Security – KRACK

오민석 정보관리기술사
(min-oh@korea.ac.kr)

KRACK, WI-Fi 보안의 핵심 취약점

Concept	**(KRACK 의 정의)** - Wi-Fi 연결을 보호하기 위한 WPA2 프로토콜의 4-way handshake 과정에서 MITM 공격을 통해 패킷의 재생, 복호화, 변조가 가능한 공격
KeyWord	**WPA2, WPA2 Vulnerability, Key Reinstallation Attacks, KRACK** **MITM(Man In The Middle)**

KRACK 의 개요

2017 년 10 월 15 일 전세계를 강타한 WPA2 취약점이 발견되었다. 이 취약점은 WPA2 의 4-way handshake 과정에서 Key Reinstallation 을 이용한 MITM(Man In The Middle) 공격을 통해 패킷의 재생, 복호화, 변조가 가능한 취약점이다. 이것이 의미하는 것은 전세계 인구의 45%가 사용하는 무선인터넷 환경이 안전하지 않게 됐다는 의미이다. 이후 WPA2 를 이용하는 장비의 추가적인 패치와 차세대 와이파이 보안 프로토콜인 WPA3 가 나왔지만 아직도 많은 모바일 기기들과 무선공유기가 KRACK 의 취약점에 노출되어 있어, 그 위험은 사라지지 않고 있다. 이에 본고에서는 WPA2 의 보안 프로세스와 이 과정에서의 KRACK 의 취약점을 이용한 공격 방법과 대응 방법에 대해 살펴 보도록 하겠다.

KRACK 의 취약점

WPA/WPA2 에 대한 KRACK 의 취약점은 현재 10 가지가 있고 관련 내용은 표 1 과 같다.

CVE 번호	취약점 요약	
CVE-2017-13077	Reinstallation of the pairwise encryption key (PTK-TK) in the four-way handshake.	
CVE-2017-13078	Reinstallation of the group key (GTK) in the four-way handshake	
CVE-2017-13079	Reinstallation of the integrity group key (IGTK) in the four-way handshake	
CVE-2017-13080	Reinstallation of the group key (GTK) in the group key handshake.	

CVE-2017-13081	Reinstallation of the integrity group key (IGTK) in the group key handshake.
CVE-2017-13082	Accepting a retransmitted Fast BSS Transition (FT) Reassociation Request and reinstalling the pairwise encryption key (PTK-TK) while processing it.
CVE-2017-13084	Reinstallation of the STK key in the PeerKey handshake
CVE-2017-13086	Reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake.
CVE-2017-13087	Reinstallation of the group key (GTK) while processing a Wireless Network Management (WNM) Sleep Mode Response frame
CVE-2017-13088	Reinstallation of the integrity group key (IGTK) while processing a Wireless Network Management (WNM) Sleep Mode Response frame

[표 1] KRACK 취약점 정보 요약

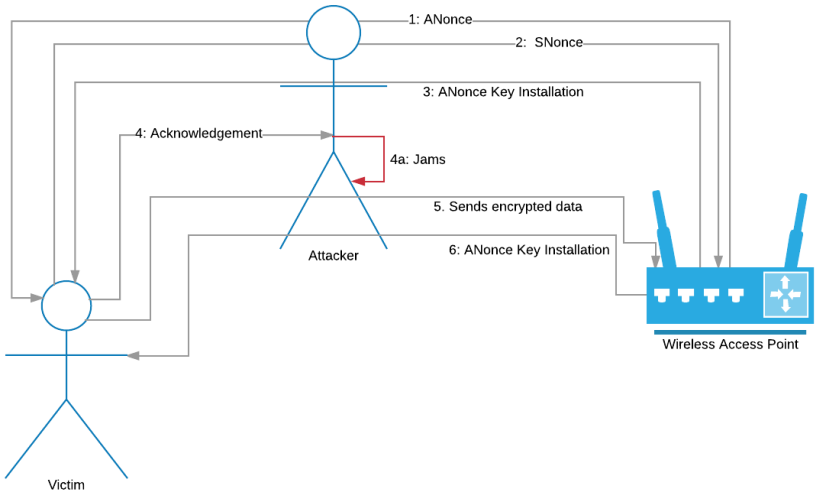
그리고 이러한 취약점들을 통해 KRACK 의 특징은 아래와 같이 요약 될 수 있다.

- ✓ 외부에서 WPA2 의 접속 암호를 알아 낼 순 없다.
- ✓ Attacker 가 Victim 과 같은 네트워크망에 있어야 한다.
- ✓ Man In The Middle 공격 통해 패킷에 대한 재생, 복호화, 변조가 가능하다.

결국, KRACK 취약점을 이용하면 AP 에 접속하지 않고서도 AP 와 Station 사이의 암호화된 데이터를 가로챌 수 있어 신용카드 정보, 각종 패스워드, 채팅, 이메일 등의 정보에 대한 도용이 가능하다.
이와 같은 KRACK 의 특징을 인지하고 WPA2 의 인증 과정에서 KRACK 취약점을 이용한 MITM 공격 시나리오에 대해 알아 보고 대응 방안에 대해 살펴 보도록 하겠다.

