CERT-EU Security Advisory 2017-021

KRACK – Key Reinstallation Attacks: Breaking WPA2

October 17, 2017 — v1.0

History:

- *17/10/2017 — v1.0: Initial publication*

Summary

Researchers in the KU Leuven University have discovered a serious weaknesses in WPA2, a protocol that secures all modern protected Wi-Fi networks. An attacker within the range of the Wi-Fi of the victim can exploit these weaknesses using key reinstallation attack (KRACK). Attackers can use this attack to read information that was previously assumed to be safely encrypted.

Attacks may include:

- arbitrary packet decryption and injection,
- TCP connection hijacking,
- HTTP content injection,
- replay of unicast and group-addressed frames

The weakness was discovered in the Wi-Fi standard itself, and so all implementations of WPA and WPA2 are likely to be affected. The weakness was found in the 4-way handshake that all protected Wi-Fi networks use to generate a fresh session key. The adversary can trick a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying handshake messages. When reinstalling the key, associated parameters, such as the incremental transmit packet number (nonce) and receive packet number (replay counter) are reset to their initial value. The attack also breaks the PeerKey, group key, and Fast BSS Transition (FT) handshake. The impact depends on the handshake being attacked, and the data-confidentiality protocol in use.

Technical Details

The attack exploits a vulnerability found in the 4-way handshake of the WPA2 protocol.

4-Way Handshake

The Wi-Fi Alliance refers to their approved, interoperable implementation of the full 802.11i as WPA2, also called RSN. This standard specifies security mechanisms for wireless networks is IEEE 802.11i-2004, or 802.11i for short, and it is an amendment to the original IEEE 802.11, implemented as Wi-Fi Protected Access II (WPA2). IEEE 802.11i provides a Robust Security Network (RSN)[1] with two new protocols: the 4-Way Handshake and the Group Key Handshake [4].

The initial authentication process is carried out either using a pre-shared key (PSK), or following an EAP exchange through 802.1X (known as EAPOL, which requires the presence of an authentication server). This process ensures that the client station (STA) is authenticated with the access point (AP). After the PSK or 802.1X authentication, a shared secret key is generated, called the Pairwise Master Key (PMK). The PSK is derived from a password that is put through PBKDF2-SHA1 as the cryptographic hash function. In a pre-shared-key network, the PSK is actually the PMK. If an 802.1X EAP exchange was carried out, the PMK is derived from the EAP parameters provided by the authentication server.

The 4-way handshake is designed so that the access point (AP) (or authenticator) and wireless client (or supplicant STA) can independently prove to each other that they know the PSK/PMK, without ever disclosing the key. The 4-way handshake is critical for protection of the PMK from malicious access points. The PMK is designed to last the entire session and should be exposed as little as possible; therefore, keys to encrypt the traffic need to be derived. A four-way handshake is used to establish another key called the Pairwise Transient Key (PTK). The PTK is generated by concatenating the following attributes: PMK, AP nonce (ANonce), STA nonce (SNonce), AP MAC address, and STA MAC address. The product is then put through a pseudo random function. The handshake also yields the GTK (Group Temporal Key), used to decrypt multicast and broadcast traffic.

The actual messages exchanged during the handshake are depicted in the figure and explained below (all messages are sent as EAPOL-Key frames):

Messages:

1. The AP sends a nonce-value to the STA (ANonce). The supplicant (client) now has all the attributes to construct the PTK.
2. The STA sends its own nonce-value (SNonce) to the authenticator (Access Point) together with a Message Integrity Code (MIC), including authentication, which is really a Message Authentication and Integrity Code (MAIC).
3. The AP constructs and sends the GTK and a sequence number together with another MIC. This sequence number will be used in the next multicast or broadcast frame, so that the receiving STA can perform basic replay detection.
4. The STA sends a confirmation to the AP.

