Security - 01 WPA3

오민석 정보관리기술사
(min-oh@korea.ac.kr)

WPA3, Strong Security of WI-Fi

Concept	**(WPA3 정의)** - Wi-Fi Alliance 에서 WPA2 의 취약점을 수정하고 추가적인 보안 기능을 더해 2018 년 01 월에 발표한 Wi-Fi 보안 프로토콜
KeyWord	WEP, WPA, WPA2, WPA3, KRACK

WPA3 의 필요성

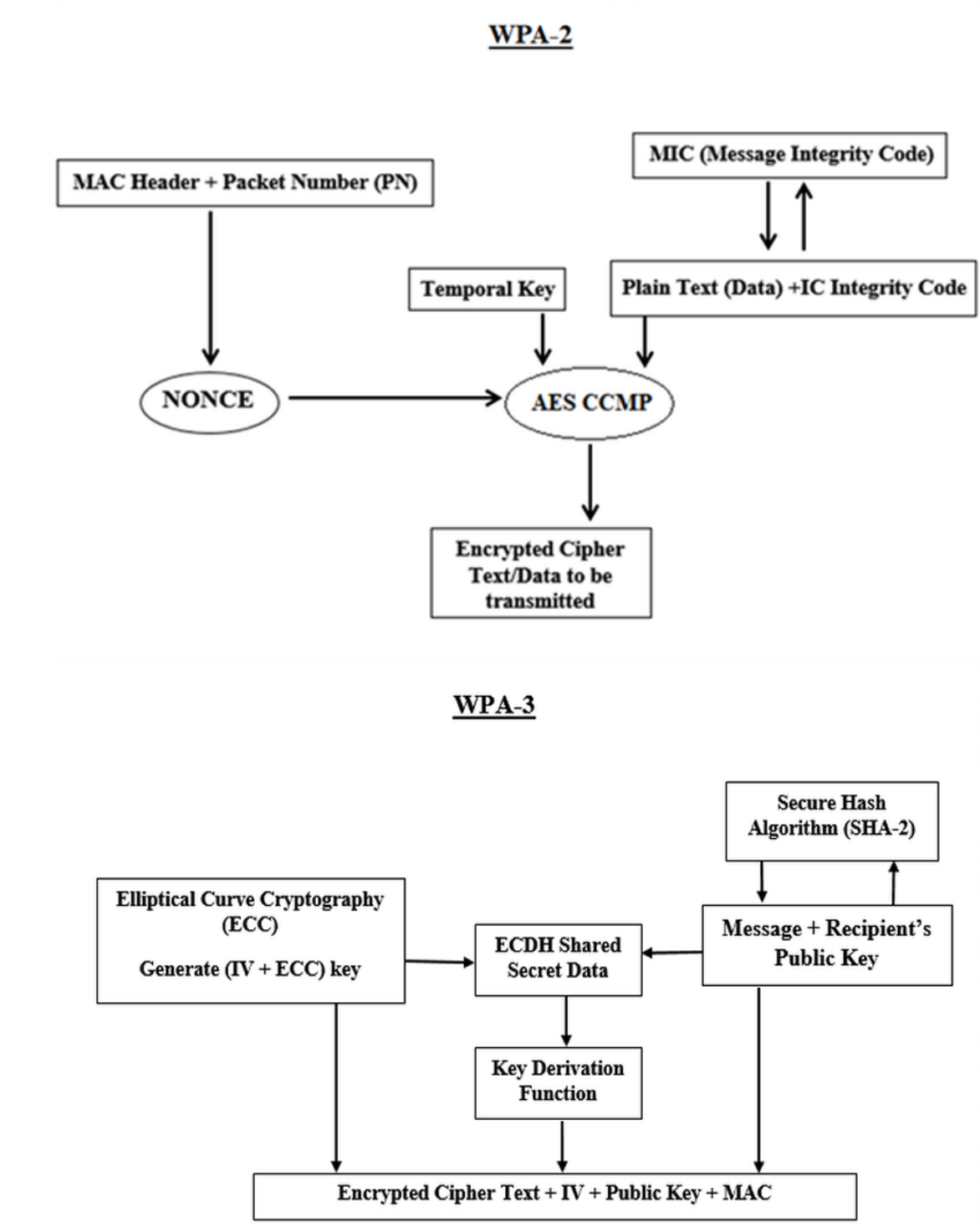
현재 와이파이는 우리의 일상 생활에서 가장 많이 사용되는 기술이다. 데스크톱 PC, 노트북, 테블릿 PC, 스마트폰까지 모두 Wi-Fi 을 사용하는 라우터를 통해 인터넷에 연결된다. 이것은 와이파이가 개인과 기업 어떤 환경이든 가장 편리하게 인터넷을 사용할 수 있는 기술이기 때문이다. 이렇게 가장 많이 사용하는 기술인 만큼 그 어떤 기술 보다도 보안이 중요한 기술이기도 하다. 와이파이의 보안은 WEP, WPA, WPA2 로 발전해 왔고 현재도 가장 많이 쓰이는 보안프로토콜은 WPA2 이다. 그러나 불행히도 2017 년 10 월 코드명 “KRACK”이라는 심각한 취약점을 통해 와이파이의 보안이 깨졌다. KRACK 의 취약점을 통해 공격자는 와이파이 네트워크에 대한 ACCESS 없이 사용자 데이터에 접근할 수 있었다. 이러한 WPA2 의 보안 취약점을 극복하고 보다 강력한 보안 기능을 장착하여 강력한 와이파이 보안을 위해 나온 기술이 WPA3 이다.

