Vivek Narayanan D
Coimbatore Institute of Technology

MODULE 6 ASSIGNMENT

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

Wi-Fi security revolves around several critical pillars that ensure safe, reliable, and trustworthy wireless communication. The main pillars include Confidentiality, Integrity, Availability, Authentication, and Accountability.

- **Authentication**: Authentication verifies that users and devices connecting to the Wi-Fi network are genuine. Pre-Shared Key (PSK) for personal networks and 802.1X authentication for enterprises play critical roles in confirming identities before granting access.
- **Confidentiality**: It ensures that the data transmitted over Wi-Fi is protected from eavesdroppers. Confidentiality is maintained through encryption methods like WPA2's AES and WPA3's SAE, which prevent unauthorized users from accessing sensitive information.
- **Integrity**: Integrity ensures that data is not tampered with during transmission. Mechanisms like Message Integrity Codes (MIC) and protocols like CCMP in WPA2 verify that received data is exactly what was sent, safeguarding against packet manipulation and injection attacks.
- **Availability**: Availability guarantees that Wi-Fi networks are operational and accessible to authorized users when needed. Threats like Denial-of-Service (DoS) attacks aim to disrupt this. Solutions include management frame protection (802.11w) and RF interference management.
- **Accountability**: Accountability involves tracking user actions within the network to ensure responsibility. Logging connection histories, using unique user credentials, and auditing activities provide traceability, which helps in forensic investigations if breaches occur.

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

Authentication is the process of verifying the identity of a user or device trying to connect to a wireless network. Its primary purpose is to ensure that only authorized individuals or devices gain access. Authentication mechanisms confirm that the person or system is who they claim to be before granting network privileges. In Wi-Fi security, authentication can happen through various methods like Pre-Shared Key (PSK) in WPA2-Personal networks or through 802.1X authentication servers (like RADIUS) in WPA2/WPA3-Enterprise

environments. For example, in a home Wi-Fi setup, entering a Wi-Fi password is a basic form of authentication. In corporate environments, users often provide digital certificates or unique login credentials to authenticate themselves securely.

Encryption is the process of converting transmitted data into a coded form that is unreadable to unauthorized users. It protects the data from being intercepted and understood by third parties. Even if an attacker captures the wireless signals, encryption ensures that the information remains confidential unless the attacker has the correct decryption key. Encryption methods in Wi-Fi include algorithms like AES (Advanced Encryption Standard) used in WPA2 and WPA3. Encryption focuses on safeguarding the content of communication after the authentication process has permitted a device to join the network.

Authentication is about deciding *who is allowed* to join the network, while encryption is about protecting *what is being sent* over the network. Authentication happens before a device or user is allowed access to the network, whereas encryption operates after the connection is established, securing the ongoing data exchange. Without authentication, anyone could join the network. Without encryption, even authenticated users' data could be vulnerable to eavesdropping.

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

WEP (Wired Equivalent Privacy) was the first Wi-Fi security standard, introduced in 1997. Its goal was to provide wireless security comparable to wired networks. WEP uses the RC4 encryption algorithm along with a static key. However, its implementation was flawed—especially due to short Initialization Vectors (IVs) of just 24 bits—which made WEP extremely vulnerable to hacking. WEP is now considered obsolete and insecure and is rarely used today.

WPA (Wi-Fi Protected Access) emerged in 2003 as a temporary solution to WEP's weaknesses while a more robust protocol was being developed. WPA also used RC4 but introduced significant improvements, like TKIP (Temporal Key Integrity Protocol), which dynamically generated keys for each packet to make attacks harder. However, TKIP was only a stopgap measure and was itself eventually found to be vulnerable. WPA was better than WEP but not strong enough for modern security needs.

WPA2 (Wi-Fi Protected Access II), introduced in 2004, became the new gold standard in Wi-Fi security for over a decade. It replaced RC4 and TKIP with the more secure AES (Advanced Encryption Standard) combined with CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). WPA2-Enterprise also allowed

businesses to use 802.1X authentication servers for managing users individually instead of sharing a single network password.

WPA3, released in 2018, addresses WPA2's shortcomings and aligns with the demands of a modern, connected world. It replaces the Pre-Shared Key (PSK) method with Simultaneous Authentication of Equals (SAE), a more robust handshake mechanism resistant to offline dictionary attacks. WPA3 mandates the use of 192-bit encryption in Enterprise mode and uses Forward Secrecy, ensuring that even if session keys are compromised, previous communications remain secure. Another important addition is Enhanced Open, which encrypts traffic on open Wi-Fi networks (without passwords) using Opportunistic Wireless Encryption (OWE). WPA3 also improves usability with features like easier device onboarding via Wi-Fi Easy Connect.