[1] The RSN is a security network that only allows the creation of robust security network associations (RSNAs), which are a type of association used by a pair of stations (STAs) if the procedure to establish authentication or association between them includes the 4-Way Handshake

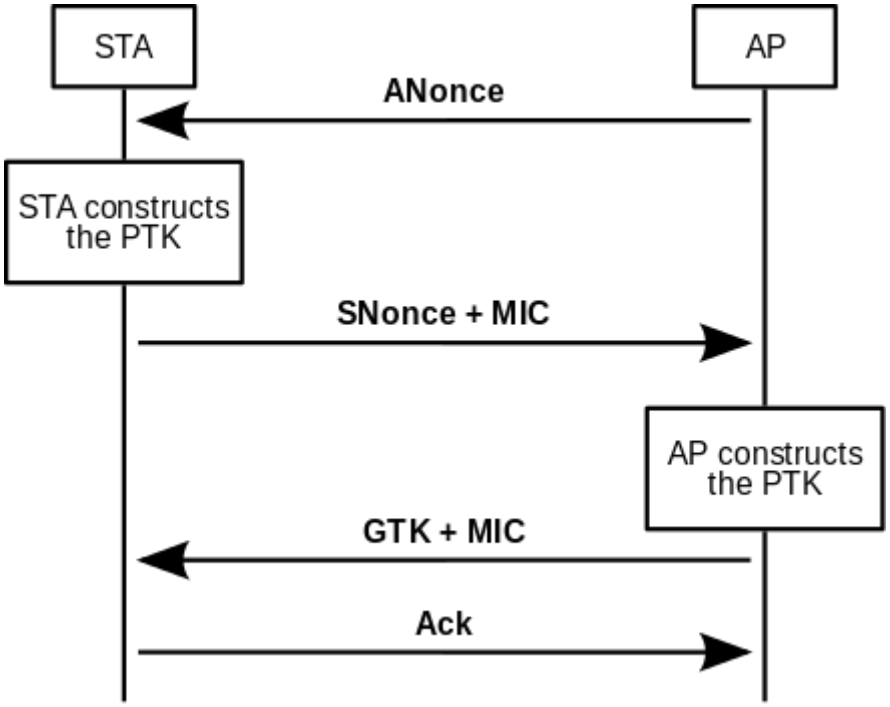

Figure 1: 4-way handshake

The Key Reinstallation Attack (KRACK)

As stated in the researchers' white paper [1], when first connecting to a network and starting the 4-way handshake (Figure 2), the supplicant (client) transitions to the PTK-INIT state (Figure 3). Here, it initializes the Pairwise Master Key (PMK). When receiving message 1, it transitions to the PTK-START stage. This may happen when connecting to a network for the first time, or when the session key is being refreshed after a previous (completed) 4-way handshake. When entering PTK-START, the supplicant generates a random SNonce, calculates the Temporary PTK (TPTK) and sends its SNonce to the authenticator using message 2. The authenticator will reply with message 3, which is accepted by the supplicant if the MIC and replay counter are valid. If so, it moves to the PTK-NEGOTIATING state, where it marks the TPTK as valid by assigning it to the PTK variable, and sends message 4 to the authenticator. Then, it immediately transitions to the PTK-DONE state, where the PTK and GTK are installed for usage by the data-confidentiality protocol using the MLME-SETKEYS.request primitive. Finally, it opens the 802.1x port such that the supplicant can receive and send normal data frames.

Note that the 4-way handshake as defined in the 802.11 standard explicitly takes into account retransmissions of either message 1 or 3, which occur if the authenticator did not receive message 2 or 4, respectively. These retransmissions use an incremented EAPOL replay counter.

The researchers abused the following properties of the protocol. First, 802.11i states that the AP retransmits message 1 or 3 if it did not receive a reply. Therefore, the client must handle retransmissions of message 1 or 3. Additionally, 802.11i states that the client should install the PTK after processing and replying to message 3.

Because the supplicant still accepts retransmissions of message 3, even when it is in the PTK-DONE state, the researchers forced a reinstallation of the PTK. More precisely, they first established a man-in-the-middle (MitM) position between the supplicant and authenticator. They used this MitM position to trigger retransmissions of message 3 by preventing message 4 from arriving at the authenticator. As a result, it will retransmit message 3, which causes the suppli-

