Laud Mills

Part A: Wireless security protocols

1. Discuss the WEP protocol regarding the points below

* Encryption algorithm
* Authentication technique
* Strengths
* Weaknesses
* Documented attack types

Wired Equivalent Privacy (WEP) is an outdated security protocol designed to secure wireless local area networks (WLANs) by providing a level of security comparable to wired networks. WEP uses the RC4 stream cipher for encryption, with key lengths of 40-bit or 104-bit and a 24-bit Initialization Vector (IV). The encryption process combines the secret key with the IV to generate a key stream, which is XORed with the data. WEP offers two authentication methods: Open System Authentication – No security and allows devices with the SSID to connect. Shared Key Authentication, which requires knowledge of the shared key but remains vulnerable to attacks due to weak challenge-response mechanisms.

Strengths:

* Simple to implement.
* Widely supported by devices.

Weaknesses:

* Weak encryption: RC4 and short IVs (24 bits) make key recovery possible through statistical analysis.
* Lack of key rotation: Keys do not change automatically and this increases exposure.
* Weak authentication: Susceptible to brute force and dictionary attacks.

Documented Attacks:

* FMS Attack: Exploits weaknesses in RC4 to recover the key.
* IV Collision: Repeated IVs allow attackers to derive the encryption key.
* Brute-Force & Dictionary Attacks: Exploit weak key lengths for faster key recovery.

1. Repeat the previous step for the WPA protocol

Wi-Fi Protected Access (WPA) is a security protocol designed to address the vulnerabilities of WEP and improve the overall security of wireless local area networks (WLANs). WPA introduced stronger encryption and authentication mechanisms to safeguard wireless communications. WPA uses the Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES) for encryption, depending on the WPA version: WPA-TKIP: Uses a dynamic 128-bit key for each packet and provides message integrity, improving upon WEP’s static key issues. WPA supports two authentication modes, Pre-Shared Key (PSK) – A shared passphrase is used for authentication, suitable for home networks.

Enterprise Mode – Involves a more complex system with a RADIUS server for user-based authentication, which is much ideal for corporate environments.

Strengths:

* Improved encryption: TKIP and AES offer much stronger protection than WEP.
* Dynamic key management: WPA regularly changes encryption keys, reducing the risk of key compromise.
* Message integrity: WPA includes mechanisms to ensure the integrity of data packets.

Weaknesses:

* While stronger than WEP, TKIP is still susceptible to certain attacks.
* If a weak passphrase is used, WPA-PSK is vulnerable to brute-force attacks.

Documented Attacks:

* Dictionary & Brute-Force Attacks (WPA-PSK): Weak passphrases can be cracked using large dictionaries or brute-force methods.
* KRACK Attack Exploits vulnerabilities in the WPA handshake, allowing attackers to decrypt traffic on affected networks.

3 Repeat the previous step for the WPA2 protocol

Wi-Fi Protected Access 2 (WPA2) is an advanced security protocol designed to provide robust protection for wireless local area networks (WLANs). It is the successor to WPA and significantly improves security by using stronger encryption algorithms and more secure key management mechanisms. WPA2 exclusively uses Advanced Encryption Standard (AES) for encryption, offering stronger security compared to WPA's TKIP. WPA2 supports two authentication modes:

Pre-Shared Key (PSK) – A shared passphrase is used for authentication in home networks, like WPA-PSK. Enterprise Mode – Involves RADIUS server authentication, ideal for larger organizations, providing more granular user access control.

Strengths:

* AES encryption: AES is more secure than TKIP, providing strong data protection and resistance to attacks.
* Stronger key management: WPA2 uses more sophisticated mechanisms for key generation, distribution, and management.
* Better message integrity: WPA2 ensures data integrity and authenticity with robust algorithms.

Weaknesses:

* WPA2-PSK vulnerabilities: If a weak passphrase is chosen, WPA2-PSK is susceptible to brute-force or dictionary attacks.
* Implementation flaws: Poorly configured networks or weak password policies can still leave WPA2 vulnerable.
* KRACK attack: A vulnerability in the WPA2 handshake protocol allows attackers to intercept and decrypt data.