- **Encryption Algorithms**: WEP and WPA used RC4 (weak), WPA2 moved to AES (strong), WPA3 enhances it with SAE and 192-bit security.
- **Key Management**: WEP used static keys, WPA introduced dynamic keys (TKIP), WPA2 strengthened key handling with AES/CCMP, WPA3 employs more resilient handshake protocols.
- **Vulnerability**: WEP is easily hackable, WPA is moderately better but still weak, WPA2 is strong but not flawless, and WPA3 fixes many remaining vulnerabilities.
- **Authentication**: WPA2 and WPA3 support robust Enterprise authentication (802.1X) apart from simple PSK; WPA3 introduces forward secrecy and stronger initial handshake security.
- **Usage**: WEP is deprecated, WPA is outdated, WPA2 is still widely used but being phased out, WPA3 is the future standard for all secure wireless networks.

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

WEP (Wired Equivalent Privacy) is considered insecure primarily due to its flawed design, weak encryption practices, and vulnerability to fast, practical attacks. Compared to WPA2 and WPA3, WEP fails fundamentally at ensuring data confidentiality and network security.

WEP lies in its use of the RC4 encryption algorithm with very short Initialization Vectors (IVs). WEP uses a 24-bit IV combined with either a 40-bit or 104-bit key. Because the IV is so small, it repeats frequently. In high-traffic networks, identical IVs are captured easily

by attackers, allowing them to analyse patterns and eventually deduce the encryption key. This repetition drastically weakens the supposed randomness and leads to rapid key recovery.

WEP keys are static. Once set, they remain unchanged unless the user manually reconfigures them. If a key is compromised, it compromises the entire network until it is manually replaced. By contrast, WPA2 and WPA3 dynamically generate new encryption keys during each session (using AES-CCMP or SAE), making it far more difficult for attackers to decrypt network traffic.

WEP lacks proper message integrity checking. It uses a weak CRC-32 checksum to detect data tampering, which is not cryptographically secure. Attackers can modify packets and recalculate a valid checksum without knowing the encryption key. In contrast, WPA2 and WPA3 use Message Integrity Codes (MIC) that are much stronger, detecting and blocking any data manipulation attempts.

WPA2 replaced WEP's weak RC4/TKIP methods with the AES encryption standard. AES uses a strong mathematical structure resistant to all known practical attacks. WPA2 also introduced CCMP for message integrity, which fixes WEP's checksum weakness. WPA3 further hardens security by introducing Simultaneous Authentication of Equals (SAE) instead of the vulnerable PSK handshake used in WPA2. SAE offers protection against offline dictionary attacks and adds forward secrecy, ensuring that even if an attacker later obtains session keys, they cannot decrypt previously captured data.

5. Why was WPA2 introduced?

- WPA2 (Wi-Fi Protected Access II) was introduced in 2004 as an essential upgrade over WPA to provide a much stronger, long-term security standard for wireless networks. It addressed several critical vulnerabilities in WPA and especially in the even older, highly insecure WEP system.
- WPA was only a temporary "patch" that improved WEP's security flaws but still relied on the same RC4 stream cipher and TKIP (Temporal Key Integrity Protocol). Although TKIP introduced better key rotation and message integrity than WEP, it was still built on outdated technology and had theoretical vulnerabilities.
- The IEEE 802.11i standard was developed to define a stronger security framework, and WPA2 was based directly on this 802.11i standard. A major reason for WPA2's introduction was the adoption of the AES (Advanced Encryption Standard) as the mandatory encryption method. AES is a symmetric encryption standard trusted by governments and industries worldwide for its high level of security. Unlike RC4, which

is a stream cipher, AES operates as a block cipher, making it far more resistant to known attacks.

- WPA2 has the use of CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) instead of TKIP for message integrity and encryption. CCMP is much stronger and ensures both data confidentiality and integrity without the vulnerabilities associated with TKIP.
- Another reason for WPA2's introduction was the need for **future-proofing Wi-Fi security**. With wireless networks becoming more widespread in homes, businesses, and public spaces, stronger security became essential to protect sensitive data against eavesdropping, man-in-the-middle attacks, and unauthorized access. WPA2 was designed to be sufficiently strong to withstand emerging threats for many years.

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 securing the 4-way handshake process during Wi-Fi authentication, especially in WPA2 and WPA3 networks. The PMK is essentially a shared secret key that both the client (supplicant) and the Access Point (authenticator) use to derive further encryption keys necessary for protecting wireless communication.

The PMK can be generated in two ways:

- In WPA2-Personal (PSK) mode, the PMK is derived from the Pre-Shared Key (password) entered by the user.
- In WPA2-Enterprise mode, the PMK is generated after successful authentication via a RADIUS server using 802.1X.

