Moulik Tammana

Wi-Fi Training Program Module – 6

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

1. Confidentiality

- **Data transmitted over Wi-Fi must be kept private from unauthorized users.**
- **Encryption (like WPA3, WPA2) is used to scramble information.**
- **Tools like VPNs and strong passwords help maintain confidentiality.**

2. Integrity

- **Ensures that data sent over Wi-Fi is not altered or tampered with.**
- **Message integrity checks (like MICs in WPA) detect unauthorized changes.**
- **Firmware updates and secure protocols prevent exploitation of vulnerabilities.**

3. Availability

- **Wi-Fi networks must stay accessible to authorized users when needed.**
- **Protection against Denial of Service (DoS) attacks is critical.**
- **Reliable hardware and network redundancy help maintain service uptime.**

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

Alright, let's break it down carefully and clearly:

Authentication in Wi-Fi Security:

- **Authentication is the process of verifying who you are before you are allowed to connect to the Wi-Fi network. (Verification)**
- **It makes sure that only authorized users or devices are allowed onto the network.**
- **How it works:**
  1. **When you try to connect to a Wi-Fi network, the router asks for some kind of proof — usually a password (in home Wi-Fi) or sometimes a certificate or username/password combo (in enterprise Wi-Fi).**
  2. **If you provide the correct credentials, you are authenticated and granted access.**
- **Examples:**
  1. **WPA2-PSK (Pre-Shared Key): You type in the Wi-Fi password.**
  2. **WPA2-Enterprise: You log in with a username and password, verified by a server (like RADIUS).**
  3. **MAC address filtering (less secure): Only approved device addresses are allowed.**

Encryption in Wi-Fi Security:

- **Encryption is the process of scrambling data so that only authorized devices (those with the right decryption keys) can understand it. (Encoding)**
- **It protects the actual information being transmitted over Wi-Fi from being read by hackers or snoopers.**
- **How it works:**
  1. **Once you're authenticated and connected, your device and the Wi-Fi router exchange a secret encryption key.**
  2. **Every piece of information you send (like website requests, emails, passwords) is encrypted using this key.**
  3. **Even if someone captures the wireless data, it will look like gibberish unless they have the key.**
- **Examples:**
  1. **WPA2 encryption uses AES (Advanced Encryption Standard).**
  2. **WPA3 encryption uses an even stronger method called SAE (Simultaneous Authentication of Equals) to create encryption keys.**

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

WEP (Wired Equivalent Privacy)

- **Introduced: 1997, the original Wi-Fi security protocol.**
- **Encryption: Used weak RC4 encryption with short (40-bit or 104-bit) keys.**
- **Problems: Easy to hack — flaws in the encryption made it crackable within minutes.**
- **Status: Completely obsolete today; no longer considered secure.**

WPA (Wi-Fi Protected Access)

- **Introduced: 2003 as a quick fix after WEP failed.**
- **Encryption: Improved RC4 encryption with TKIP (Temporal Key Integrity Protocol) for dynamic key generation.**
- **Problems: Stronger than WEP but still vulnerable to some attacks (especially today).**
- **Status: Better than WEP, but now also considered insecure.**

WPA2 (Wi-Fi Protected Access 2)

- **Introduced: 2004, mandatory for all Wi-Fi devices since 2006.**
- **Encryption: Uses AES (Advanced Encryption Standard) — very strong and widely trusted.**
- **Security Mode: Can use PSK (Pre-Shared Key) for home, or Enterprise mode with RADIUS servers for businesses.**
- **Problems: Strong, but vulnerable to brute force attacks if passwords are weak; also vulnerable to the KRACK attack (patched in most devices now).**

WPA3 (Wi-Fi Protected Access 3)

- **Introduced: 2018, the latest and most secure standard.**
- **Encryption: Improved encryption with SAE (Simultaneous Authentication of Equals) replacing PSK, making password guessing attacks much harder.**
- **Features: Includes Forward Secrecy (new encryption keys for every session) and stronger protection for open networks (like cafes) via Opportunistic Wireless Encryption (OWE).**
- **Status: Most secure option today; slowly becoming standard on new devices.**

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

1. **Weak Encryption (RC4 with Static Keys):**

- **WEP uses an old encryption method (RC4) with very short key lengths (40 or 104 bits).**
- **Keys were often reused, making it easy for hackers to capture enough packets and crack the key in minutes using simple tools.**

2. **Poor Key Management:**

- **WEP does not automatically change keys during a session.**
- **Once a hacker captures a small amount of network traffic, they can easily find patterns and break the encryption.**

3. **No Protection Against Modern Attacks:**

- **WEP was designed before today's powerful computers and hacking techniques.**
- **Tools like Aircrack-ng can easily break WEP security with minimal effort.**

4. **Compared to WPA2/WPA3:**

- **WPA2 uses AES encryption (very strong, secure, and trusted even for government use).**
- **WPA3 adds even better security with SAE handshake, forward secrecy, and stronger password protection, even on public networks.**

Q5. Why was WPA2 introduced?

