Name: Devansh Srivastava

Registration number: 21BCE0527

Wi-Fi Training Programme

Module 6

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

Ans. The three pillars of Wi-Fi security are:

1. **Authentication:** Ensures that the device or user attempting to connect to the Wi-Fi network is authentic. It checks identity before providing access.

2. **Encryption:** Secures the data that is being carried over Wi-Fi from being intercepted and accessed by unauthorized individuals. It renders readable data into unreadable form.

3. **Integrity:** Ensures that the data sent and received over the Wi-Fi network is not altered or manipulated. If someone attempts to change it on the way, it can be identified.

Key Learning:

→ Wi-Fi security is founded on solid pillars such as authentication authorization encryption and integrity.

→ Wi-Fi security is not merely about passwords — it's about authenticating identity, concealing information, and guarding its purity.

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

Ans.

Authentication	**Encryption**
1. Identifies and verifies users/devices.	1. Secures the transmitted data by scrambling it.
2. It happens before data transmission begins.	2. It happens during data transmission.
3. Ensures that only authorized users can access the network.	3. Prevents outsiders from reading the data even if they capture it.

Key Learning:

→ Authentication checks who you are, while encryption hides what you are sending.

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

Ans

WEP (Wired Equivalent Privacy)	**WPA (Wi-Fi Protected Access)**	**WPA2 (Wi-Fi Protected Access 2)**	**WPA3 (Wi-Fi Protected Access 3)**
1. Released in 1999	1. Released in 2003 (temporary fix for WEP)	1. Released in 2004	1. Released in 2018
2. For Encryption it uses RC4 stream cipher (64-bit or 128-bit keys)	2. For Encryption it uses RC4 with TKIP (Temporal Key Integrity Protocol)	2. For Encryption it uses AES-CCMP (Advanced Encryption Standard - Counter Mode)	2. For Encryption it uses SAE (Simultaneous Authentication of Equals) (Dragonfly Key Exchange)
3. Basic encryption only	3. Message integrity check, key mixing	3. Strong encryption with AES, mandatory Wi-Fi certification since 2006	3. Forward secrecy, protection from dictionary attacks, better public Wi-Fi security
4. Major drawback is easily cracked in minutes, weak IV management	4. Major drawback is TKIP vulnerabilities, susceptible to attacks	4. Major drawback is vulnerable to KRACK attack (patched), weak password attacks possible	4. It is very strong, but still dependent on password strength
5. Current status is Obsolete and unsafe	5. Current status is deprecated and considered insecure	5. Current status is it is still widely used but slowly being phased out	5. Current status is that Current standard, mandatory for Wi-Fi certification since 2020

Key Learning:

→ Wi-Fi technology evolved from WEP → WPA → WPA2 → WPA3, each version aimed to fix previous vulnerabilities and make wireless communication more secure. Today, WPA3 is the gold standard for modern, secure Wi-Fi connections.

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

Ans. WEP is considered insecure compared to WPA2 or WPA3 because of :-

1. **Weak algorithm**: WEP used the RC4 cipher with poor key management.
2. **Short keys**: WEP keys were easy to guess because of their short length (40 or 104 bits).
3. **Reused Initialization Vectors (IVs)**: These repeated IVs made it easier for attackers to crack the keys.
4. **Passive attacks**: Hackers could simply capture packets and crack WEP passwords within minutes.

Key Learning:

→ WEP is outdated and unsafe, which is why newer standards like WPA2 and WPA3 were necessary for modern wireless security.

5. Why was WPA2 introduced?

Ans.

- WPA was only a temporary fix after the failure of WEP.
- Security experts wanted a permanent, future-ready solution.
- WPA2 provides: -
  - AES encryption (Advanced Encryption Standard) which is much stronger.
  - Full compliance with the new IEEE 802.11i security standard.
  - Support for 802.1X authentication in enterprise networks.

WPA2 became the industry standard because it solved major weaknesses and ensured strong, scalable Wi-Fi security.

