Answers for session 4a - Various Wi-Fi Security Protocols

1.If we are sending MPDU packets, that means many IVs should be there right ?Then why are we sending only one IV to the end side to decrypt all packets??

When sending MPDU (MAC Protocol Data Unit) packets in wireless communication, each packet typically has its own Initialization Vector (IV) for security purposes, especially in encryption protocols like WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access). The purpose of using unique IVs for each packet is to enhance security by preventing certain types of attacks and ensuring that each packet is encrypted differently.

However, it seems there might be a misconception in your question. In standard practice, each packet is not decrypted using just one IV for all packets. Instead, a key point in the security of these protocols is the use of unique IVs for each packet. Reusing the same IV for multiple packets weakens the security, as it can lead to vulnerabilities and compromise the encryption.

In summary, multiple unique IVs are used in wireless communication to enhance security by encrypting each packet differently. Reusing the same IV for all packets would be a security risk and is generally not a standard practice in modern wireless security protocols.

2.What is the main use of FCS ?

In wireless communication, the main use of FCS (Frame Check Sequence) is to detect errors in data frames as they are transmitted over the air. This is crucial for maintaining data integrity and ensuring reliable communication. FCS is a type of error-detecting code that is calculated for each frame of data before transmission. The receiver then recalculates the FCS based on the received data and compares it to the transmitted FCS. If the two values match, it indicates that the frame has been received without errors. If the values do not match, it indicates that an error has occurred, and the frame will be discarded.

3.What is the main difference between MIC and TKIP ?

The main difference between MIC (Message Integrity Check) and TKIP (Temporal Key Integrity Protocol) lies in their functions within wireless security protocols:

MIC (Message Integrity Check):

- Function: MIC is responsible for ensuring the integrity of the data during transmission.
- Purpose: It provides a way to detect if the data has been tampered with or altered during its journey across the network.
- Usage: Typically used in WPA2 (Wi-Fi Protected Access 2) and WPA3 to enhance data integrity.

TKIP (Temporal Key Integrity Protocol):

- Function: TKIP is a key management protocol designed to address vulnerabilities in the WEP (Wired Equivalent Privacy) protocol.
- Purpose: It dynamically generates unique encryption keys for each data packet, addressing the weaknesses of static WEP keys.
- Usage: Primarily used in WPA (Wi-Fi Protected Access) as a temporary solution before the adoption of more secure protocols like WPA2.

In summary, MIC focuses on ensuring the integrity of the transmitted data, while TKIP is a key management protocol that dynamically generates unique keys to address security vulnerabilities. Both are components of wireless security protocols designed to enhance the overall protection of Wi-Fi networks.

4.Is wpa3 unhackable ??

No, WPA3 (Wi-Fi Protected Access 3) is not considered "unhackable." While it represents a significant improvement over its predecessors (WPA and WPA2) in terms of security features, it does not guarantee absolute invulnerability. Cybersecurity is an evolving field, and new vulnerabilities or attack methods may emerge over time.

5.Does WPA -3 support windows/MAC, android etc?

Operating System	WPA3 Support

Windows 10 May 2019 Update (version 1903) or later	Yes
macOS Catalina (version 10.15) or later	Yes
Android 10 or later	Yes
iOS 13 or later	Yes

6.Is it also possible with WPA3?

The demo we showed is not possible with WPA3, we cant decrypt the password though we have the 4 way handshake captured because This is because the PMK (Pairwise Master Key) is not derived from the PTK (Pairwise Transient Key) specific to each client. In this scenario, the PMK is generated through the dragonfly handshake, resulting in a unique key for each client. Consequently, cracking the password via this approach proves challenging.