To Fix WPA's Shortcomings:

- **WPA (the first version) was only a temporary solution to replace broken WEP security.**
- **WPA still used RC4 encryption (just with better key management through TKIP), but RC4 was already becoming outdated and vulnerable.**

Need for Stronger Encryption:

- **Organizations and security experts demanded a much stronger, future-proof encryption method.**
- **WPA2 introduced AES (Advanced Encryption Standard) — a powerful encryption method used even by governments and banks.**

Meet Industry Standards (IEEE 802.11i):

- **WPA2 was designed to fully comply with the IEEE 802.11i security standard, which set a formal, complete security framework for Wi-Fi networks.**
- **WPA had only been a stopgap before 802.11i was finalized.**

Better Protection Against Evolving Attacks:

- **As hackers and computers got more powerful, simple fixes like TKIP were no longer enough.**
- **WPA2 provided stronger defences against brute force attacks, replay attacks, and packet tampering.**

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 securing Wi-Fi connections during the 4-way handshake process. After a device successfully authenticates (for example, by entering the correct Wi-Fi password in WPA2-PSK networks), both the client (like your phone) and the Wi-Fi access point derive the same PMK independently. The PMK acts as the shared secret that is never directly transmitted over the air. Instead, it is used to securely create new encryption keys that will protect the data exchange between the client and the access point.

During the 4-way handshake, the PMK is combined with fresh random values (called nonces) generated by both the client and the access point. Using these nonces and the PMK, they both compute a new, unique key called the Pairwise Transient Key (PTK). This PTK is then used to encrypt the actual communication session. By using the PMK this way, the network ensures that even if an attacker is listening, they can't derive the session keys without knowing the PMK — making the Wi-Fi connection highly secure.

Q7. How does the 4-way handshake ensure mutual authentication between the client and the access point?

The 4-way handshake is designed so that both the client (like a laptop or phone) and the access point (Wi-Fi router) prove to each other that they both know the same secret — the Pairwise Master Key (PMK) — without ever sending the PMK itself over the air.

Here's step-by-step how mutual authentication happens:

1. **Access Point Sends ANonce (Random Number):**

- **After the client tries to connect, the access point sends a freshly generated ANonce (Access Point Nonce) to the client.**
- **This is a random value and will be used to help create encryption keys.**

2. **Client Creates PTK and Sends MIC (Message Integrity Code):**

- **The client generates its own random number called SNonce (Supplicant Nonce).**
- **Using the PMK, the ANonce, SNonce, and both MAC addresses (client and AP), the client computes a Pairwise Transient Key (PTK).**
- **The client then sends the SNonce plus a Message Integrity Code (MIC) back to the access point.**
- **The MIC is like a "signature" made using the PTK, proving the client knows the right PMK without revealing it.**

3. **Access Point Verifies the Client:**

- **The access point also computes the PTK using the same method.**
- **It checks the MIC it received from the client.**

- **If the MIC is correct, it knows the client really has the PMK.**

4. **Access Point Sends Another MIC (and Group Key):**
- **After verifying the client, the access point sends another message with its own MIC (and sometimes a group key for multicast/broadcast traffic).**
- **This lets the client verify that the access point also knows the PMK.**

5. **Client Verifies the Access Point:**
- **The client checks the MIC sent by the access point.**
- **If it matches, it confirms that the access point is authentic too.**

Message	Sender	Description
Message 1	Access Point	Sends a random number (ANonce) to the client to start the handshake process.
Message 2	Client	Sends its own random number (SNonce) along with a Message Integrity Code (MIC), proving it knows the PMK.
Message 3	Access Point	Verifies the MIC from the client. If it matches, it computes the Pairwise Transient Key (PTK) and sends it back along with its own MIC and sometimes a Group Key.
Message 4	Client	Verifies the MIC from the access point. If it matches, the 4-way handshake is complete, and both parties can securely communicate.

Q8. What will happen if we put a wrong passphrase during a 4Way handshake?