Key Learning:

→ WPA2 was introduced to provide strong, long-term security to protect Wi-Fi networks against modern threats.

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

Ans.

- The PMK is a secret key shared between the client and the access point (AP).

- It is never transmitted directly over the air, which keeps it safe.
- During the 4-way handshake:

  1. The PMK is used to derive a new temporary key called the Pairwise Transient Key (PTK).
  2. This PTK is then used to encrypt actual communication data between the client and AP.

Key Learning:

→ Pairwise Master Key (PMK) is essential to WPA2 security since it serves as the basis for creating session keys that safeguard client-access point communication.

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

Ans. It takes place in four steps;-

➔ Step 1: Access Point sends ANonce (AP's Random Number) to Client

- The Access Point generates a random number called an ANonce.
- It sends this ANonce to the client (laptop, phone, etc.).
- This step challenges the client to prove that it knows the secret PMK.

➔ Step 2: Client generates PTK and sends SNonce (Client's Random Number) back

- After receiving the ANonce, the client:
  - Uses the PMK, the ANonce (received), its own randomly generated SNonce, and both MAC addresses to calculate a new key called the PTK (Pairwise Transient Key).
- The client then sends the SNonce and a Message Integrity Code (MIC) to the Access Point.
- This MIC is calculated using the new PTK — proving to the Access Point that the client knows the PMK without revealing it.

➔ Step 3: Access Point generates its own PTK and verifies

- Now, the Access Point:
  - Takes the PMK, ANonce, SNonce, and both MAC addresses to generate the PTK by itself.
- It compares its generated PTK with the MIC received from the client.
- If the MIC is valid, the Access Point confirms that the client is genuine.

➔ Step 4: Access Point sends confirmation (and installs keys)

- After verification, the Access Point sends a final confirmation message.
- This includes installing the encryption keys for actual data communication.
- Now the client also installs the keys, and secure communication can begin!

Key Learning:

→ The 4-way handshake ensures that both the client and the Access Point can prove possession of the secret key (PMK) securely, without directly revealing it, making the Wi-Fi connection safe from attackers.

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

Ans.

- The client will generate a wrong PMK because the passphrase is incorrect.
- This leads to mismatched PTKs during the handshake.
- As a result:
  - The handshake will fail.
  - The client won't connect to the network.
  - It will probably retry a few times before giving up.

Key Learning:

→ If the Wi-Fi password is wrong, the 4-way handshake **automatically protects the network** by blocking connection attempts.

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

Ans Key problems 802.1X solves are: -

1. **Unauthorized Access:** Without 802.1X, anyone who has wireless or physical access would be able to connect to the network. 802.1X requires authentication prior to access, preventing unauthorized users and devices from passing through.
2. **Inadequate User/Device Identification:** Traditional approaches rely on shared passwords for Wi-Fi, and thus it is not possible to track and control personal access. 802.1X authenticates each device or user separately prior to offering network connectivity.

3. **Security Risks in Open Networks:** In environments like guest Wi-Fi or public networks, open networks pose significant security risks. 802.1X can be employed to authenticate users even on such networks, adding an additional layer of security.
4. **Man-in-the-Middle Attacks:** By making use of sound authentication methods and often encryption, 802.1X virtually eliminates the possibility of bad motives intercepting traffic over the network and capturing authentication details.
5. **Centralized Access Control:** 802.1X often employs a central authentication server (like RADIUS), which provides one point to impose and regulate network access policies across all devices attached.

Key Learning:

→ 802.1X protects the network's gates by checking identity before allowing any device inside.

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

Ans. It provides: -
1. Port-based control: The network switch or access point only opens the connection (port) if authentication succeeds.

2. Dynamic keys: Once authentication is done, a unique encryption keys can be given to every device.

3. Centralized management: Administrators can manage who can connect, can monitor activity, and revoke access easily.

4. Protects against attacks: It reduces the risks of man-in-the-middle attack, rogue APs, and unauthorized access.

Key Learning:

→ In wireless environments, where physical security is harder to control, 802.1X adds a strong logical barrier against attackers.