Hanwha Techwin
6, Pangyo-ro 319 beon-gil, bundang-gu, Seongman-si, Gyeonggi-do, 463-400 Rep. of KOREA
TEL 82.70.7147.8753 FAX 82.31.8018.3740 www.hanwha-security.com

February 8, 2018 Hanwha Techwin

KRACK (Key Reinstallation Attack)

[Summary]

. This attack is against the 4-way and group-key handshake of the WPA2 protocol (including WPA).

. The vulnerability does not expose the encryption key per se but leads to an intentional and recurring installation of the encryption key. As a result, the same initialization vector is used to allow decryption and forging of data.

Keys Used for 4-Way and Group-Key Handshake

. There are three keys used in a handshake. The generation, management, and installation of the respective keys work as follows:

. Pairwise Transient Key (PTK) is used for encrypting unicast communication between AP and client, and is generated and installed each time a wireless connection is set up. PTK is periodically refreshed during connection and when the client roams from one AP to another with FT protocol.

. Group Temporal Key (GTK) is used for encrypting. It is generated and managed by AP and is safely transmitted from to client and installed each time a wireless connection is set up.

. Integrity GTK (IGTK) is used to provide integrity of data (messages managed) broadcast and multicast from AP to clients from AP to clients. It is generated and managed by AP and is safely transmitted from to client and installed each time a wireless connection is set up.

Vulnerabilities in 4-Way Handshake

. A 4-way handshake is performed when a new client joins a Wi-Fi network. The handshake uses messages 1/4 and 2/4 to confirm whether the client and AP have the right authentication (shared master secret called PMK).

. Then, messages 3/4 and 4/4 are used to reinstall the keys for data encryption (PTK, GTK) and data integrity (IGTK).

. The vulnerabilities created allow an unauthenticated user to control the transmission of message 3/4 of the

handshake and, as a result, decrypt data transmitted between client and AP. Depending on the network environment, data forging and retransmission (unicast or broadcast/multicast) from AP to client may also be possible.

. If message 3/4 gets lost or dropped during the transmission (and AP assumes it failed to receive message 4/4 from client), the AP will retransmit message 3/4.

. When the client receives message 3/4 multiple times, it will reinstall the same PTK, and thereby reset the transmit packet number (PN) used as an initialization vector for packet encryption. As a result, the same encryption key (PTK) and initialization vector is used multiple times to encrypt the message, creating vulnerabilities for data decryption. As a result, the replay counter received is reset to trigger vulnerabilities for retransmission attack against the encrypted (unicast) message received. (CVE-2017-13077)

. When client receives message 3/4 multiple times, it will generate the same GTK and IGTK and, at the same time, the replay counter received will be reset to trigger vulnerabilities for retransmission attack against the encrypted (broadcast and multicast) message received. (CVE-2017-13078, CVE-2017-13079)

[Encryption using GTK (for message broadcasting) and provision of integrity using IGTK is only performed by AP. Therefore, data decryption and disablement of integrity test triggered by a reinstallation of GTK and IGTK is not possible on client side.]

Vulnerabilities in Group Key Handshake

. The AP periodically refreshes the group key (so that only recently authenticated clients can have access to the key) and distributes this new group key to all clients using the group key handshake.

. A typical AP refreshes the group key every hour but in some network environment, the group key is reset every time the client disconnects from the network. In addition, a client may request for a group key handshake, creating vulnerabilities for an intentional attack.

. This vulnerability allows an unauthenticated user to control the transmission of group message 1/2 and, as a result, retransmit (broadcast and multicast) data from AP to client.

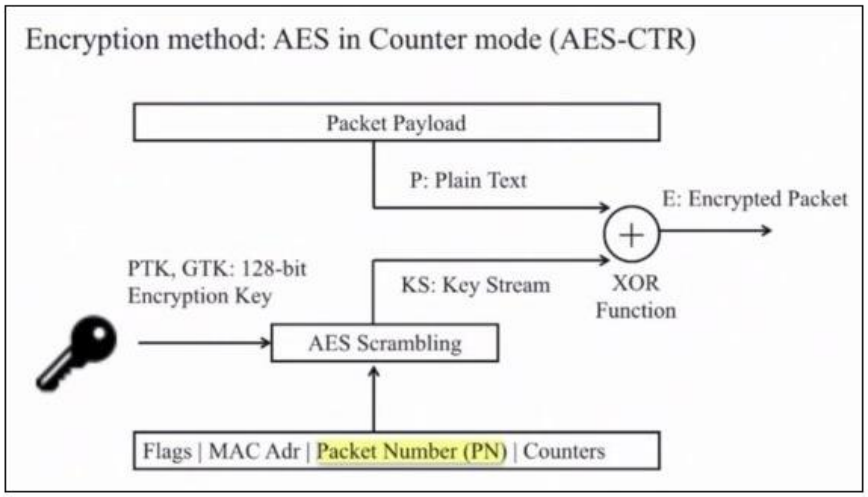
. If group message 1/2 gets lost or dropped during the transmission (and AP assumes it failed to receive group message 2/2 from client), the AP will retransmit group message 1/2.