The **main purpose** of the PMK is to derive the **Pairwise Transient Key (PTK)** securely during the 4-way handshake without ever sending the PMK itself over the air.

1. The Access Point sends a random number (ANonce) to the client.
2. The client generates its own random number (SNonce) and now has both nonces.
3. Using the PMK + ANonce + SNonce + MAC addresses (of both devices), the client and AP each independently compute the PTK.
4. The PTK is then used to create keys for encryption (temporal keys) and for message integrity.

Thus, the PMK remains secret throughout the exchange and is never transmitted directly, preventing interception. Without the PMK, devices cannot correctly generate the same PTK, meaning the session encryption would fail, and the connection would not be established.

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

The 4-way handshake is a critical process in WPA2 and WPA3 Wi-Fi security protocols. Its main purpose is to prove that both the client (also called the supplicant) and the Access Point (AP) possess the correct Pairwise Master Key (PMK) without actually transmitting it over the air. This process ensures mutual authentication — meaning both sides verify each other's legitimacy before secure communication begins.

Before the handshake begins, both the client and the AP already share a Pairwise Master Key (PMK), which is obtained either from the Wi-Fi password (in WPA2-Personal) or from 802.1X authentication (in WPA2-Enterprise). Importantly, the PMK itself is never transmitted; it is used internally to derive session-specific encryption keys.

The 4-Way Handshake Steps

- Message 1 (AP → Client): The AP sends an ANonce (a random number) to the client. This allows the client to begin computing the Pairwise Transient Key (PTK), although no authentication is proven yet.
- Message 2 (Client → AP): The client generates its own SNonce and calculates the PTK using both nonces and the PMK. It then sends the SNonce along with a Message Integrity Code (MIC). The AP verifies the MIC — if correct, it confirms that the client possesses the correct PMK, authenticating the client.
- Message 3 (AP → Client): The AP sends the Group Temporal Key (GTK), encrypted using the PTK, and a MIC. The client verifies the MIC, ensuring that the AP too possesses the correct PMK, thus authenticating the AP.
- Message 4 (Client → AP): The client sends a confirmation message, signalling that it has installed the encryption keys, completing the mutual authentication.

Throughout the 4-way handshake, neither the PMK nor the PTK is transmitted directly. Instead, by verifying the MICs bound to fresh nonces and keys, both the client and AP prove their identities securely, ensuring encrypted and trusted communication.

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

In Wi-Fi networks secured with **WPA2** or **WPA3**, the **4-way handshake** is a critical process that establishes trust and encryption between a client (like a laptop or smartphone) and an Access Point (AP, like a router).

For the handshake to succeed, both the client and the AP must derive the exact same Pairwise

Master Key (PMK) — a key generated from the Wi-Fi passphrase (or through 802.1X authentication in Enterprise setups).

If a client enters the wrong Wi-Fi passphrase, the following sequence of failures occurs:

1. Incorrect PMK and PTK Derivation

The passphrase entered by the client is used to derive the PMK through a process called PBKDF2 (Password-Based Key Derivation Function 2). If the passphrase is wrong, the resulting PMK will also be incorrect. Subsequently, when the client and AP exchange nonces (random numbers) during the handshake, the client will attempt to compute the Pairwise Transient Key (PTK) using its wrong PMK along with the ANonce, SNonce, and MAC addresses. Because the PMK is incorrect, the derived PTK will also be wrong.

2. Message Integrity Code (MIC) Validation Failure

During the 4-way handshake:

- In Message 2, the client sends its SNonce and a Message Integrity Code (MIC) computed using its PTK.
- The AP, using its correct PMK and PTK, checks the MIC to ensure it matches.

Since the client's PTK is wrong, the MIC it generates will not match the AP's expectations. When the AP verifies the MIC, the validation will fail immediately.

This MIC mismatch is a clear sign to the AP that the client does not possess the correct PMK (and therefore an incorrect password was used).

3. Immediate Abortion of the Handshake

Upon detecting a MIC failure, the AP will abort the handshake process. It will not proceed to Message 3 or Message 4. The client will be disassociated from the network, and no keys (like PTK or GTK) will be installed for encryption. Thus, the Wi-Fi connection will fail completely. The client remains disconnected and cannot send or receive any encrypted traffic.

4. Retry Attempts and Limitations

Some devices are configured to retry connecting automatically if an authentication attempt fails. However, each retry will also fail if the wrong passphrase is not corrected. Excessive failed attempts may trigger security measures such as temporary blocking or rate limiting from the AP to defend against brute-force attacks.

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

IEEE 802.1X is a network access control (NAC) protocol that is used to secure both wired and wireless networks by providing an authentication framework for devices attempting to access a network. This standard addresses the critical issue of unauthorized access to a network, enhancing security by ensuring that only authenticated devices and users can connect to the network. It is particularly important in environments where sensitive data is being transmitted or where network resources need to be protected from malicious actors.

