KRACK

https://youtu.be/4WnOz-XHIxw

KRACK

Key Reinstallation Attacks (키 재설치 공격)

- Wi-Fi 연결을 보호하는 Wi-Fi Protected Access(WPA) 프로토콜의 4-way handshake & groupkey handshake 취약점을 이용한 공격

- 암호화키 자체 노출되지 않고,기존 사용하고 있는 WIFI 네트워크 망에 인위적&반복적인 암호화키 재설정유도

  -> 암호화에 사용하는 초기 벡터(IV)가 재사용되어 데이터 복호화와 위변조 가능

4-way handshake

4-way handshake 목적

- 쌍방간 PMK(Pairwise Master Key) 보유 및 현행성 확인
- PMK로부터 PTK(Pairwise Transient Key) 유도
- STA와 AP에서 유도된 PTK 설치
- Cipher Suite (TLS 암호통신 할 때 사용되는 암호알고리즘 집합)확정

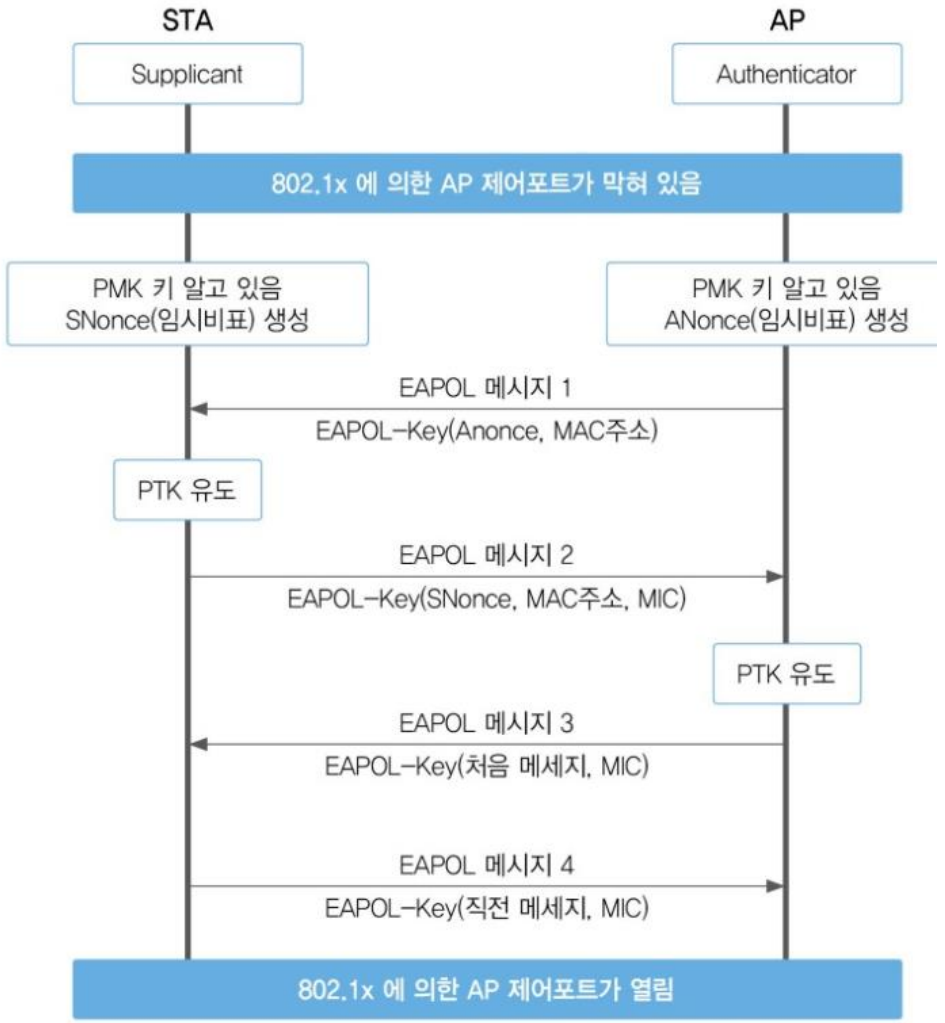
4-way handshake 절차

1. AP -> STA
- AP의 MAC 주소 및 Nonce 값(ANonce)이 포함된 메시지 전송

2. STA -> AP
- STA는 Nonce 값 생성
- STA의 MAC 주소, PMK, ANonce, SNonce 이용하여 PTK(Pairwise Transient Key) 유도 생성
- STA의 MAC주소, SNonce이 포함된 메시지(MIC;메시지 무결성 코드) 전송

