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 공격 (키 재설정 공격)

[취약점 요약]

. WPA2(WPA도 포함) 프로토콜의 4-way 핸드쉐이크 / 그룹키 핸드쉐이크 취약점을 이용한 공격으로서

. 암호화키 자체가 노출되는 것은 아니며, 기존 사용하고 있는 WI-FI 네트워크망에 인위적이고 반복적인 암호화키 재설정을 유도함으로써 암호화에 사용하는 초기 벡터(IV)가 재사용되어 데이터 복호화와 위변조를 가능하게 하는 취약점입니다.

4-way/그룹키 핸드쉐이크에서 사용하는 키

. 핸드쉐이크에서 사용하는 3개의 키 용도 및 생성, 관리, 설치 주체는 다음과 같습니다.

. PTK는 AP와 클라이언트간의 유니캐스트 통신을 암호화하기 위해 사용하며, 무선 연결 설정 시 AP와 클라이언트에 의해서 각각 생성 및 설치됩니다. 연결 중에도 사전 지정된 시간이 지나면 갱신되며, 클라이언트가 FT 프로토콜을 사용하는 AP간의 로밍을 하는 상황에서도 갱신이 됩니다.

. GTK는 AP로부터 클라이언트들에게 브로드캐스트/멀티캐스트하는 데이터 암호화하기 위해 사용하며, AP에 의해서 생성/관리 및 무선 연결 설정 시 AP에서 클라이언트로 안전하게 전달되어 설치됩니다.

. IGTK는 AP로부터 클라이언트들에게 브로드캐스트/멀티캐스트하는 데이터(관리 메시지)의 무결성을 제공하기 위해 사용하며, AP에 의해서 생성/관리 및 무선 연결 설정 시 AP에서 클라이언트로 안전하게 전달되어 설치됩니다.

4-way 핸드쉐이크 취약점

. 4-way 핸드쉐이크는 새로운 클라이언트가 WI-FI 네트워크망에 추가될 때 실행이 되며, 핸드쉐이크하는 4개의 메시지 중 1번째, 2번째 메시지를 사용하여 클라이언트와 AP가 올바른 인증 정보(네트워크의 사전 공유된 비밀번호, PMK)를 소유하고 있는지 확인하며

. 이후 핸드쉐이크하는 4개의 메시지 중 3번째, 4번째 메시지를 사용하여 데이터들을 암호화하기 위해 사용할 키(PTK, GTK)와 무결성을 제공하기 위해 사용할 키(IGTK)를 새롭게 설정합니다.

. 본 취약점은 4-way 핸드쉐이크 4개의 메시지 중 3번째 메시지 전송을 비인가자가 인위적으로 제어함으로

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

써 클라이언트와 AP간의 전송되는 데이터 복호화가 가능한 점이며 네트워크 환경에 따라 데이터 위변조도 가능합니다. 또한, AP에서 클라이언트로 전송되는 (유니캐스트, 브로드캐스트/멀티캐스트) 데이터를 재전송할 수 있게 합니다.

. AP가 클라이언트에 보내는 3번째 메시지가 전송 중 손실될 경우(클라이언트로부터 전송되는 4번째 메시지가 수신되지 않을 경우로 판단함)를 대비해 3번째 메시지를 재전송하게되는데

. 3번째 메시지를 재수신한 클라이언트는 동일한 PTK를 재설정함과 동시에 패킷 암호화의 초기 벡터(IV)로 사용하는 전송 패킷 넘버(PN)를 초기화하면서 메시지 암호화에 동일 암호화키(PTK)와 동일 초기 벡터(IV)를 여러 번 사용하게 되어 데이터 복호화가 가능한 취약점을 노출시키게 되며, 수신된 리플레이 카운터(RC)가 초기화되면서 수신된 암호화 (유니캐스트) 메시지를 여러 번 사용하게 하는 재전송 공격 취약점을 노출시키게 됩니다. (CVE-2017-13077)

. 3번째 메시지를 재수신한 클라이언트는 동일한 GTK, IGTK를 재설정함과 동시에 수신된 리플레이 카운터(RC)가 초기화되면서 수신된 암호화 (브로드캐스트/멀티캐스트) 메시지를 여러 번 사용하게 하는 재전송 공격 취약점을 노출시키게 됩니다. (CVE-2017-13078, CVE-2017-13079)

[GTK를 이용한 암호화(메시지 브로드캐스팅 목적) 및 IGTK를 이용한 무결성 제공은 AP에서만 수행되므로 클라이언트에서의 GTK 및 IGTK 재설정으로 인한 데이터 복호화 및 무결성 검사 무력화는 불가능합니다]

그룹키 핸드쉐이크 취약점

. AP는 주기적으로 그룹키를 갱신(최근에 승인된 클라이언트들만 그룹키를 소유하게 하기 위한 목적)하며 그룹키 핸드쉐이크를 이용하여 모든 클라이언트들에게 새로운 그룹키를 배포합니다.