WPA2 의 보안 프로세스와 KRACK 의 MITM Attack 시나리오

KRACK 취약점은 AP 와 Station 간에 상호작용하는 인증 절차의 과정에서 발생된다. AP 또는 Station 이 보낸 암호화 검증 메시지를 중간에 가로채어 동일하게 전달함으로써 발생되는 오류를 이용한 재인증 공격 방법이다.
그림 1 은 이러한 KRACK 의 MITM 공격에 시나리오를 도식화 하여 보여 주고 있다.



[그림 1] KRACK 의 MITM 공격 시나리오

Attacker 가 AP 와 Victim 의 사이에서 MITM 공격을 통해 패킷을 스니핑하고 이를 복호화 하여 악용 할 수 있는 시나리오이다. 이는 WPA 의 인증을 위한 4way-handshake 과정에서 key 의 Reinstall 을 이용한 공격이며, 이 과정을 보다 상세히 설명해주고 있는 것이 그림 2 의 프로세스이다.

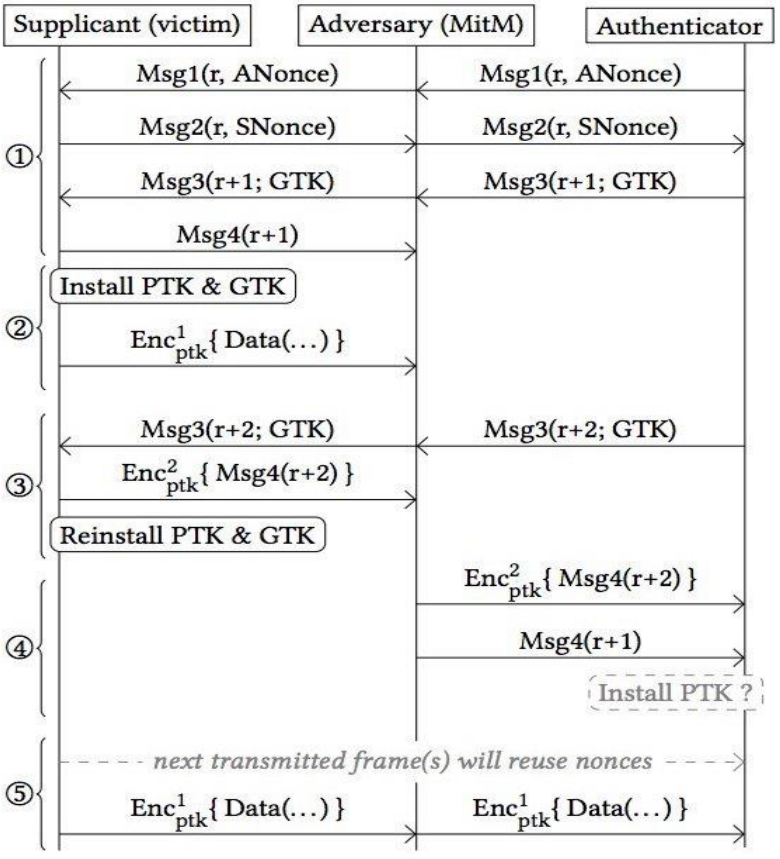


Figure 4: Key reinstallation attack against the 4-way handshake, when the supplicant (victim) still accepts plaintext retransmissions of message 3 if a PTK is installed.

[그림 2] WPA2 4-way hanfshake 과정에서의 KRACK 시나리오

그림 2 에서의 공격 시나리오를 자세히 살펴보면 아래와 같다.

① 공격자는 메시지를 보다가 Msg4 를 가로채고 보내지 않는다.
② 클라이언트는 Msg4 를 보낸 직후 PTK & GTK 를 설치하고, 설치한 PTK 로 데이터를 암호화해서 보낸다.
③ AP 는 Msg4 가 오지 않으므로 클라이언트가 Msg3 를 못 받은 걸로 생각하고, 다시 MSG4 를 설치했던 PTK 로 암호화해서 보낸다. 공격자는 이걸 그대로 전달한다. 클라이언트는 Msg3 를 받고 nonce 와 replay 카운터를 초기화 한다.
④ AP 사이드에 연결을 성립시켜서 PTK 설치하게 한다. 생각해보면 AP 는 Msg4 를 받지 않아 아직 PTK 가 설치 되어 있지 않기 때문에, 클라이언트가 보낸 암호화된 Msg4 를 reject 할 것이다. 그러나 802.11 표준을 유심히 살펴보면 마지막 counter 뿐만 아니라 4-way handshake 에 사용된 모든 replay counter 를 받아들이도록 되어 있어서 문제 없다. 즉, 어떤 AP 는 r+1 을 받아들이고 어떤 AP 는 이전에 암호화된 Msg4 를 받아들임
⑤ 클라이언트가 데이터를 다시 동일한 Nonce 와 PTK 로 암호화해서 보낸다.

기존에 WPA 가 보안을 유지하는 방식은 Key 를 계속 Refresh 하여 악의적인 복호화 등으로부터 기밀성을 유지하는 것인데 MITM 을 통해 key 를 재사용 하고 Packet Number 를 초기화 함으로써 WPA 의 기밀성에 대한 보안을 무력화 시키는 것이다.

