Module 6 Answers

Wi-Fi Training Program

Siddharth Balaji

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

Confidentiality:

- It ensures that sensitive information is only accessible to those who are authorized to view it.
- The methods used to achieve confidentiality include encryption, access control, authentication, and data classification.

Integrity:

- It ensures that data remains accurate, consistent, and unmodified during storage, transmission, and processing.
- The methods used to ensure integrity include hashing, checksums, digital signatures, and data validation mechanisms.

Authenticity:

- Authentication is the process of verifying the identity of a user, device, or system before granting access to resources.
- It is about making sure that the entity trying to access a system or data is who they claim to be.

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

FEATURE	**AUTENTICATION**	**ENCRYPTION**
Defintion	Verifies who is connecting to the Wi-Fi network.	Secures what data is being transmitted over the network.
Purpose	Ensures only authorized users or devices can connect.	Protects data privacy by making it unreadable to unauthorized parties.
Process	Involves verifying user/device identity (e.g., via passwords, certificates, etc.).	Involves scrambling data using a cryptographic algorithm (e.g., AES).
Wi-Fi standards	WPA2/WPA3 Authentication (e.g., PSK, 802.1X/EAP)	WPA2/WPA3 Encryption (e.g., AES, TKIP)
Methods	Pre-shared Key (PSK), 802.1X/EAP (Enterprise)	WPA2 (AES or TKIP encryption), WPA3 (AES encryption)
Role	Ensures only legitimate devices can connect to the network.	Protects data confidentiality during transmission.
Attacks prevented	Protects against unauthorized access (e.g., hacking the network).	Protects data from eavesdropping and man-in-the-middle attacks.

Impact on performance	Authentication may introduce a slight delay during connection.	Encryption can slightly reduce throughput due to processing overhead, but crucial for privacy.
Time of action	It happens when the device first tries to connect.	It happens during the actual data transmission, after connection.
Example	Pre-shared Key (PSK), 802.1X/EAP (Enterprise)	Data sent over the Wi-Fi is encrypted, making it unreadable to outsiders.

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

FEATURE	WEP (WIRED EQUIVALENT PRIVACY)	WPA (WI-FI PROTECTED ACCESS)	WPA2 (WI-FI PROTECTED ACCESS 2)	WPA3 (WI-FI PROTECTED ACCESS 3)
YEAR	1997	2003	2004	2018
SECURITY LEVEL	Low	Moderate	High	Very High
ENCYRPTION TYPE	RC4 (stream cipher)	TKIP (Temporal Key Integrity Protocol), RC4	AES (Advanced Encryption Standard)	AES (Advanced Encryption Standard), 192-bit for Enterprise
KEY LENGTH	0-bit or 104-bit	128-bit (with TKIP)	128-bit or 256-bit (AES)	128-bit or 256-bit (AES), 192-bit for Enterprise
AUTHENTICATION	Shared key (no server-based authentication)	PSK (Pre-Shared Key) or 802.1X/EAP (Enterprise)	PSK (Pre-Shared Key) or 802.1X/EAP (Enterprise)	Simultaneous Authentication of Equals (SAE) for PSK, 802.1X/EAP for Enterprise
DATA INTEGIRTY	Weak integrity (RC4+CRC-32), vulnerable to attacks	Vulnerable to certain attacks (e.g., dictionary attacks on PSK)	More secure but susceptible to certain vulnerabilities (e.g., KRACK attack)	Strong integrity (AES with CBC-MAC, higher protections)
VULNERABILITY	Highly insecure, vulnerable to many attacks (e.g., key reuse, weak encryption)	Vulnerable to certain attacks (e.g., dictionary attacks on PSK)	More secure but susceptible to certain vulnerabilities (e.g., KRACK attack)	Very secure, resistant to dictionary attacks, protects against offline brute-force attacks

STRENGTH OF ENCRYPTION	Weak, easily cracked (due to RC4 weaknesses)	Better than WEP but still weaker than WPA2	Strong encryption, AES ensures high-level security	Strongest encryption, harder to crack, uses more robust algorithms
PROTECTION AGAINST DICTIONARY ATTACKS	None	Weak protection, easily attacked by brute-force or dictionary methods	Stronger protection with PSK, vulnerable to offline attacks if weak passwords used	Strong protection against brute-force and offline dictionary attacks, using SAE (Dragonfly)
BACKWARDS COMPATIABILITY	Supported by most legacy devices	Compatible with WEP and WPA2, but not ideal due to security weaknesses	Not backward-compatible with WEP, but works with WPA	Not backward-compatible with WEP, supports WPA2, but newer devices should be preferred

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

I have represented the reasons in a tabular form.