. 대부분의 AP는 매시간 그룹키를 갱신하며, 일부 네트워크에서는 클라이언트가 네트워크 연결을 해제할 때마다 그룹키를 갱신하기도 합니다. 더 나아가 클라이언트가 그룹키 핸드쉐이크를 요청할 수도 있기 때문에 의도적인 공격이 가능하게 됩니다.

. 본 취약점은 그룹키 핸드쉐이크 2개의 메시지 중 1번째 그룹 메시지 전송을 비인가자가 인위적으로 제어함으로써 AP에서 클라이언트로 전송되는 (브로드캐스트/멀티캐스트) 데이터를 재전송할 수 있게 합니다.

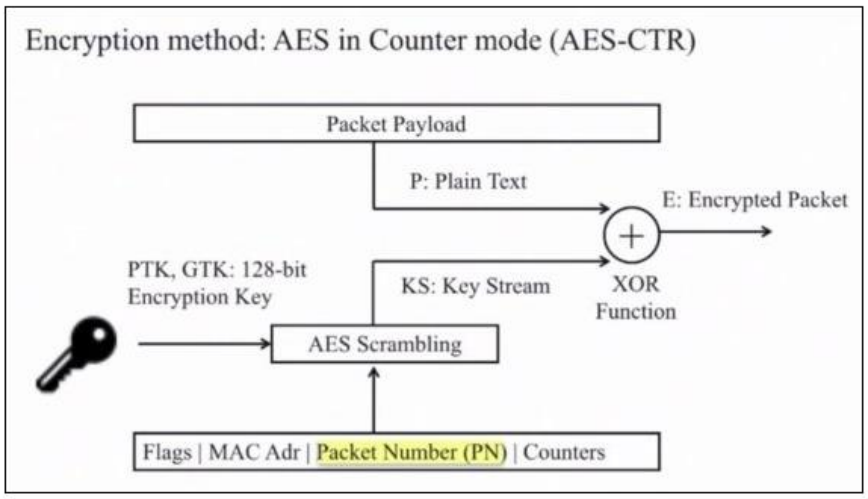
. AP가 클라이언트에 보내는 1번째 그룹 메시지가 전송 중 손실될 경우(클라이언트로부터 전송되는 2번째 그룹 메시지가 수신되지 않을 경우로 판단함)를 대비해 1번째 그룹 메시지를 재전송하게되는데

. 1번째 그룹 메시지를 재수신한 클라이언트는 동일한 GTK, IGTK를 재설정함과 동시에 수신된 리플레이 카운터(RC)가 초기화되면서 수신된 암호화 (브로드캐스트/멀티캐스트) 메시지를 여러 번 사용하게 하는 재전송 공격 취약점을 노출시키게 됩니다. (CVE-2017-13080, CVE-2017-13081)

데이터 복호화가 가능한 이유

. CCMP(AES-CTR) 프로토콜 기준으로 메시지(Packet Payload)에 대한 암호화는 다음과 같은 과정을 따르게 됩니다. PTK (또는 GTK) 암호화키와 몇 가지 값(플래그, MAC 주소, 전송 패킷 넘버, 카운터)들을 조합한 KS(키 스트림)과 평문 메시지(Packet Payload)를 배타적 논리합(XOR)으로 연산을 하면 암호화된 메시지(Encrypted Packet)를 얻게 됩니다. 여기서 플래그, MAC 주소, 카운터는 이미 고정된 값이며, 전송 패킷 넘버(PN)만 변수입니다.