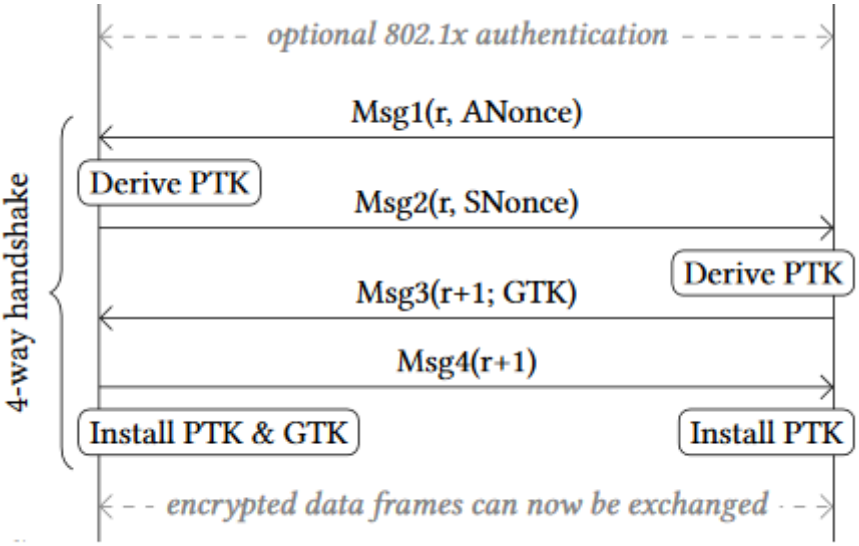

Figure 2: 4-way handshake starting messages

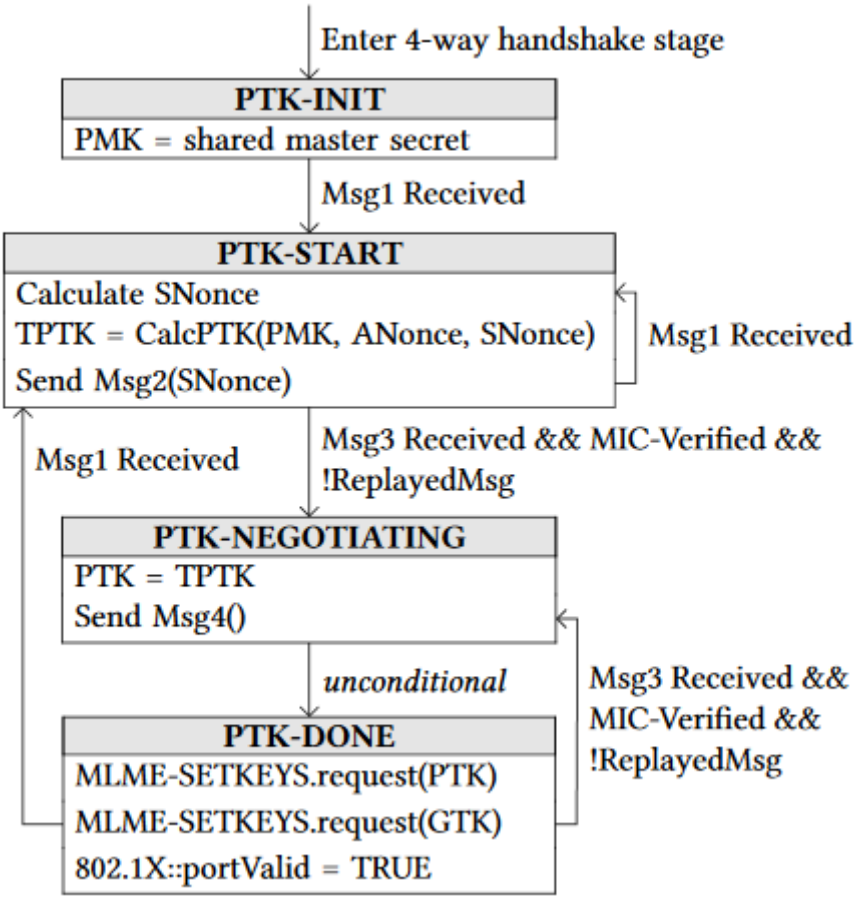

Figure 3: KRACK attack on the 4-way handshake

cant to reinstall an already-in-use PTK. In turn, this resets the nonce being used by the data-confidentiality protocol. Depending on which protocol is used, this allows an adversary to replay, decrypt, and/or forge packets.

Key reinstallation attack even occurs spontaneously if certain handshake messages are lost due to background noise. This means that under certain conditions, implementations are reusing nonces without an adversary being present.

Depending on the type of handshake being used between the nodes on the Wi-Fi network, the attack can do varying levels of damage [2]:

- For connections using AES and the Counter with CBC-MAC Protocol ((AES)-CCMP), an attacker can decrypt network packets, making it possible to read their contents and to inject malicious content into TCP packet streams. But the key itself cannot be broken or forged, so the attacker can't forge a key and join the network—instead, they have to use a "cloned" access point that uses the same MAC address as the access point of the targeted network, on a different Wi-Fi channel.
- For WPA2 systems using the Temporal Key Integrity Protocol (TKIP), the Message Integrity Code key can be recovered by the attacker. This allows them to replay captured packets to the network; they can also forge and transmit new packets to the targeted client posing as the access point. For devices that use the Galois/Counter Mode Protocol (GCMP), the attack is the worst since it is possible to replay and decrypt packets. Additionally, it is possible to recover the authentication key, which in GCMP is used to protect both communication directions [as client or access point] therefore, unlike with TKIP, an adversary can forge packets in both directions. That means that the attacker can essentially join the network and pretend to be a client or the access point, depending on the type of access they want. "Given that GCMP is expected to be adopted at a high rate in the next few years under the WiGig name, this is a worrying situation," the researchers noted.