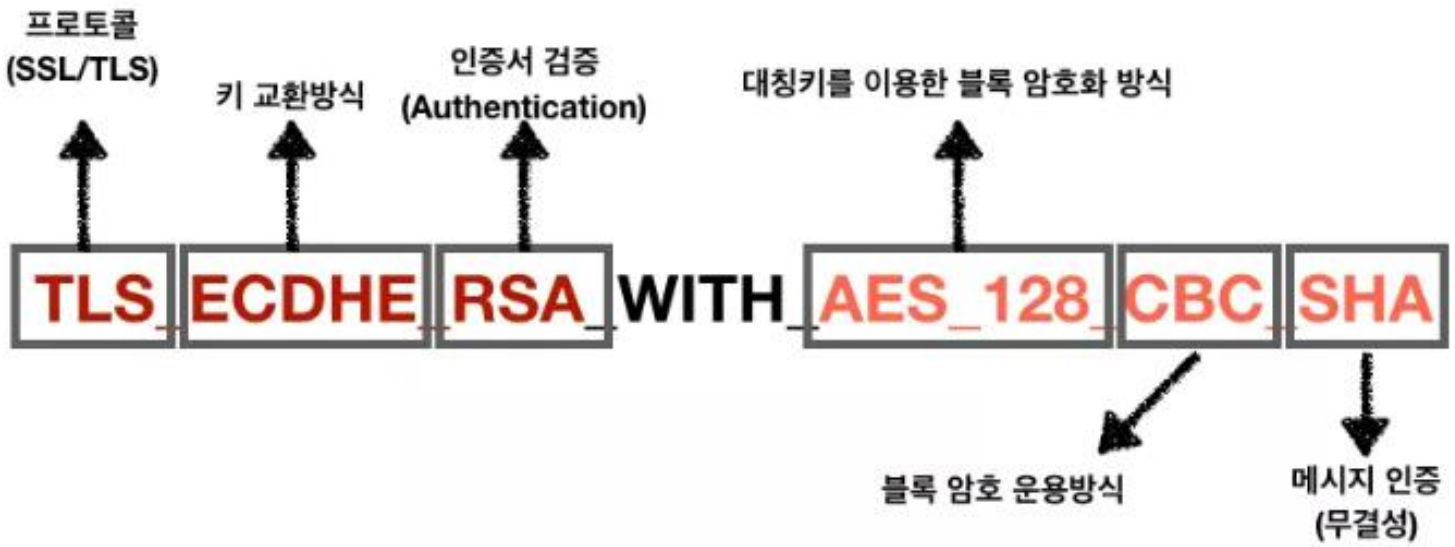
3. AP -> STA
- 처음 메시지 1과 동일하면서, MIC가 추가된 메시지 전송

4. STA -> AP
- 직전 메시지 3 에 대한 단순 수신 응답(MIC포함 전송)



출처 http://www.ktword.co.kr/abbr_view.php?m_temp1=1842

Cipher Suite의 구조



Cipher Suite

Cipher Suite 3가지 종류의 알고리즘을 포함

1) **Key exchange algorithm** : 암호통신시 사용하는 대칭암호키를 교환하는 (확정하는) 알고리즘

2) **bulk encryption algorithm** : record를 encryption을 할 때 사용하는 대칭키 알고리즘

3) **message authentication code(MAC) algorithm** : 전달된 message의 무결성(Integrity) 과 인증(Authentication)을 위해 사용되는 알고리즘

4-way handshake

4-way handshake 목적

- 쌍방간 PMK(Pairwise Master Key) 보유 및 현행성 확인
- PMK로부터 PTK(Pairwise Transient Key) 유도
- STA와 AP에서 유도된 PTK 설치
- Cipher Suite (TLS 암호통신 할 때 사용되는 암호알고리즘 집합)확정

4-way handshake 절차

1. AP -> STA

- AP의 MAC 주소 및 Nonce 값(ANonce)이 포함된 메시지 전송

  *ANonce : 액세스 포인트 (인증 자)에 의해 생성 된 난수

2. STA -> AP

- STA는 Nonce 값 생성
- STA의 MAC 주소, PMK, ANonce, SNonce 이용하여 PTK(Pairwise Transient Key) 유도 생성
- STA의 MAC주소, SNonce이 포함된 메시지(MIC;메시지 무결성 코드) 전송

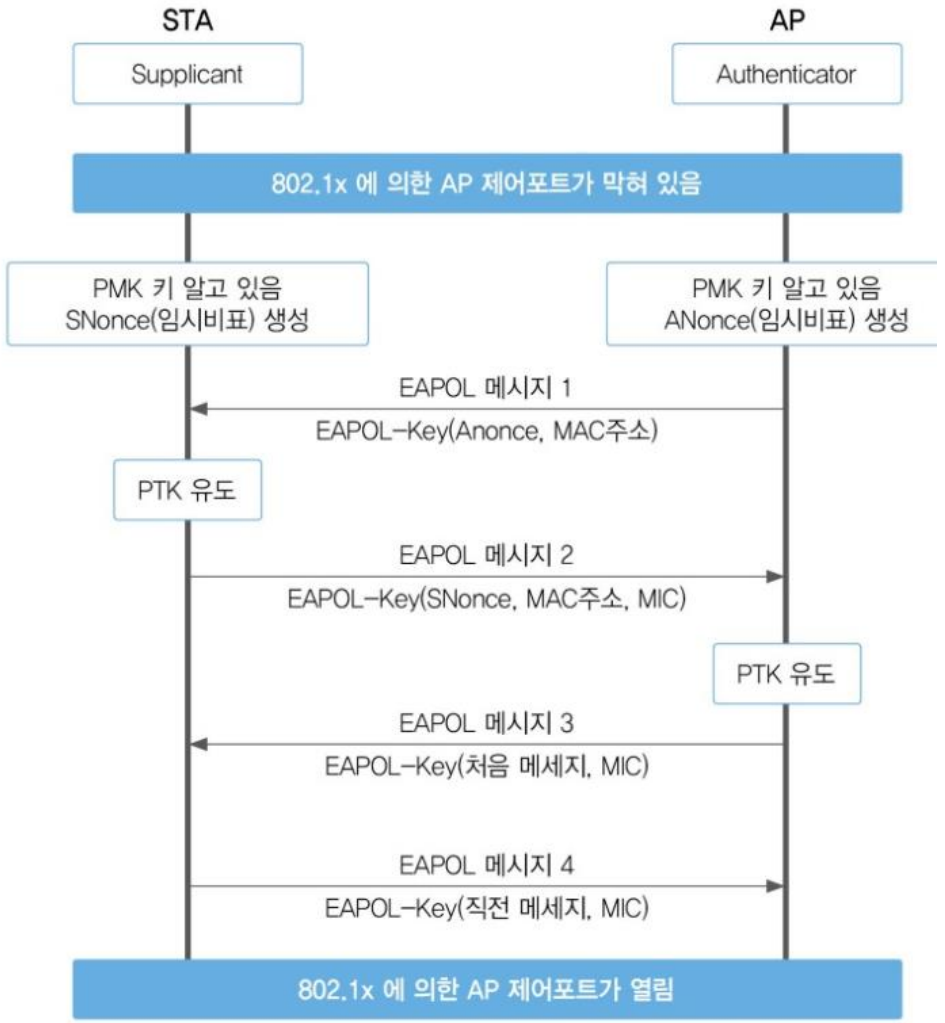
  *SNonce : 클라이언트 장치 (요청자)에 의해 생성 된 난수

3. AP -> STA

- 처음 메시지 1과 동일하면서, MIC가 추가된 메시지 전송

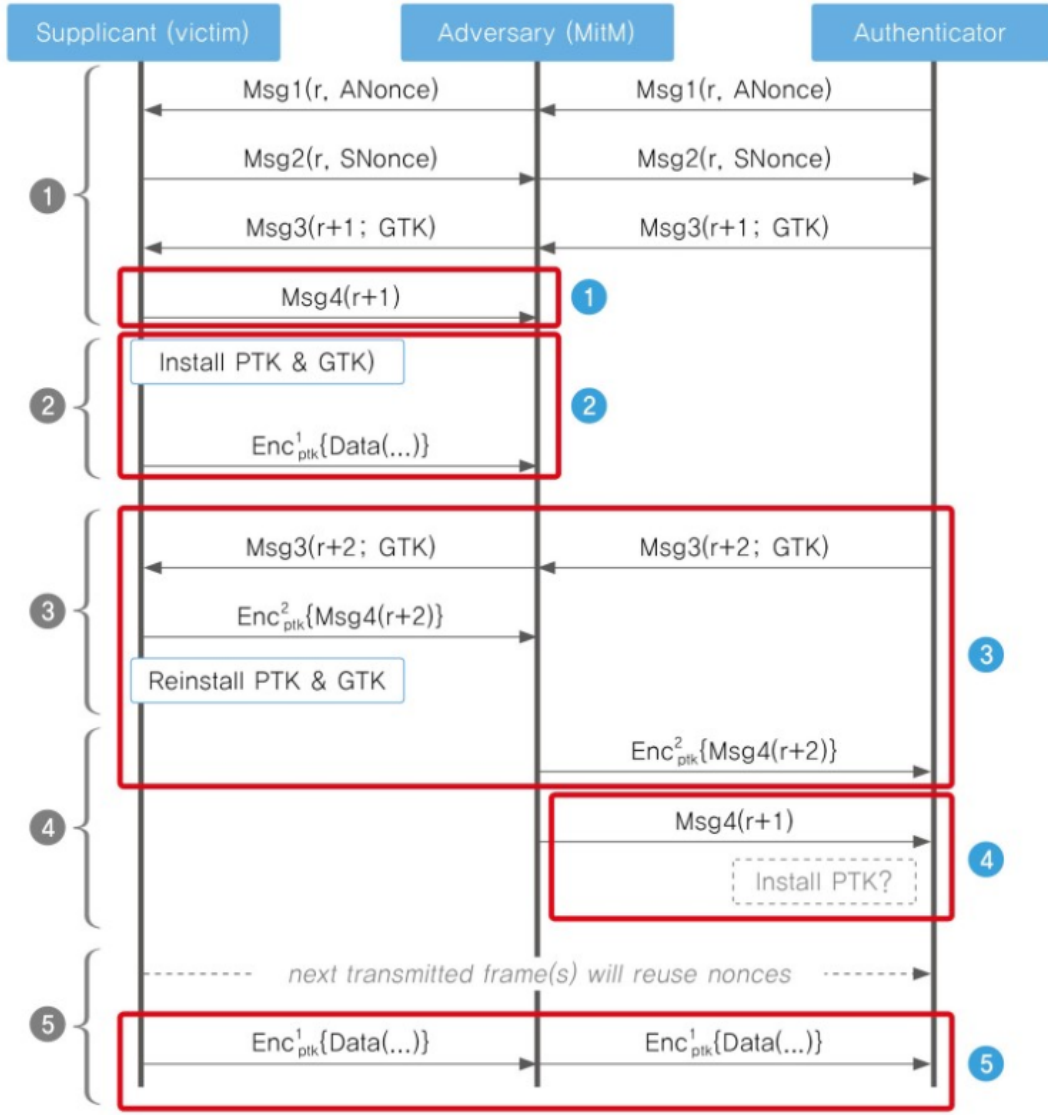
4. STA -> AP

- 직전 메시지 3 에 대한 단순 수신 응답(MIC포함 전송)



출처 http://www.ktword.co.kr/abbr_view.php?m_temp1=1842

4-way handshake 취약점



출처 : https://m.blog.naver.com/PostView.nhn?blogId=skinfosec2000&logNo=221144209528&proxyReferer=https%3A%2F%2Fwww.google.com%2F

4-way handshake 취약점

- AP는 클라이언트 측에서 잘 수신하였다는 메세지를 받지 못했다면 message3을 다시 전달

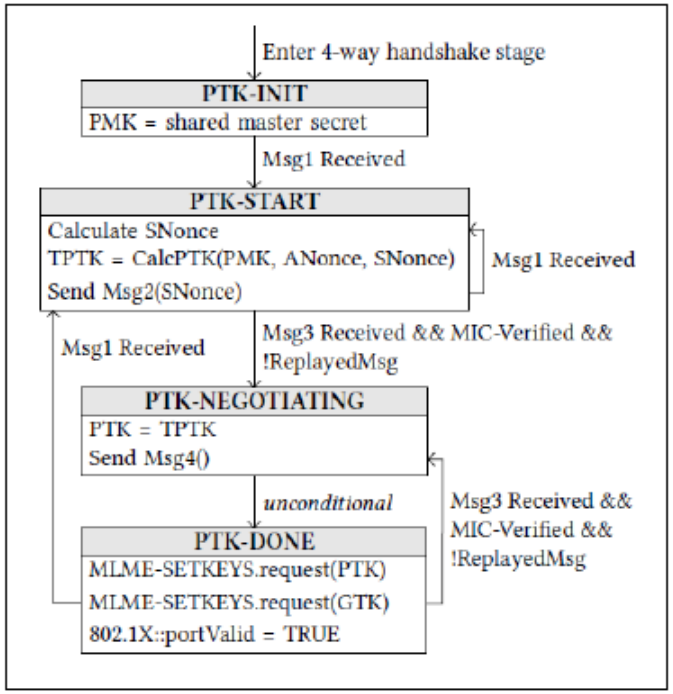
  ->클라이언트는 여러번의 message3을 받을 가능성 존재

- 클라이언트는 매번 message를 받을 때 마다 암호키, 데이터 패킷의 nonce와 수신한 재생 카운터 다시 재설정

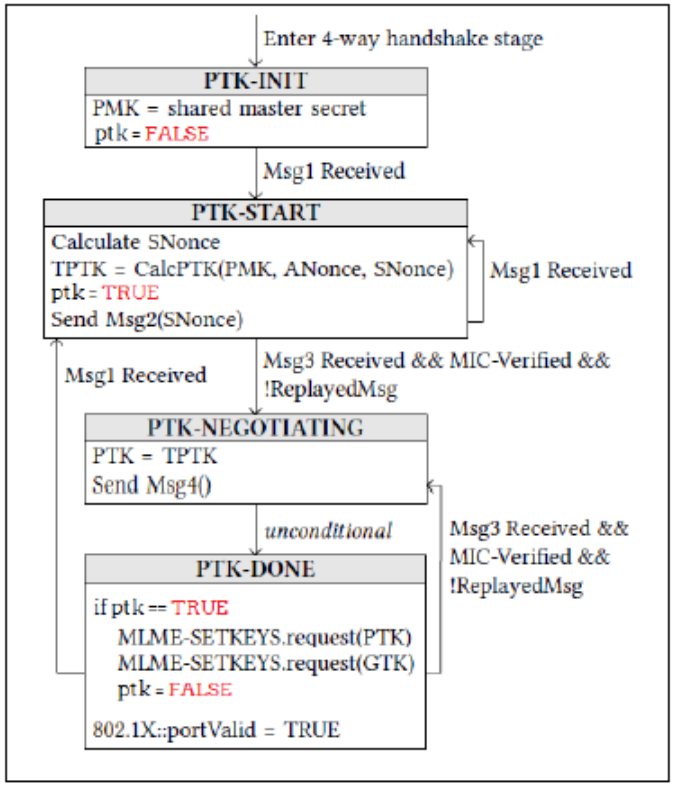
- 공격자는 수집과 재발송된 message3이 강제적으로 재설정한 nonce를 통하여 성공적으로 암호화 프로토콜의 재사용 공격 가능

출처 http://www.ktword.co.kr/abbr_view.php?m_temp1=1842

4-way handshake 취약점개선 방향



취약점 개선 전



취약점 개선 후

1. 키가 재설정되는 경우, 관계되는 패킷 넘버(PN)와 리플레이 카운터(RC)가 초기화되지 않도록 구현

2. 설정되는 키가 한번만 설정되도록 구현

이외의 handshake

1. Group Key HandShake

4-Way Handshake를 통해 PTK와 GTK를 확보한 STA에,
Multicast 또는 Broadcast용 데이터 암호화를 목적으로 GTK를 분해하기 위한 2-Way Handshake 과정

2. Peer Key HandShake

AP에 연결된 단말기 간의 연결을 보호하기 위하 STK(Short-Term Key)의 설치를 위해 4-Way Handshake를 활용하여 세션 키를 교환

3. fast BSS transition HandShake (802.11r)

기지국에서 다른 곳으로 끊김 없이, 빠르고 안전한 채널전환을 지원하기 위해, BSS 전환 시 4-Way HandShake를 활용하여 세션 키 교환

Q & A