1. Unauthorized Access Prevention

One of the primary problems that 802.1X addresses is the risk of unauthorized access to a network. Without any authentication mechanism, any device within range of a network (wired or wireless) can potentially access it, thereby gaining access to network resources, data, and services. This vulnerability exposes the network to security breaches, including data theft, denial of service (DoS) attacks, and malware infiltration.

2. Network Security and Data Integrity

In an environment without strong authentication, sensitive data traveling over a network may be intercepted by unauthorized users. This can lead to data theft, man-in-the-middle attacks, or modification of data in transit. 802.1X enforces authentication, ensuring that only devices that can verify their identity are allowed to join the network. This helps protect the confidentiality and integrity of the data transmitted over the network by blocking unauthorized access before it happens.

3. Device Authentication

802.1X provides device-based authentication, meaning that each device must provide credentials to access the network. This process can involve several authentication methods such as EAP (Extensible Authentication Protocol), which supports different methods like EAP-TLS (Transport Layer Security) and EAP-PEAP (Protected EAP). The 802.1X process authenticates the user or device against a central authentication server (often a RADIUS server).

4. Network Visibility and Control

802.1X provides administrators with detailed visibility into which devices are connected to the network and their authentication status. This enables administrators to enforce security policies more efficiently and track the behaviour of devices on the network. In case of any suspicious activity or unauthorized attempts to connect, administrators can take immediate action such as blocking access or isolating compromised devices. This visibility extends across both wired and wireless networks, ensuring consistent security management.

5. Protection for Wireless Networks

In wireless networks, the risk of unauthorized access is even more significant because signals can be intercepted more easily than in wired networks. 802.1X plays a crucial role in securing wireless networks by adding an authentication layer before granting network access. In Wi-Fi networks, 802.1X works alongside WPA2/WPA3 enterprise security protocols, which encrypt data and enforce user authentication to prevent unauthorized users from gaining access to the network.

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

IEEE 802.1X enhances security over wireless networks by providing a robust authentication framework that ensures only authorized devices and users can connect to the network.

1. Device and User Authentication

802.1X requires devices to authenticate before gaining access to the network. This process uses Extensible Authentication Protocol (EAP), which supports multiple authentication methods, such as EAP-TLS (Transport Layer Security) and EAP-PEAP (Protected EAP).

2. Mutual Authentication

One of the key features of 802.1X is mutual authentication, where both the device (supplicant) and the network (authenticator) authenticate each other. This ensures that the device connecting to the network is legitimate, and the network is trusted by the device. This mutual authentication eliminates the risk of a man-in-the-middle attack, where an attacker could pose as a legitimate access point to intercept sensitive data or gain unauthorized access to the network.

3. Encryption of Data Transmission

When 802.1X is used with WPA2 or WPA3 security protocols, it ensures that communication between the device and the access point is encrypted. This prevents unauthorized interception of sensitive data during transmission. Without strong encryption, wireless networks are vulnerable to eavesdropping, as the signals are broadcast over the air.

4. Prevents Unauthorized Device Access

In traditional Wi-Fi networks, anyone within range of the access point can attempt to connect if they know the network password. If that password is compromised, malicious actors can easily gain access. 802.1X solves this by requiring each device to authenticate with a central RADIUS server. Only devices that are verified by the server are allowed to access the network. This provides a much stronger layer of security compared to shared passwords, as each device needs to authenticate with unique credentials.

5. Granular Access Control

802.1X allows for role-based access control (RBAC). After a device is authenticated, the RADIUS server can assign it to specific Virtual LANs (VLANs) based on the device's identity or the user's role. For example, corporate devices might be placed on a VLAN that has full access to internal resources, while guest devices could be assigned to a VLAN with limited access (e.g., internet-only access). This segmentation helps prevent unauthorized users from accessing sensitive resources on the network and ensures that each user or device can only access the resources they are authorized for.

6. Dynamic Authentication for Guests

For networks that need to accommodate guest access (such as public Wi-Fi hotspots), 802.1X enables more secure management. Instead of relying on a simple shared password for guests, administrators can use a captive portal or other EAP methods to authenticate guest users. The authentication process for guests can also be configured to provide limited access, ensuring the network remains secure even with external users.

7. Prevention of Rogue Access Points

802.1X also helps prevent the use of rogue access points (APs) that could be set up by malicious actors to intercept network traffic. Because 802.1X requires authentication for devices to connect, unauthorized access points will not be able to participate in the network's authentication process. This makes it much harder for attackers to create unauthorized APs that could trick legitimate users into connecting and exposing sensitive data.