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



. 따라서, KS(키 스트림)를 얻기 위해 조합하는 과정에서 전송 패킷 넘버(PN)가 고정값이 되는 경우 다음과 같이 두 개의 암호화된 메시지들의 논리적 배타합(E1⊕E2)의 결과와 두 개의 평문 메시지들의 논리적 배타합(P1⊕P2)의 결과가 같아지며 한 개의 평문 메시지(P1)를 이미 알고 있거나 유추가 가능한 경우 P2 메시지의 복호화가 가능해집니다. 그리고, 전송 패킷 넘버(PN)는 키 재설정 과정에서 초기화가 되며 의도적인 고정값으로 유도할 수 있으므로, KRACK 취약점을 이용한 복호화가 가능하게 됩니다.

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

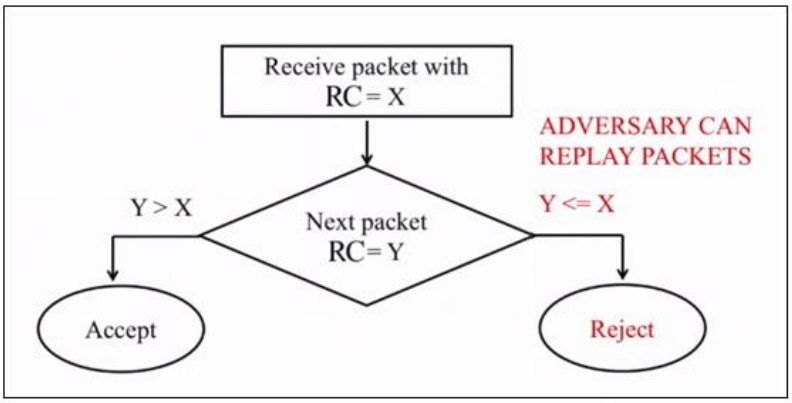
In that case:

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

재전송 공격이 가능한 이유

. 악의적인 공격자가 AP로부터 보내는 메시지를 탈취하여 클라이언트로 재전송하는 공격을 막기 위해 클라이언트에서는 수신 메시지에 포함된 리플레이 카운터(RC)를 검사해야만 합니다(그림 참조). 즉, 현재 수신된 리플레이 카운터(Y)가 이전 수신된 리플레이 카운터(X)보다 클 경우만 메시지를 허용해야 합니다만, 이러한 로직이 생략되어 있어 재전송 공격이 가능합니다.

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



[취약점 발생 범위 및 영향]

. WI-FI WAP2 표준 스펙에서 취약점이 발생하였으며, 이 때문에 해당 표준을 엄격히 지키는 제품에서 오히려 취약점이 발생하였습니다.

. 당사 제품의 경우 wpa_supplicant 오픈소스를 사용하고 있는 B2C 카메라에 해당 취약점이 노출된 상황이며, 4-way 핸드쉐이크의 PTK, GTK, IGTK 재설정 취약점(CVE-2017-13077, CVE-2017-13078, CVE-2017-13079)과 그룹키 핸드쉐이크의 GTK, IGTK 재설정 취약점(CVE-2017-13080, CVE-2017-13081)이 존재하는 것으로 확인되었습니다.

√ 심각한 취약점 존재, √ 취약점 존재, ✗ 취약점 없음

클라이언트 (구현된 OS / 오픈소스)	4-way 핸드쉐이크			그룹키 핸드쉐이크	
	PTK 재설정 (CVE-2017-13077)	GTK/IGTK 재설정 (CVE-2017-13078, 13079)	비 고	GTK/IGTK 재설정 (CVE-2017-13080, 13081)	비 고
OS X 10.9.5	√	√	표준 준수	√	표준 준수
macOS Sierra 10.12	√	√	표준 준수	√	표준 준수
iOS 10.3.1	✗	✗	표준 위반	√	표준 준수
wpa_supplicant v2.3	√	√	표준 준수	√	표준 준수
wpa_supplicant v2.4-5	√	√	표준 준수 / 구현상의 버그	√	표준 준수
wpa_supplicant v2.6	✗	√	표준 준수	√	표준 준수
Android 6.0 & above	√	√	표준 준수 / 구현상의 버그	√	표준 준수
OpenBSD 6.1 (rum)	√	√	표준 준수	✗	표준 위반
OpenBSD 6.1 (iwn)	√	√	표준 준수	✗	표준 위반
Windows 7	✗	✗	표준 위반	√	표준 준수
Windows 10	✗	✗	표준 위반	√	표준 준수
MediaTek	√	√	표준 준수	√	표준 준수