REASON	WEP	WPA2/WPA3
WEAK ENCRYPTION ALGO	WEP uses the RC4 stream cipher, which has several known vulnerabilities.	WPA2 and WPA3 use AES (Advanced Encryption Standard), a much stronger encryption method.
SHORT KET LENGTH	WEP uses 40-bit or 104-bit keys, which are too short by modern standards. It makes brute-force attacks feasible.	WPA2 and WPA3 use 128-bit or 256-bit keys (AES), providing much stronger protection.
KEY REUSE	WEP keys are often reused and static, meaning the same key is used repeatedly. This makes it easy for attackers to analyze the data.	WPA2 and WPA3 use dynamic keying, meaning keys change periodically, reducing the risk of key reuse attacks.
WEAK INTIALIZATION VECTOR (IV)	WEP uses a 24-bit IV (Initialization Vector), which is too short and repeats too quickly. This leads to patterns that can be exploited by attackers.	WPA2 and WPA3 use longer IVs and different methods to handle IVs, making it much harder for attackers to find patterns in encrypted data.
LACK OF INTEGIRTY CHECKING	WEP does not use strong integrity checking for data. It uses a simple CRC-32 checksum, which is vulnerable to attacks like bit-flipping.	WPA2 and WPA3 use strong integrity checks with AES and CBC-MAC to prevent attacks on the data's integrity.

VULNERABILITY TO ATTACKS	WEP is highly vulnerable to several types of attacks, including cracking the WEP key using tools like Aircrack-ng, and IV collision attacks	WPA2 and WPA3 are much harder to break into. WPA3, in particular, is designed to resist brute-force and dictionary attacks.
REPLAY ATTACKS	WEP doesn't have robust protections against replay attacks, where encrypted data is intercepted and resent to the network.	WPA2 and WPA3 include mechanisms to prevent replay attacks, making communication more secure.
USER AUTHENTICATION	WEP lacks a mechanism for strong user or device authentication.	WPA2 and WPA3 provide strong authentication using 802.1X/EAP for enterprise networks and better protection with SAE (Simultaneous Authentication of Equals) in WPA3 for personal networks.

Q5. Why was WPA2 introduced?

SECURITY VULNERABILITIES:
WEP had several serious security flaws, such as weak encryption (RC4), short key lengths (40-bit/104-bit), and the reuse of IVs (Initialization Vectors), making it vulnerable to attacks.

WEAK ENCRYPTION (RC4):
WEP used the RC4 stream cipher, which had known vulnerabilities and was easy to break with modern computing power. WPA2 addressed this by using the much stronger AES (Advanced Encryption Standard).

STATIC KEYING IN WEP:
WEP used static, hard-coded keys that were often reused. WPA2 implemented dynamic keying using AES, making it far more difficult for attackers to crack keys.

LACK OF STRONG INTEGRITY CHECKING:
WEP used a simple CRC-32 checksum for integrity, which could easily be manipulated. WPA2 replaced this with AES and CBC-MAC for robust integrity and data protection.

PROTECTION AGAINST BRUTE-FORCE ATTACKS:
WEP was vulnerable to brute-force attacks because of its weak encryption. WPA2 used stronger encryption algorithms and dynamic keys to significantly reduce this risk.

NO PROTECTION AGAINST REPLAY ATTACKS:
WEP did not provide sufficient protection against replay attacks (where attackers retransmit captured data). WPA2 implemented mechanisms to protect against these attacks.

BETTER AUTHENTICATION:
WPA used the TKIP protocol, which still had vulnerabilities, and did not provide strong authentication. WPA2 introduced 802.1X/EAP (Extensible Authentication Protocol) for more secure enterprise-level authentication.

REGULATORY REQUIREMENT:
The introduction of WPA2 was in line with the IEEE 802.11i security standard, which was mandated for all Wi-Fi devices starting in 2006. WPA2 was required for compliance with new security regulations.

ADVANCED SECURITY FOR ENTERPRISE NETWORKS:
WPA2 provided stronger security features for enterprise networks by supporting 802.1X for user authentication and offering stronger encryption, making it ideal for large-scale networks.

Q6. What is the role of the Pairwise Master Key (PMK) in the 4-way handshake?

I have listed the step and the PMK's role in the 4-way handshake in the following table.

STEPS	DESCRIPTION
1. AP sends Message 1 to Client (supplicant)	The access point (AP) sends a message containing a nonce (random number) to the client. This is part of the process to ensure that the session keys are unique for each session.
2. Client sends Message 2 to AP	The client responds with its own nonce and an Message Integrity Code (MIC) based on the PMK and the previously received nonce from the AP. This message also confirms that the client has the correct PMK.
3. AP sends Message 3 to Client	The AP sends a message back to the client with a MIC and other parameters needed to establish the session. This is to confirm the client's identity and validate that both the AP and client have the correct PMK and are authorized to communicate securely.

4. Client sends Message 4 to AP	The client sends an acknowledgment to the AP, confirming the completion of the 4-way handshake. This step completes the secure connection establishment process.

USAGE OF PMK IN 4-WAY HANDSHAKE:

- The PMK is derived from the pre-shared key (PSK) in WPA2-PSK mode or from a more complex process involving 802.1X/EAP authentication in WPA2-Enterprise mode.
- The PMK is never directly transmitted between the AP and client, but both parties generate the same PMK using a shared password or certificate, ensuring mutual trust.
- The PMK is used to derive the Pairwise Transient Key (PTK), which is the actual encryption key used to encrypt the data traffic between the client and AP.
- The PTK is generated by combining the PMK with other elements like the AP and client's nonces and MAC addresses.
- The MIC is used in the 4-way handshake to ensure that the messages are not tampered with.
- The MIC is derived from the PMK and ensures that both the AP and client are using the correct session key material and have not been impersonated by attackers.

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

- The 4-way handshake ensures mutual authentication between the client (supplicant) and the access point (AP) by verifying that both parties have the correct shared secrets (e.g., Pairwise Master Key (PMK), which is derived from the pre-shared key or through 802.1X authentication).
- Mutual authentication means that both the client and the AP confirm each other's identity, ensuring that neither party is an imposter.

STEPS	**ACTION**
1.AP sends Message 1	The AP (access point) sends a nonce (random number) to the client. This nonce will be used in subsequent steps for key generation.
2.Client sends Message 2	The client responds with its nonce, a Message Integrity Code (MIC), and a confirmation that it has the correct PMK.
3.AP sends Message 3	The AP confirms that it also has the correct PMK by generating a MIC and sending it to the client. The AP also includes its nonce in this message.
4.Client sends Message 4	The client sends a final acknowledgment to the AP. This confirms that the handshake has completed successfully and that both the client and AP have established a secure session.

Q8. What will happen if we put a wrong passphrase durng a 4-way handshake?

BEFORE HANDSHAKE STARTS:
The client will still associate with the access point (AP).

DURING THE 4-WAY HANDSHAKE:
The handshake **fails** at the **Message Integrity Code (MIC)** validation step.

AFTER FAILURE:

- The AP discards the handshake.
- The client sees an error like "Incorrect Password" or "Authentication Failed".
- The client may retry the handshake a few times, and then give up or show a connection failure.

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

UNAUTHORIZED USERS CONNECTING TO THE NETWORK:
Solution: Authentication before access
802.1X forces every device/user to authenticate (e.g., with username/password, certificate) before granting network access.

NO USER/DEVICE VERIFICATION:
Solution: Identity verification using RADIUS and EAP
802.1X uses authentication servers (like RADIUS) to verify if the user/device is allowed to access the network.

OPEN ETHERNET PORTS ARE SECURITY RISKS:
Solution: Port-based access control
802.1X locks the Ethernet (or Wi-Fi) port and only unlocks it after successful authentication. If authentication fails, no access is given.

ANYONE CAN PLUG IN AND GET NETWORK ACCESS:
Solution: Dynamic port blocking
Switches/Wireless Access Points (called "Authenticators") block traffic from a port until authentication succeeds.

MANUAL ACCESS CONTROL IS HARD TO MANAGE (ESPECIALLY WITH MANY DEVICES):
Solution: Centralized authentication (AAA server)
Instead of configuring every switch manually, 802.1X relies on centralized RADIUS servers to handle who can/cannot access.

NO WAY TO ASSIGN DIFFERENT PERMISSIONS TO DIFFERENT USERS:
Solution: Role-based network access
Based on authentication, 802.1X can assign VLANs or access rights (example: guests vs. employees).

DIFFICULTY DETECTING ROGUE DEVICES:
Solution: Authentication logs and auditing
After authentication, different security policies (like firewall rules, VLAN assignments) can be automatically applied.

NO PROTECTION FOR WIRELESS NETWORKS AGAINST UNAUTHORIZED CONNECTIONS:
Solution: Wireless 802.1X (WPA2-Enterprise/WPA3-Enterprise)
In Wi-Fi, 802.1X ensures that only authenticated users can connect, protecting against Wi-Fi freeloaders and attacks.

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

User/Device Authentication:
Instead of a single shared Wi-Fi password, each user/device must authenticate individually with unique credentials (e.g., username/password, certificate).

Individual Credentials:
802.1X uses individual user accounts, so if someone leaves the organization, you can simply disable their account without changing Wi-Fi passwords for everyone.

Dynamic Session Keys:
802.1X dynamically generates unique encryption keys for each session after authentication, preventing key reuse or guessing.

Per-Session Encryption:
After successful authentication, a unique Pairwise Master Key (PMK) and encryption keys are derived for every client, protecting data even if others are nearby.

User Identity Logging:
Authentication attempts (success and failure) are logged on the authentication server, so you can track who connected and when.

Dynamic VLAN Assignment:
802.1X can assign different users/devices to different VLANs automatically after authentication (e.g., staff vs. guest vs. IoT).

Centralized Access Control:
Admins can quickly revoke access by disabling accounts on the authentication server, no need to change network configurations.

Scalable Authentication Framework:
802.1X scales easily to hundreds or thousands of users by using RADIUS servers, certificates, and identity-based policies.