Documented Attacks:

* Dictionary & Brute-Force Attacks (WPA2-PSK): Weak passwords are still vulnerable to offline dictionary or brute-force attacks.
* KRACK Attack: The Key Reinstallation Attack (KRACK) exploits a flaw in the WPA2 protocol's 4-way handshake, allowing attackers to intercept and decrypt traffic.

4 What is your conclusion? Which of the protocols above is best for modern wireless networks?

In conclusion, I would say one must avoid the use of the WEP protocol because it is outdated and has much attack surface with no inherent security that stands the test of time. For home networks and systems that do not support huge assets in such a large scale, the use of the WPA could be a better alternative to the WEP. Above all these, the WPA2 stands tall in terms of security and technology. In considering these three technologies vis a vis the Cyber Security triad of Confidentiality, Integrity and Availability, it would be very important to choose WPA2 as a much rubust technology against WEP and WPA. It is also instructive to consider the issue of better configurations as well as the use of recommended password regimes to make WPA2 serve its proper purpose as a better option.

Part B: Wireless infrastructure & security

1. Explain the difference between ad hoc and infrastructure modes in wireless networking.

Ad hoc mode is a decentralized wireless network where devices communicate directly with each other without the need for a central access point. It is commonly used for temporary, peer-to-peer connections in small-scale environments. In contrast, infrastructure mode relies on a central access point (AP) that manages communication between devices and may provide internet connectivity. This mode is widely used in larger, more structured networks, offering greater range, scalability, and security. The choice between ad hoc and infrastructure mode depends on the network's size, purpose, and required reliability.

1. What is an SSID? What security risks are associated with it? How do you protect against these risks?

An SSID (Service Set Identifier) is a unique name assigned to a wireless network, used to identify and distinguish it from other nearby networks. By default, most access points broadcast their SSID, making the network visible to devices within range. However, this can pose security risks, such as unauthorized access, eavesdropping, and the creation of rogue access points (Evil Twin attacks), where attackers impersonate legitimate networks to steal sensitive data. To mitigate these risks, it is recommended to disable SSID broadcasting, use strong encryption methods like WPA2 or WPA3, and create a unique SSID that is difficult to guess. Additionally, enabling MAC address filtering and regularly monitoring network activity can help prevent unauthorized access. These measures enhance network security and reduce the likelihood of attacks.

1. What is aircrack-ng? What functionalities does it offer? List five individual utilities which are available within aircrack-ng.

Aircrack-ng is a comprehensive suite of tools designed for wireless network auditing and penetration testing, primarily used to assess the security of Wi-Fi networks. It focuses on identifying vulnerabilities in wireless encryption protocols like WEP and WPA. The suite offers various functionalities, including packet sniffing, cracking WEP/WPA keys, network monitoring, replay attacks, and de authentication attacks. These features allow users to test network strength and identify weaknesses that could be exploited by attackers.

Some of the key utilities within Aircrack-ng include

Airmon-ng (for enabling monitor mode on wireless interfaces)

Airodump-ng (for packet capturing and network monitoring)

Aircrack-ng (for cracking WEP/WPA keys)

Aireplay-ng (for packet injection and attack execution)

Airdecap-ng (for decrypting captured files).

1. What is airodump-ng? What parameters does it capture? Give an example of a command.

Airodump-ng is a tool within the Aircrack-ng suite used for monitoring and capturing wireless packets from nearby Wi-Fi networks. It operates in monitor mode, enabling it to capture critical information such as the network's BSSID, SSID, channel, encryption type, and connected clients. This tool is especially useful for capturing WPA/WPA2 handshakes, which are essential for cracking Wi-Fi passwords. Airodump-ng can also provide data on signal strength and network traffic.

An example command to run Airodump-ng would be:

airodump-ng wlan0mon

where wlan0mon is the interface in monitor mode. It helps with network analysis and security assessments.