In WPA 2 first, the access point sends a random number (ANonce) to the client. The client creates its own random number (SNonce). Next, using the Pre-Shared Key (PSK) and both nonces, the client derives the Pairwise Transient Key (PTK). Then it will send the SNonce and a Message Integrity Code (MIC) to the AP (to prove it knows the PSK). Third, the AP also derives the same PTK using the PSK, ANonce, and SNonce. It sends the Group Temporal Key (GTK) (used for broadcast traffic), encrypted with the PTK, and another MIC. Finally, the client sends a final confirmation message. Now, both clients and AP have the same keys and can start encrypted communication.

The handshakes seem secure but unfortunately are broadcast in a way that any device can listen to. If an attack can capture the entire process, then they have access to generate a hash and only need to acquire the PSK. The attacker can use a brute force attack to generate the hashes of a library of passwords then use a matching one to authenticate on the network.

There are two main attacks leveraged against this security protocol Group key decryption and KRACK. These attacks target traffic encryption and session integrity, but they don’t compromise the key used to authentication to the access point.

KRACK is the key reinstallation attacks which read information that was previously assumed to be safely encrypted. This attack specifically can be used to help inject and manipulate data in transit. First, the attacker captures and replays Message 3 of the handshake multiple times. Second, each time the client receives Message 3, it reinstalls the same encryption key (PTK). Third, every key installation resets the internal packet counters (nonce, replay counter) used by the encryption protocol (CCMP). Fourth, because the counters reset, packets can be replayed or encryptedunder the same key, violating WPA2’s core security guarantee. Firth, this allows the attacker to Decrypt packets (passively), Replay old data packets, Inject malicious data (in some cases, especially on Android/Linux clients)

WPA3 fixes the KRACK vulnerability by replacing the flawed four-way handshake used in WPA2. Using a more secure authentication method called Simultaneous Authentication of Equals (SAE), also known as Dragonfly. Unlike WPA2, where the same encryption key could be reinstalled if handshake messages were replayed, SAE establishes a new, unique session key for every connection attempt using a Diffie-Hellman–based key exchange. This process is resistant to key reinstallation because the key derivation is tied to a mutual, one-time negotiation rather than dependent on message retransmissions. SAE also eliminates offline dictionary attacks by requiring real-time interaction with the access point for each password guess, meaning an attacker cannot simply capture a handshake and brute force the password later. Just like with deauthentication/disassociation being on a newer standard is imperative to mitigating these well-known attacks.

References

<https://blogs.dsu.edu/digforce/2023/07/11/penetrating-networks-by-cracking-wpa2/>

<https://outpost24.com/blog/wps-cracking-with-reaver/>

<https://www.fortinet.com/blog/business-and-technology/wpa2-has-been-broken-what-now>

<https://cyberhub.sa/posts/5658>

<https://www.krackattacks.com/>

<https://en.wikipedia.org/wiki/KRACK>

<https://medium.com/@alonr110/the-4-way-handshake-wpa-wpa2-encryption-protocol-65779a315a64>