. When the client receives message 1/2 multiple times, it will reinstall the same GTK and IGTK, and, as a result, the replay counter received is reset to trigger vulnerabilities for retransmission attack against the encrypted (broadcast/multicast) message received. (CVE-2017-13080, CVE-2017-13081)

How data decryption is possible

. In a CCMP (AES-CTR) protocol, the encryption of the message (packet payload) follows the following process. When applying XOR logical operator to a key stream and packet payload that combine PTK (or GTK) encryption key with a number of values (flags, MAC address, packet number, counters), an encrypted packet is generated. Here, flags, MAC address, and counters are fixed values and only the packet number is

a variable.



. Therefore, if the packet number becomes a fixed value in the process of combining the values to obtain a key stream, the sum of the result of the XOR operation of the two encrypted messages (E1⊕E2) and the sum of the result of the XOR operation of the two plain texts (P1⊕P2) become the same. If one plain text (P1) is already known or can be inferred, P2 message can be decrypted. The packet number, in the meantime, is reset in the process of reinstalling the key and may be intentionally induced to a fixed value, allowing decryption via KRACK.

Suppose two packets P1 and P2 are encrypted with PTK:

E1 = P1⊕KS1 and E2 = P2⊕KS2

If P1 and P2 were to use same Packet Number (PN), then:

KS1 = KS2

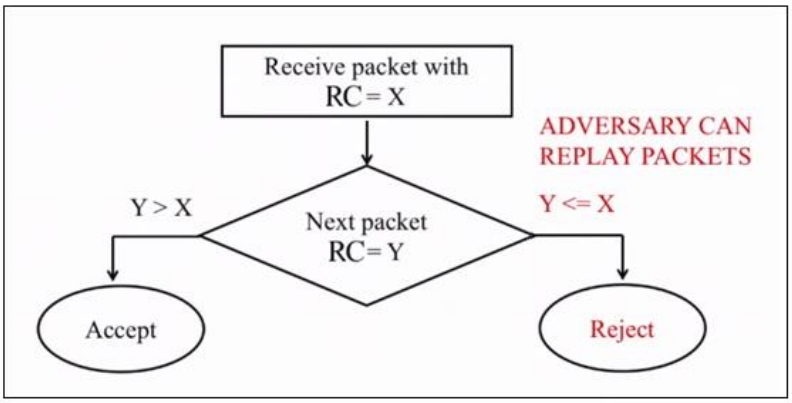
In that case:

E1⊕E2 = P1⊕P2 --- Effect of encryption eliminated!

How retransmission attack is possible

. In order to prevent a malicious attacker from stealing the message sent from AP and retransmitting it to client, the replay counter included in the received message has to be examined (see diagram) on the client side. That is, messages should be allowed only when the current replay counter (Y) is bigger than the previously received replay counter (X), and an omission of such logic enables a retransmission attack.

Hanwha Techwin
6, Pangyo-ro 319 beon-gil, bundang-gu, Seongman-si, Gyeonggi-do, 463-400 Rep. of KOREA
TEL 82.70.7147.8753 FAX 82.31.8018.3740 www.hanwha-security.com



[Scope and Impact]

. Vulnerabilities have been found in the standard Wi-Fi WAP2 specification, thus, ironically enough, leading products in strict compliance with the standard to be exposed to the vulnerabilities.

. Among Techwin products, B2C cameras that use the wpa_supplicant open source were found vulnerable to the attack, specifically the reinstallation of PTK, GTK, IGTK in 4-way handshake (CVE-2017-13077, CVE-2017-13078, CVE-2017-13079) as well as reinstallation of GTK and IGTK in group key handshake (CVE-2017-13080, CVE-2017-13081).

√ severe vulnerability, √ vulnerability, ✗ n/a

Client (OS / Open Source Implementation)	4-way Handshake			Group Key Handshake	
	PTK Reinstallation (CVE-2017-13077)	GTK/IGTK Reinstallation (CVE-2017-13078, 13079)	Remark	GTK/IGTK Reinstallation (CVE-2017-13080, 13081)	Remark
OS X 10.9.5	√	√	compliant	√	compliant
macOS Sierra 10.12	√	√	compliant	√	compliant
iOS 10.3.1	✗	✗	noncompliant	√	compliant
wpa_supplicant v2.3	√	√	compliant	√	compliant
wpa_supplicant v2.4-5	√	√	compliant / bug at implementation	√	compliant
wpa_supplicant v2.6	✗	√	compliant	√	compliant
Android 6.0 & above	√	√	compliant / bug at implementation	√	compliant
OpenBSD 6.1 (rum)	√	√	compliant	✗	noncompliant
OpenBSD 6.1 (iwn)	√	√	compliant	✗	noncompliant
Windows 7	✗	✗	noncompliant	√	compliant
Windows 10	✗	✗	noncompliant	√	compliant
MediaTek	√	√	compliant	√	compliant