표 2 는 WPA 의 암호알고리즘의 KRACK 에 대한 취약점을 보여주고 있다.

Encryption	Vulnerability	Decryption
AES CCMP	패킷 복호화	KRACK 공격을 통해 Packet Number 를 초기화하여 패킷 재조합 가능
WPA TKIP	패킷 복호화 위변조·삽입 가능	IV 재사용으로 발생된 WEP 취약점 보안을 위해 IV Field 를 PN(Packet Number)으로 사용함. KRACK 공격을 통해 Packet Number 를 초기화할 수 있으므로 암호화 시 사용된 IV*값을 획득할 수 있음
GCMP		Wireless Gigabit(WiGig)에 사용되는 암호화 방식. 두 가지 통신방향에서 동일한 인증키를 사용하므로 KRACK 취약점을 통한 인증키 탈취 가능

[표 2] WPA 에 사용되는 암호알고리즘과 KRACK 에 대하

KRACK 의 대응방안

1)AP 와 Station 에서의 대응방안

Type	CVE	*Root Cause Fix	*Mitigation	*Zero-day Protection
Station Side	CVE-2017-13077 Reinstallation of the pairwise encryption key (PTK-TK) in the four-way handshake.	Update Station Software	Update AP Software	AP MAC Spoofing Protection
	CVE-2017-13078 Reinstallation of the group key (GTK) in the four-way handshake			
	CVE-2017-13079 Reinstallation of the integrity group key (IGTK) in the four-way handshake			
	CVE-2017-13080 Reinstallation of the group key (GTK) in the group key handshake.			
	CVE-2017-13081 Reinstallation of the integrity group key (IGTK) in the group key handshake.			
	CVE-2017-13087 Reinstallation of the group key (GTK) while processing a Wireless Network Management (WNM) Sleep Mode Response frame			
AP Side	CVE-2017-13082 Accepting a retransmitted Fast BSS Transition (FT) Reassociation Request and reinstalling the pairwise encryption key (PTK-TK) while processing it.	Update AP Software		

[표 3] AP 와 Station 에서의 KRACK 의 대응방안

2) 사용자 관점에서의 대응방안

- ✓ 무선으로 연결된 모든 기기를 업데이트하라.
  - 컴퓨터, 스마트폰, 태플릿 PC 등 와이파이가 연결된 모든 기기와 라우터의 보안 패치를 가장 최신의 것으로 업데이트하라. 미래에 발생할 수 있는 보안 취약점에 대비해 보안 패치를 자동 업데이트 모드로 설정하는 것도 한 방법이다.
- ✓ 라우터를 살펴라.
  - 라우터의 펌웨어 역시 업데이트가 필요하다. 인터넷 서비스 제공자(ISP)에서 라우터를 제공받았다면, 해당 회사에 알맞은 패치 키트가 무엇인지 물어보라.

결론

KRACK 과 같은 취약점이 발견되면 전문가들이 빠른 속도로 패치를 내어 놓고 근본적으로 이러한 취약점을 대응 할 수 있는 새로운 프로토콜을 금새 개발하곤 한다. 그러나 많은 기업, 일반 사용자들은 이러한 것이 관심을 두고 있지 않다. 아직도 오래된 프로토콜을 사용하고 패치를 하지 않은 소프트웨어를 사용하고 있다. 옛말에 구슬이 서 말 이어도 꿰어야 보배라는 말이 있다. 우리가 안전한 무선인터넷 환경을 활용하기 위해서는 이러한 보안 취약점에 대해 항상 관심을 갖고 지속적인 패치를 하는 것이 가장 중요하다. 오늘부터라도 이글을 읽는 순간부터라도 내가 사용하고 있는 무선환경들이 최신의 소프트웨어로 패치 되었는지 관심을 가지고 확인해보도록 하자.

"끝"

Reference

1)https://ko.wikipedia.org/

2)https://www.krcert.or.kr/data/secNoticeView.do?bulletin_writing_sequence=26752&queryString=cGFnZT0xJnNvcnRfY29kZT0mc2VhcmNoX3NvcnQ9dGl0bGVfbmFtZSZzZWFyY2hfd29yZD1rcmFjayZ4PTAmeT0w

3)http://www.norma.co.kr/wpa2-krack-%EC%B7%A8%EC%95%BD%EC%A0%90-%EC%A0%95%EB%A6%AC/

4) http://blog.skinfosec.com/221144209528

Contents connect communications!!

아이리포에 오시면 더 많은 지식을 가져가실 수 있습니다.

아이리포 온라인 : http://www.ilifo.co.kr
아이리포 지덤시리즈 : http://www.jidum.com
아이리포 IT 지식창고 : https://www.ilifo.co.kr/boards/knowledge
아이리포 기술사/감리사 카페 : http://cafe.naver.com/itlf

서울시 마포구 상암동 1610 번지, DDMC 3 층 아이리포 교육센터
TEL: 02-303-9997 | MAIL: edu@ilifo.co.kr