The following thing can happen if we put a wrong passphrase:

1. Incorrect PMK Generation
- **The Pairwise Master Key (PMK) is derived from the passphrase. When you enter the wrong passphrase, the PMK generated on your device will be incorrect.**
- **The access point and the client (your device) must have the same PMK to proceed with the handshake, and since the PMK is wrong, they won't be able to generate matching Pairwise Transient Keys (PTK).**

2. MIC Mismatch
- **During the 4-way handshake, the client computes a Message Integrity Code (MIC) based on the PTK and sends it to the access point.**
- **Since the client is using the incorrect PMK, the PTK will be incorrect, and the MIC generated will not match the one expected by the access point.**
- **When the access point receives the MIC, it will verify the message, and because it doesn’t match the expected value, the access point will know that the authentication has failed.**

3. Handshake Failure
- **As a result of the MIC mismatch, the access point will reject the client's attempt to authenticate.**
- **The handshake will fail, and the device will not be able to establish a connection with the Wi-Fi network.**
- **The device will usually show a "wrong password" or "authentication failed" error message.**

4. No Access Granted
- **Since the 4-way handshake failed due to the wrong passphrase, the client will not be granted network access.**
- **The device will either retry the handshake or show an error message, prompting the user to check the password.**

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

1. Unauthorized Access to Networks

Without proper access control, anyone can connect to a network if they have physical access to it (e.g., plugging into an Ethernet port or connecting to a Wi-Fi network). This could lead to:

- **Unauthorized devices gaining access to sensitive resources.**
- **Malicious actors attempting to exploit the network.**

2. Lack of Secure Wireless Authentication (for Wi-Fi)

Wi-Fi networks, especially those using older security protocols like WEP, lacked robust authentication mechanisms. Even with WPA and WPA2, the use of Pre-Shared Keys (PSK) led to security issues:

- **Weak passwords can be easily guessed, allowing attackers to access the network.**
- **Devices may not be properly authenticated, leading to the risk of network infiltration.**

3. Centralized Authentication Management

In large organizations, managing device authentication can be challenging, especially when there are numerous devices that need to be securely managed and controlled.

4. Vulnerability to Network Attacks (Man-in-the-Middle, Spoofing)

Without proper authentication, attackers can attempt to spoof legitimate devices or perform Man-in-the-Middle (MitM) attacks where they intercept communication between the client and the network.

Problem	Solution
Unauthorized Access to Networks	802.1X ensures that only authorized devices can gain access to the network by implementing strong authentication before a device can connect. It requires the device to authenticate itself with an Authentication Server (usually via RADIUS) before being allowed access to the network.
Lack of Secure Wireless Authentication (for Wi-Fi)	In Wi-Fi networks, 802.1X provides centralized authentication and dynamic encryption key management, making it much more secure than WPA2-PSK. Each device is required to authenticate before connecting, and encryption keys are generated on a per-session basis, preventing unauthorized devices from accessing the network.
Centralized Authentication Management	802.1X integrates with centralized authentication servers like RADIUS. This allows for: • Centralized management of authentication policies and user credentials. • The ability to enforce network access policies (e.g., which devices can access what resources). • Real-time auditing and monitoring of which devices are connected to the network.
Vulnerability to Network Attacks (Man-in-the-Middle, Spoofing)	By requiring mutual authentication (between the client and the network infrastructure), 802.1X prevents: • Spoofing: Only authenticated devices can access the network, preventing attackers from pretending to be legitimate clients. • Man-in-the-Middle (MitM): By using strong encryption during authentication (often with EAP-TLS), it prevents attackers from intercepting or altering communication during the authentication process.

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

1. Prevents Unauthorized Access to the Network

- **802.1X applies port-based network access control (PNAC), requiring devices to authenticate before they can gain access to the network.**
- **This ensures that only devices with valid credentials are allowed to connect, blocking any unauthorized device from accessing the network just by being in proximity.**
- **This makes it significantly more challenging for unauthorized users or attackers to penetrate the network.**

2. Advanced Authentication Techniques

- **802.1X leverages the Extensible Authentication Protocol (EAP), which supports multiple authentication methods, including:**
  1. **EAP-TLS, which uses certificates for authentication,**
  2. **EAP-PEAP and EAP-TTLS, providing encrypted username/password authentication,**
  3. **Other options like EAP-MD5 and EAP-SIM, depending on specific network needs.**
- **This flexibility allows for stronger security by supporting advanced authentication mechanisms such as digital certificates or smartcards, which provide more robust protection compared to traditional methods like WEP or PSK.**

3. Mutual Authentication for Increased Protection

- **802.1X enables mutual authentication, ensuring that both the client device and the access point (AP) authenticate each other.**
- **This guarantees that users are connecting to a legitimate AP and prevents attacks where rogue access points (known as evil twins) may be used to intercept communication.**
- **By supporting mutual authentication, it significantly reduces the risk of spoofing attacks, making it much harder for attackers to trick users into connecting to malicious APs.**

4. Dynamic Encryption Key Generation

- **After a successful authentication, 802.1X ensures the creation of unique, dynamic encryption keys between the client and the AP.**
- **These keys are generated per session, ensuring that every communication is encrypted, providing additional protection against eavesdropping.**
- **In WPA2 and WPA3 networks, the Pairwise Master Key (PMK) is used to generate session keys during the 4-way handshake, ensuring that each session is isolated and secure, even if previous sessions have been compromised.**