WPA/WPA2

What is it?

A Wi-Fi standard that was designed to improve upon the security features of WEP. The technology is designed to work with existing Wi-Fi products that have been enabled with WEP.

Improvements when compared to WEP

- Improved data encryption through the temporal key integrity protocol (TKIP)
    - TKIP scrambles the keys using a hashing algorithm and ensures that the key have not been tampered with through the integrity-checking feature.
- User authentication, which is generally missing in WEP, is also added through the extensible authentication protocol (EAP).
    - EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.
    - WEP on the other hand regulates access to a wireless network based on the hardware-specific MAC address, which is relatively simple to sniff out

WPA vs WPA2

WPA2 is the security method added to WPA that provides a stronger data protection and network access control.

Attack

Attack is carried out using key reinstallation attacks (KRACKs) when the attacker is within the range of the victim

- attacker can read data that is encrypted → able to read sensitive information

Affects all modern protected Wi-Fi network

The attack is targeted against the 4-way handshake of the WPA/WPA2 protocol

Basic process when joining the client joins the network

- when a client joins the network, it executes the 4-way handshake to negotiate a fresh encryption key. It will install the key after receiving message 3 of the 4-way handshake
- Once the key is installed, it will be used to encrypt data frames using an encryption protocol

Attack technique

- adversary tricks a victim into reinstalling an already-in-use key
    - this can be done by manipulating and relaying cryptographic handshake message
- when the victim reinstalls the key, associated parameters such as the incremental transmit packet number and receive packet number are reset to their initial value. This means that the same key is only used once. However, this is not the case for WPA/WPA2

Attack point

- when the client does not receive the 3rd message, the Access Point(AP) will retransmit the 3rd message if it did not receive an appropriate response.
    - This would mean that the client would receive multiple message 3 and each time the key is received , it is being reinstalled .
        - This reset the incremental transmit packet number and receive replay counter used by the encryption protocol.
- By forcing the transmit packet number reuse in this manner, the encryption protocol can be attacked
    - This can be done by simply forcing these transmit packet number resets by collecting and replaying retransmission of message 3 of the 4-way handshake

Impact

- Packets can be intercepted, passwords and cookies can be stolen for further attacks
- Keys would be reuse due to the value of transmit packet number being reset to their initial value
    - Easier to decrypt information
- Ability to decrypt TCP SYN packets —> hijack TCP connections
- Ability to forge and inject packets if the victim uses WPA-TKIP or GCMP encryption instead of AES-CCMP
    - GCMP uses the same authentication key in both communication directions and this key can be recovered if the transmit packet number is reuse

Reference:

https://papers.mathyvanhoef.com/ccs2017.PDF
https://www.webopedia.com/TERM/W/WPA2.html