* 4-way 핸드쉐이크에 사용하는 암호화(data-confidentiality) 프로토콜에 따라 데이터 위변조도 가능함

. (AES-)CCMP는 위변조 불가, (WPA-)TKIP, GCMP는 위변조 가능

. 위변조 가능한 데이터의 범위는 EAPOL 전체 메시지는 불가하며 데이터 프레임만 가능

[취약점 개선 방안]

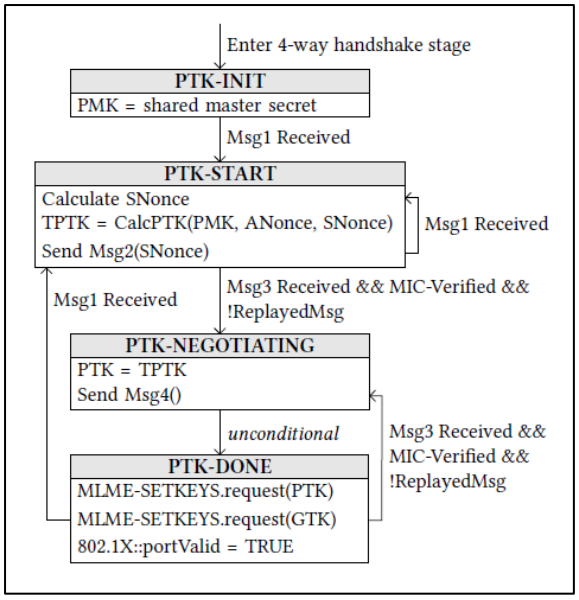
. 해당 취약점의 개선 방안은

첫째, 키(PTK, GTK, IGTK)가 재설정되는 경우 관계되는 패킷 넘버(PN)와 리플레이 카운터(RC)가 초기화되지 않도록 구현하거나

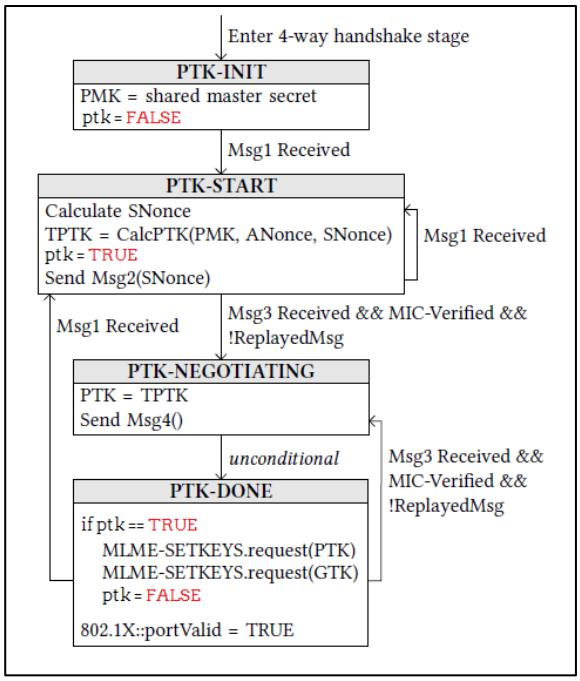
둘째, 설정되는 키(PTK, GTK, IGTK)가 한번만 설정되도록 구현하는 방안이 있습니다.

[하기 상태 전이도 참조]

. wap_supplicant 2.6 이상 버전에서는 둘째 방안이 적용되었으며, 당사의 제품들도 이 방안으로 패치가 되었습니다.



취약점 개선 전



취약점 개선 후

[4-way 핸드쉐이크의 취약점 개선 전/후]

[취약점 개선 결과]

. 해당 취약점은 최신 버전의 wpa_supplicant 패치 버전을 사용하여 해결하였으며, 제공된 테스트스크립트*4를 이용하여 검증되었습니다. 다만, IGTK 재설정 취약점의 경우 테스트 스크립트가 제공되지 않아 검증은 생략되었습니다.

테스트 항목	테스트 스크립트	테스트 결과	
		패치전	패치후
CVE-2017-13077	4-way handshake Key Reinstallation - PTK-TK, TPTK, TPTK (Random Anonce)	일부 취약	양호

CVE-2017-13078	4-way handshake Key Reinstallation-GTK	취약	양호
CVE-2017-13080	Group key handshake Key Reinstallation	취약	양호

[참조 링크 및 문서]

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