Note: The attack is especially catastrophic against version 2.4 and above of *wpa_supplicant*, a Wi-Fi client commonly used on Linux. The client will install an all-zero encryption key instead of reinstalling the real key. This vulnerability appears to be caused by a remark in the Wi-Fi standard that suggests to clear the encryption key from memory once it has been installed for the first time. When the client now receives a retransmitted message 3 of the 4-way handshake, it will reinstall the now-cleared encryption key, effectively installing an all-zero key. Because Android uses wpa_supplicant, Android 6.0 and above also contains this vulnerability. This makes it trivial to intercept and manipulate traffic sent by these Linux and Android devices.

Products Affected

The vulnerability affects the core WPA2 protocol itself and is effective against devices running Android, Linux, and OpenBSD, and to a lesser extent macOS and Windows, as well as other types of devices.

Scripts to detect whether an implementation of the 4-way handshake, group key handshake, or Fast BSS Transition (FT) handshake is vulnerable to key reinstallation attacks are ready by the researchers but have not yet been published.

	Replay [c]	Decrypt [a]	Forge
4-way impact			
TKIP	AP → client	client→ AP	client→ AP [b]
CCMP	AP → client	client→ AP	
GCMP	AP → client	client→ AP	client↔ AP [b]
FT impact			
TKIP	client→ AP	AP → client	AP → client
CCMP	client→ AP	AP → client	
GCMP	client→ AP	AP → client	AP ↔ client [b]
Group impact			
any	AP → client [c]		

[a] With this ability, we can hijack TCP connections to/from an Internet endpoint and inject data into them.

[b] With this ability, we can use the AP as a gateway to inject packets towards *any* device connected to the network.

[c] This denotes in which direction we can replay unicast and group-addressed frames. For the group key handshake, only group-addressed frames can be replayed.

Figure 4: Different KRACK flavors

Recommendations

Since the vulnerability affects the core WPA2 protocol itself, the recommended solution is that all Wi-Fi devices, like routers, smartphones, tablets, and laptops should be updated (software and firmware) as soon as updates become available. Most vendors are or will be shortly providing specific advisories as to how these vulnerabilities may be patched (e.g., Cisco has provided already an advisory to this effect [5]).

Until fixes are available, the recommended solution is that users with vulnerable access points and clients should either avoid using Wi-Fi or assume that the security of the Wi-Fi network may not be guaranteed.

In case Wi-Fi access is necessary, service providers should:

- Inform their users that if they are not using any other encryption layer they should know that their data could be public, and traffic potentially manipulated.
- Advise to use an additional layer of encryption such as HTTPS, STARTTLS, Secure Shell, and other reliable protocols to encrypt traffic as it passes between client devices and access points of the Wi-Fi network.
- Where possible, use a reliable VPN service to encrypt network traffic passing though the Wi-Fi network.

Related CVEs

The vulnerabilities received several CVE numbers [3]:

- CVE-2017-13077: reinstallation of the pairwise key in the 4-way handshake
- CVE-2017-13078: reinstallation of the group key in the 4-way handshake
- CVE-2017-13079: reinstallation of the integrity group key in the Four-way handshake
- CVE-2017-13080: reinstallation of the group key in the Group Key handshake
- CVE-2017-13081: reinstallation of the integrity group key in the Group Key handshake
- CVE-2017-13082: accepting a retransmitted Fast BSS Transition Re-association Request and reinstalling the pairwise key while processing it
- CVE-2017-13084: reinstallation of the STK key in the PeerKey handshake
- CVE-2017-13086: reinstallation of the Tunnelled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake
- CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame
- CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame

References

[1] https://papers.mathyvanhoef.com/ccs2017.pdf

[2] https://arstechnica.com/information-technology/2017/10/how-the-krack-attack-destroys-nearly-all-wi-fi-security/

[3] https://www.krackattacks.com/#details-android

[4] https://en.wikipedia.org/wiki/IEEE_802.11i-2004

[5] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa