KRACK attack against WPA2:

**Description of the attack:**

This attack abuses design or implementation flaws in cryptographic protocols to reinstall an already-in-use key. This resets the key’s associated parameters such as transmit nonces and receive replay counters. As you know all protected Wi-Fi networks use the 4-way handshake to generate a fresh session key. The 4-way handshake provides mutual authentication and session key agreement. Together with (AES)-CCMP, a data-confidentiality and integrity protocol, it forms the foundation of the 802.11i amendment. 4-way handshake is a process after association of the client to the Access Point, and after that Group by handshake will happen. Since its first introduction in 2003, under the name WPA, this core part of the 802.11i amendment has remained free from attacks except for known weaknesses of 802.11i are in (WPA-)TKIP []. However, now it has been proved that the 4-way handshake is vulnerable to a key reinstallation attack. [paper]. Here you can see the message format and the 4-way handshaking process.

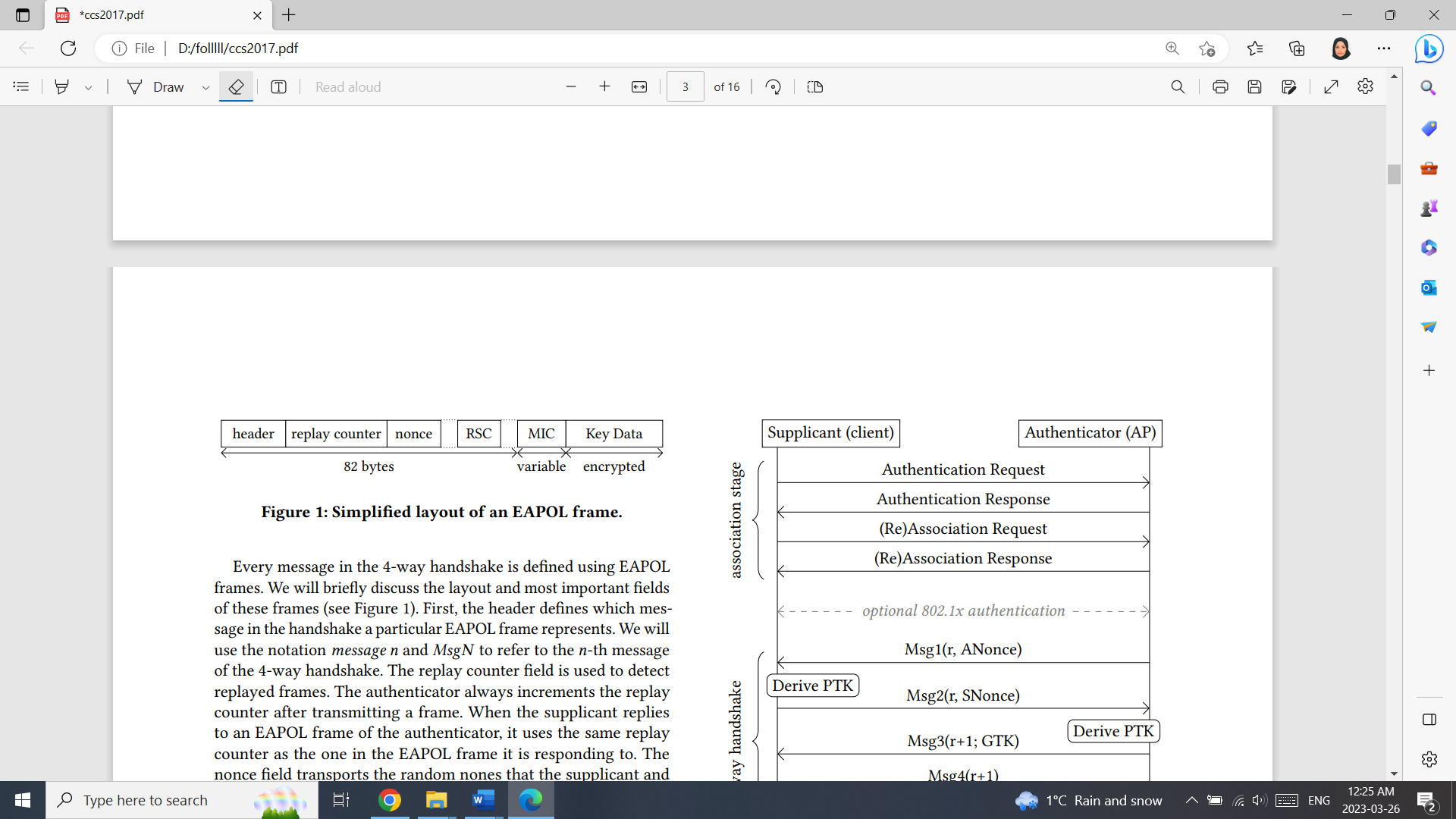


Figure. 1: layout of EAPOL message [1]

|  |  |
| --- | --- |
| Figure. 2: How 4-way hand shake works[1] | **A Summary of 4-way hand shaking[1]:**  The authenticator initiates the 4-way handshake by sending message 1 which contains the ANonce (not protected by a MIC).  On reception of this message, the supplicant generates the SNonce and derives the PTK.It send SNonce to the authenticator in message 2.  Once the authenticator learns the SNonce, it also derives the PTK.  Access point sends the group key (GTK) to the supplicant. Finally, to finalize the handshake, the supplicant replies with message 4 and after that installs the PTK and GTK. |

**High level steps of the attack in different situations:**

The weakness of this process happens in exchanging message 3. because the supplicant always accepts retransmissions of message 3, and even when it is in the PTK-DONE state, we can force a reinstallation of the PTK. There are three different key reinstallation attack scenarios base on the vulnerable component that cause the issue on the attack time. These vulnerable components are: [2]