Hanwha Techwin
6, Pangyo-ro 319 beon-gil, bundang-gu, Seongman-si, Gyeonggi-do, 463-400 Rep. of KOREA
TEL 82.70.7147.8753 FAX 82.31.8018.3740 www.hanwha-security.com

* Data forging is possible with data-confidentiality protocol used in 4-way handshake

. (AES-) CCMP: unforgeable, (WPA-) TKIP, GCMP: forgeable

. The entire EAPOL message cannot be forged; only the data frame

[Countermeasures]

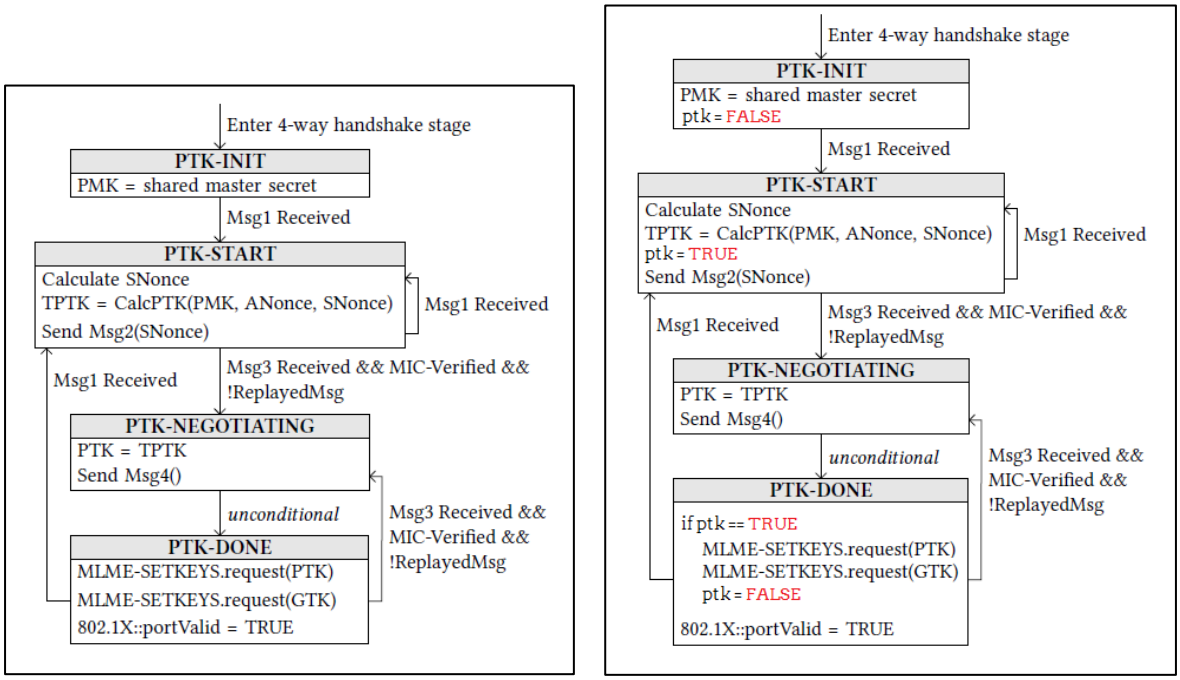
. The countermeasures for the vulnerabilities are as follows:

first, implement the relevant packet number and replay counter so that they do not get reset when keys (PTK, GTK, IGTK) are reinstalled; and

second, allow the keys (PTK, GTK, IGTK) to be installed just once.

[See state transition diagram below]

. The second countermeasure was taken for versions wap_supplicant 2.6 and up, which is also the way Techwin products were patched.



Before After

[Before and after patching 4-way handshake vulnerability]

[Result]

. The vulnerability was fixed through the most recent version of the wpa_supplicant patch and verified through test scripts[*4] provided, except for IGTK reinstallation attack, whose test script was not available.

Tested Items	Test Script	Test Result	
		Before Patch	After Patch
CVE-2017-13077	4-way handshake Key Reinstallation - PTK-TK, TPTK, TPTK (Random Anonce)	Partial vulnerable	fixed

Hanwha Techwin
6, Pangyo-ro 319 beon-gil, bundang-gu, Seongman-si, Gyeonggi-do, 463-400 Rep. of KOREA
TEL 82.70.7147.8753 FAX 82.31.8018.3740 www.hanwha-security.com

CVE-2017-13078	4-way handshake Key Reinstallation-GTK	vulnerable	fixed
CVE-2017-13080	Group key handshake Key Reinstallation	vulnerable	fixed

[Reference]

1. https://www.krackattacks.com/
2. https://blog.mojonetworks.com/wpa2-vulnerability
3. https://papers.mathyvanhoef.com/ccs2017.pdf
4. https://github.com/vanhoefm/krackattacks-scripts