Wi-Fi Security Assignment

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

Authentication is the process of verifying that a device or user is who they claim to be before granting access to the network.

Encryption involves securing the data transmitted between devices and access points, ensuring that it cannot be intercepted or read by unauthorized parties.

Integrity ensures that the data has not been altered or tampered with during transmission, maintaining its accuracy and trustworthiness.

Access control is the practice of managing who is allowed to connect to the network and specifying what resources they can access, ensuring proper security and resource management.

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

Authentication and Encryption in Wi-Fi Networks

Authentication is a fundamental security process used to confirm the identity of a user or device attempting to access a wireless network. In the context of Wi-Fi, authentication mechanisms ensure that only authorized users are permitted to connect. This verification process can involve the use of a pre-shared key (PSK), where users must enter a known password, or more advanced methods such as certificate-based authentication typically found in enterprise environments, where credentials like digital certificates or usernames and passwords are used.

Encryption, on the other hand, is the method of protecting data by converting it into a coded format during transmission. This ensures that even if the wireless communication is intercepted, the data remains unintelligible to unauthorized parties. Only devices that possess the correct decryption key can decode and access the original information. Encryption plays a critical role in safeguarding the privacy and integrity of data transmitted over Wi-Fi networks.

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

Feature	WEP	WPA	WPA2	WPA3
Full form	Wired Equivalent Privacy	Wi-Fi Protected Access	Wi-Fi Protected Access II	Wi-Fi Protected Access III

Year introduced	1997	2003	2004	2018
Encryption	RC4 (weak)	TKIP (temporary fix)	AES-CCMP (strong)	AES-GCMP (stronger)
Key Management	Static	Dynamic	Dynamic	Dynamic with improved protections
Vulnerabilities	Easily crackable	Still vulnerable (but harder than WEP)	Secure (with strong password)	Very secure, resistant to offline attacks
Authentication	Shared Key	802.1X / PSK	802.1X / PSK	Simultaneous Authentication of Equals (SAE)

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

Wired Equivalent Privacy (WEP), once a standard for securing wireless networks, is now widely regarded as highly insecure due to multiple technical weaknesses in its design and implementation.

One of the primary flaws in WEP lies in its weak encryption mechanism. It relies on the RC4 stream cipher and supports only short key lengths—either 40-bit or 104-bit—which are insufficient by modern cryptographic standards. These keys can be broken in a matter of minutes using readily available tools, posing a significant risk to network security.

Another critical issue with WEP is its use of static encryption keys. Since these keys remain unchanged during communication, an attacker who captures enough data packets can analyze the traffic and eventually deduce the encryption key. This vulnerability is further exacerbated by WEP's use of 24-bit Initialization Vectors (IVs), which are too short and often reused. The repeated use of IVs introduces patterns in encrypted data, making it easier for attackers to perform statistical analysis and break the encryption.

Moreover, WEP is susceptible to numerous well-known exploits. Tools such as Aircrack-ng can automate the process of capturing packets and cracking WEP keys, making even novice attackers capable of breaching WEP-secured networks with minimal effort.

In comparison, more modern protocols like WPA2 have addressed these vulnerabilities by introducing dynamic key generation and adopting the AES-CCMP encryption algorithm, which offers far greater security. These enhancements make it significantly more difficult for attackers to decrypt traffic or gain unauthorized access to a network.

Due to its inherent weaknesses, WEP is no longer recommended for use and has been officially deprecated in favor of more secure alternatives.

5. Why was WPA2 introduced?

Wi-Fi Protected Access II (WPA2) was developed as a robust security protocol to overcome the critical vulnerabilities present in earlier standards such as WEP and WPA. Introduced in 2004, WPA2 became the mandatory security protocol for all Wi-Fi-certified devices from 2006 onwards, providing a significantly more secure and reliable framework for wireless communication.

One of the key improvements in WPA2 is its adoption of Advanced Encryption Standard (AES) for data encryption. Unlike the outdated RC4 algorithm used in WEP and the transitional TKIP mechanism in WPA, AES provides a much stronger and modern encryption method, making it highly resistant to brute-force and cryptographic attacks.

In addition to stronger encryption, WPA2 enhances data integrity through the use of CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). This protocol ensures that data has not been altered during transmission by providing robust integrity checking mechanisms alongside encryption. CCMP is considered far more secure than the Message Integrity Check (MIC) used in previous protocols.

WPA2 also aligns with strict security compliance requirements, making it suitable for enterprise and government-level deployments. By incorporating features such as 802.1X authentication for enterprise networks, it ensures that access control is based on strong, identity-based mechanisms.

Moreover, WPA2 was designed with future-proofing in mind. As cybersecurity threats continued to evolve, WPA2 provided a resilient foundation capable of withstanding many sophisticated attacks, especially when used with strong passwords and proper configuration.

In summary, WPA2 was introduced not just as a temporary enhancement, but as a long-term, reliable solution for securing Wi-Fi networks. Its combination of robust encryption, improved integrity checks, and regulatory compliance established it as the gold standard for wireless security for many years.

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

Role of the Pairwise Master Key (PMK) in the 4-Way Handshake

In WPA and WPA2 wireless security protocols, the Pairwise Master Key (PMK) serves as a foundational element in the authentication and encryption process, particularly during the execution of the 4-way handshake. The PMK is a shared secret that is either derived from a passphrase in WPA/WPA2-PSK (Pre-Shared Key) mode or obtained from an authentication server, such as a RADIUS server, in WPA/WPA2-Enterprise deployments.

During the 4-way handshake, the client device (known as the *supplicant*) and the access point (referred to as the *authenticator*) both possess the PMK. Using this shared key, they generate a unique session key known as the Pairwise Transient Key (PTK). This session key is constructed using the PMK along with other values exchanged during the handshake, such as nonces and MAC addresses, ensuring the resulting key is unique to each session.

The PTK is then used to secure the data transmission between the client and the access point by providing encryption and message integrity. In essence, the PMK functions as the root secret from which all further encryption keys are derived, playing a critical role in maintaining the confidentiality and integrity of wireless communication.

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

Mutual Authentication in the 4-Way Handshake

The 4-way handshake is a critical process in WPA and WPA2 security protocols that facilitates mutual authentication between a wireless client and an access point. Its primary purpose is to verify that both parties possess the correct Pairwise Master Key (PMK)—the shared secret—without ever transmitting the PMK directly over the air, thereby maintaining security.

The handshake begins with Message 1, in which the access point (AP) sends a randomly generated number known as the ANonce (Authenticator Nonce) to the client. In Message 2, the client replies with its own random number, called the SNonce (Supplicant Nonce), and includes a cryptographic message integrity code based on the PMK and the two nonces.

Upon receiving this message, the access point uses the provided information to calculate a cryptographic value and compares it with the one received from the client. If they match, it confirms that the client possesses the correct PMK. In Message 3, the AP sends its own cryptographic confirmation to the client. The client, in turn, performs a similar verification. If successful, it proves that the AP also possesses the correct PMK.

Through this carefully coordinated exchange, both the client and the access point verify each other's identity and establish a shared Pairwise Transient Key (PTK), which will be used to encrypt and authenticate all subsequent data. Importantly, this entire process avoids transmitting the actual PMK, thereby protecting the connection from eavesdropping and impersonation attacks.

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

When a wrong passphrase is entered during the authentication process in WPA or WPA2 networks, the 4-way handshake fails due to a mismatch in the derived cryptographic keys. Specifically, the client uses the entered passphrase to generate the Pairwise Master Key (PMK). If the passphrase is incorrect, the resulting PMK will not match the one generated by the access point (AP), which uses the correct passphrase configured on the network.

During the handshake, both the client and the AP calculate a Message Integrity Code (MIC) using their respective PMKs as part of verifying each other's identity. If the PMKs do not match, the MICs will also differ. The AP detects this mismatch and immediately aborts the handshake process, refusing to authenticate the client.

As a result, the client is unable to complete the handshake and is denied access to the network. This mechanism ensures that only users with the correct credentials can successfully establish a secure connection.

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

Role of 802.1X in Network Security

The 802.1X standard is a network access control mechanism that addresses several key challenges in securing wired and wireless networks, particularly in large-scale environments such as enterprises, educational institutions, and government organizations. It plays a vital role in enhancing security by enabling user-based authentication before granting access to network resources.

One of the primary problems that 802.1X solves is the ability to control network access based on user identity. Unlike traditional systems that rely on a shared password (as in WPA-PSK), 802.1X uses an

authentication server—typically a RADIUS server—to verify each user or device individually. This ensures that only authorized users or devices are granted network access.

Another major advantage of 802.1X is that it separates the authentication process from the encryption mechanism. This separation allows for more flexible and secure network configurations. Once a user is authenticated, the system can dynamically generate unique encryption keys for that session. This approach significantly reduces the risk of key compromise compared to using static or shared keys.

Furthermore, 802.1X supports identity-based access control, enabling network administrators to enforce security policies based on specific users or groups. This granular level of control is essential in environments with large numbers of users, where managing and securing shared credentials would be both insecure and impractical.

In summary, 802.1X is a powerful framework that enhances network security by offering scalable, user-specific authentication, secure key management, and identity-based access control—making it particularly suitable for enterprise-level deployments.

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

How 802.1X Enhances Wireless Security

802.1X significantly strengthens the security of wireless networks by addressing several vulnerabilities associated with traditional shared password-based systems. Rather than relying on a single passphrase for all devices (as in WPA-PSK), 802.1X uses unique credentials—such as usernames, digital certificates, or smart cards—making the authentication process more secure and individualized. This ensures that each user or device is authenticated based on their identity rather than a shared key.

Another key benefit of 802.1X is its ability to authenticate each user or device separately through an authentication server, typically a RADIUS (Remote Authentication Dial-In User Service) server. This process ensures that only authorized users and devices can access the network, reducing the likelihood of unauthorized access.

In addition to user authentication, 802.1X enables dynamic generation of encryption keys for each session. By creating unique encryption keys on a per-session basis, it mitigates the risk of session hijacking or eavesdropping, as any intercepted key would only be useful for the duration of that specific session.

802.1X also supports stronger authentication protocols, such as EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), which utilizes digital certificates for authentication, further enhancing security by providing robust encryption and identity verification.

Furthermore, 802.1X makes it difficult for rogue devices to connect to the network. This helps prevent Man-in-the-Middle (MitM) attacks and the creation of rogue access points (APs), which are common threats to Wi-Fi networks. By requiring devices to authenticate before establishing a connection, 802.1X significantly reduces the risk of such attacks.

In summary, 802.1X provides enterprise-grade security for Wi-Fi networks, offering advanced authentication, dynamic key management, and enhanced protection against unauthorized access and network-based attacks.