* + 1- Typical PTK 4-Way Handshake between AP and a client
  + Peerkey 4-way Handshake for communication between peer client
  + Group Key Handshake for AP to inform its existence
  + Fast BSS Transition (FT) Handshake

The impact of exploiting these vulnerabilities includes decryption, packet replay, TCP connection hijacking, HTTP content injection, and others. The way that Man in The Middle (MITM) works for these scenarios is the channel side MITM.[2] In two state the attack can happen; when the client (victim) accepts plaintext retransmissions of message 3 and when the victim only accepts encrypted retransmissions of message 3 which has been in following figures 3 and 4.

|  |  |
| --- | --- |
| Figure 3. Attack in Plaintext Retransmission of message 3 [1] | Figure 4. Attack in Encrypted Retransmission of message 3 [1] |

* **Attack while Plaintext Retransmission of message 3** : in this case the adversary uses a channel-based MitM attack and manipulate handshake messages [1] .
  + The attacker blocks message 4 from arriving at the authenticator. This is illustrated in stage 1 of Figure 3.
  + Immediately after sending message 4, the victim will install the PTK and GTK. At this point the victim also opens the 802.1x port, and send normal data frames. The first data frame uses a nonce value of 1 in the data-confidentiality protocol.
  + Then, in the third stage of the attack, the authenticator retransmits message 3 because it did not receive message 4. The adversary forwards the retransmitted message 3 to the victim, causing it to reinstall the PTK and GTK. Therefore, it resets the nonce and replay counter used by the data-confidentiality protocol.
* **Attack while Encrypted Retransmission of message 3** : ***Figure 4*** illustrates the details of the attack. Th AP actions are clear from context while it’s not in the image. Similar to the previous scenario, Again, the adversary uses a channel-based MitM position. [1]
  + ***Fist Adversary*** lets the victim and adversary execute the initial 4-way handshake, and waits until a second 4-way handshake is initiated to refresh the PTK.(Base on the unique length of message.) Unlike the previous case of attack.
  + in stage 2, the adversary does not instantly forward the first message 3 but waits until the AP retransmits message 3, and then forwards both messages right after one another to the victim. The wireless NIC decrypt both messages using the current PTK, and forwards them to the packet receive queue of the main CPU.
  + In the third stage of the attack, the main CPU of the victim processes the first message 3, replies to it, and ask NIC to install the new PTK.
  + In the fourth stage, the main CPU picks the second message 3 from the receive queue. Since a PTK is installed, the main CPU will mandate that the message was encrypted. However, it does not check under which key the message was encrypted. As a result, even though the message was decrypted under the old PTK, the main CPU will process it. The message 4 sent as a reply is now encrypted under the new PTK using a nonce value of 1.
  + After this, the main CPU commands the NIC to reinstall the PTK, thereby resetting the nonce and replay counters. Finally, the next data frame that the victim transmits will again be encrypted using the new PTK with a nonce of 1.

**Attack Tools:**

The way this attack works uses the MITM attack side channel, therefore all tools that can do the MITM side channel attack can be used in this scenario [2]. This attack has been never reported by attacker or cybersecurity companies, but some Cybersecurity concerned companies [3], discovered the potential attack in 2017 , and then they asked the vendors release the related patches to prevent it happen in real world.

In Feb. 2020, RSA company and ESET presented a potential attack based on the 4-way hand shake vulnerability and the vulnerability of some WiFi Chipset (Broadcom and Crypress). They discovered it when they were working on a new product, Amazon EC2. This new vulnerability was called ***Kr00k*** because it was the result of resetting the master key to “All Zero” in the hardware chipset by default after disassociation of the client from the AP. It leads the MITM can decrypt all messages that still are in the buffer until the new handshake happen. [3]

**Countermeasures:**

Canging your WiFi network password or even swapping out your network router is not going to help [4]. The key to mitigating this vulnerability is *patching the software.* The vendor companies were informed of this vulnerability and releases some updates and patches.[4]. The Vendors that released patched included:

* + [Cisco](https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa) ,[Intel](https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00101&languageid=en-fr) ,[Netgear](https://kb.netgear.com/000049498/Security-Advisory-for-WPA-2-Vulnerabilities-PSV-2017-2826-PSV-2017-2836-PSV-2017-2837" \t "_blank) ,[Aruba](http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2017-007.txt)
  + [OpenBSD](https://marc.info/?l=openbsd-announce&m=148839684520133&w=2) released WPA2 patches, [Debian](https://www.debian.org/security/2017/dsa-3999) also released patches and [Ubuntu](https://askubuntu.com/a/965685) fixes have been issued.
  + Microsoft, Apple and Google have stated that patches as soon as they asked.

It should be mentioned that, if the device that is being used does not have any patch available , the countermeasure is to disable the retransmission of message 3 while in a normal operation it should not be disabled. [2]

***References:***

[1] M.Vanhoef, F.Piessens, 2017, “Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2”, <https://papers.mathyvanhoef.com/ccs2017.pdf>, Accessed: 9 March

[2] [Bill Buchanan, Feb 2020,](Bill%20Buchanan,%20Feb%202020,) Medium.com, < <https://medium.com/asecuritysite-when-bob-met-alice/krack-is-back-meet-kr%C3%B8%C3%B8k-c0832fd4b598> >, Accessed : 9 March [Online]

# [3] KRACK - The Details and the Reality, <<https://www.youtube.com/watch?v=pjTTG2nZax0>>, Accessed : 16 March [Online]

# [4] R.Percy, Oct. 2017, auth0.com, < <https://auth0.com/blog/krack-attack-wpa2-and-what-it-means/> >, Accessed: 16 March [Online]