMP)
  - **WPA3** – uses stronger encryption with **SAE (Simultaneous Authentication of Equals)**

3. Integrity Protection

- Protects data from being **altered or tampered with** during transmission.
- Uses **Message Integrity Check (MIC)** in WPA2/WPA3 to detect forged packets.

4. Access Control

- Controls **who can connect** and what **resources** they can access.
- Can involve:
  - MAC address filtering
  - VLAN tagging
  - Role-based access policies

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

Authentication

- **Purpose**: Confirms **who** is allowed to access the Wi-Fi network.
- **What it does**: Verifies the identity of the device or user (e.g., using a password or certificate).
- **Example**: When you enter a Wi-Fi password to connect to a secured network, that's authentication.
- **Protocols**: WPA2-PSK, WPA3, 802.1X (enterprise networks).

Encryption

- **Purpose**: Protects the **data** sent over the Wi-Fi from being read by others.
- **What it does**: Scrambles the information so only the intended receiver can understand it.
- **Example**: Even if someone intercepts your data on a public network, encryption prevents them from understanding it.
- **Algorithms**: AES (used in WPA2/WPA3), TKIP (used in older WPA).

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

Feature	**WEP (1997)**	**WPA (2003)**	**WPA2 (2004)**	**WPA3 (2018)**
Full Form	Wired Equivalent Privacy	Wi-Fi Protected Access	Wi-Fi Protected Access 2	Wi-Fi Protected Access 3
Encryption	RC4 (weak)	TKIP (RC4-based, better than WEP)	AES-CCMP (strong)	AES-GCMP (stronger)
Key Management	Static key	Temporal keys (per session)	Dynamic key (4-way handshake)	SAE (Simultaneous Authentication of Equals)
Security Level	Very Weak	Improved, but still weak	Strong	Very Strong
Vulnerabilities	Easily crackable	Susceptible to certain attacks	Vulnerable to KRACK (patched)	Resistant to offline dictionary attacks
Enterprise Support	No	Basic	Yes (802.1X)	Yes (802.1X + modern encryption)
Device Support	Legacy only	Older devices	Most modern devices	Newest devices (2019+)

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

Weaknesses of WEP (Wired Equivalent Privacy):

1. **Weak Encryption Algorithm:**
    - Uses **RC4** with short (40 or 104-bit) keys and a 24-bit IV (Initialization Vector), which is too small.
    - IVs **repeat frequently**, making it easy to crack the encryption.
2. **No Key Management:**
    - WEP uses a **static key** shared across all devices.
    - Once known, an attacker can **decrypt all traffic**.
3. **Vulnerable to Attacks:**
    - Tools like **Aircrack-ng** can break WEP in minutes using packet sniffing and replay attacks.
4. **Lacks Integrity Protection:**
    - Weak **CRC-32** check allows attackers to **alter packets** without detection.

WPA2/WPA3 Are Better:

Feature	**WEP**	**WPA2**	**WPA3**
Encryption	RC4 (weak)	AES-CCMP (strong)	AES-GCMP (stronger)
Key Management	Static key	Dynamic key (4-way handshake)	SAE (secure key exchange)
Integrity Check	CRC-32 (weak)	MIC (Message Integrity Code)	Enhanced MIC

5. Why was WPA2 introduced?

WPA2 (Wi-Fi Protected Access 2) was introduced by the Wi-Fi Alliance in 2004 to replace WPA and fully address the major security flaws of WEP.

Reasons for WPA2 Introduction:

1. **Stronger Encryption:**
    - **Replaced WEP's weak RC4 algorithm with AES-CCMP, providing robust data protection.**
2. **Improved Security Protocol:**
    - **WPA2 implements the full IEEE 802.11i standard, including better authentication, encryption, and integrity checking.**

3. **Resistance to Attacks:**
    - **WPA2 was designed to prevent key recovery, packet injection, and replay attacks that were possible in WEP and partially in WPA.**
4. **Mandatory for Certification:**
    - **Since 2006, all Wi-Fi certified devices must support WPA2, ensuring a universal security baseline.**

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

Role of PMK:

- The **PMK is a shared secret** between the client (STA) and access point (AP), generated during authentication.
- It is used to **derive session-specific keys**, including:
    - **Pairwise Transient Key (PTK)** – used to encrypt unicast traffic.
    - **Message Integrity Code (MIC) key** – for ensuring data integrity.

In the 4-Way Handshake Process:

1. **PMK is known** to both client and AP after authentication (via PSK or 802.1X).
2. It is used along with nonces and MAC addresses to derive the **PTK**.
3. The handshake validates both parties **know the PMK**, preventing spoofing.
4. 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** by proving that **both the client and the access point (AP) possess the same Pairwise Master Key (PMK)** without ever sending it over the air.

Steps Enabling Mutual Authentication:

1. **AP sends ANonce** (a random number) to the client.
2. **Client uses ANonce + PMK** to derive the **Pairwise Transient Key (PTK)**, then sends its **SNonce** (client's nonce) and a **Message Integrity Code (MIC)** back to the AP.
3. **AP also derives PTK** using PMK + SNonce + ANonce and verifies the MIC.
    - If correct → AP confirms **client has the correct PMK**.
4. Then, the AP sends its own MIC (encrypted), which the client verifies.
    - If correct → client confirms **AP has the correct PMK**.

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 the **wrong passphrase** is used during the **4-way handshake**, the **Pairwise Master Key (PMK)** generated by the client will not match the one on the access point (AP).

Resulting Consequences:

1. **PMK Mismatch:**
    - The client and AP will derive **different PTKs (session keys)** from the mismatched PMK.
2. **MIC Verification Fails:**
    - The Message Integrity Code (MIC) sent by the client **won't match** what the AP expects.
    - The AP **rejects the handshake**.
3. **Repeated Failures:**
    - The client may keep trying to connect, but the **4-way handshake will fail repeatedly**.
4. **Connection Denied:**
    - The client **won't be able to join the Wi-Fi network**.

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

IEEE 802.1X solves the problem of unauthorized access to a wired or wireless network by providing port-based network access control.

Key Problems Solved by 802.1X:

1. **Unauthorized Device Prevention:**
    - **Only authenticated users/devices are allowed to access the network.**
2. **Secure User Authentication:**
    - **Uses protocols like EAP over LAN to verify user credentials via a RADIUS server.**
3. **Enterprise-Grade Access Control:**
    - **Ideal for environments needing individual user credentials, like companies, campuses, and secure public networks.**

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?

IEEE 802.1X enhances wireless security by enabling **strong, per-user authentication** and **dynamic encryption key management** before granting network access.

Key Ways 802.1X Improves Wireless Security:

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