WPA3 는 어떻게 강력해 졌는가?

정보는 4 차산업혁명시대에 가장 중요한 자산이면서 가장 보호해야 할 영역이다. 결국 이러한 정보를 지키기 위해 가장 핵심적인 부분은 기밀성과 무결성을 보장하기 위한 암호화 영역이며 와이파이 보안 기술도 이러한 암호화 영역의 발전과정 이라고도 할 수 있다. 그러면 WPA3 는 이러한 부분에서 어떻게 강력해 졌는지 살펴보도록 하자.

우선 WPA3 는 높은 수준의 보안이 필요한 정부, 국방 및 산업 네트워크를 보호하는 CNSA (Commercial National Security Algorithm) 제품 군과 함께 192 비트 보안 제품 군을 사용한다. CNSA 암호화는 Elliptic Curve Diffie-Hellman (ECDH), Elliptic Curve 디지털 서명 알고리즘 및 Elliptic Curve Integrity Encryption Scheme (ECIES)와 같은 광범위한 암호화 체계와 프로토콜을 가진 Elliptical Curve Cryptography (ECC)를 사용한다. 또한 WPA3 는 DSA (Digital Signature Algorithm)를 이용하여 개인 키에서 직접 가져온 두 160 비트 숫자와 서명 할 데이터의 해시로 구성된 디지털 서명을 생성한다. 그리고 데이터 무결성을 보장하기 위해 SHA-2 알고리즘을 사용한다.

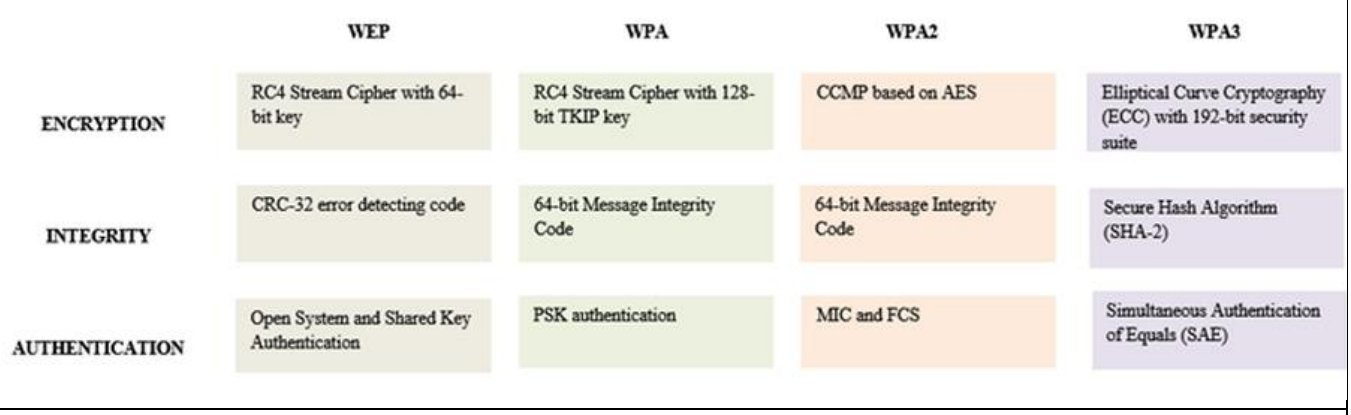
그림 1 은 WPA2 와 WPA3 의 암호화 프로세스를 비교, 도식화하여 보여 주고 있다.



[그림 1] WPA2 와 WPA3 의 암호화 Process 비교

도식화 된 그림을 보면 기존 WPA2 에서의 AES 알고리즘을 대체하여 WPA3 에서는 ECC 알고리즘을 사용하여 보다 강력한 암호화를 수행하고, 키유도함수 프로토콜인 SAE (Simultaneous Authentication of Equals)을 사용하여 보다 강력한 인증을 제공하며, SHA-2 알고리즘 기반의 MAC 을 통해 메시지의 무결성과 송신처인증을 수행하는 보다 안전한 보안 메커니즘들이 WPA3 에 적용 된 것을 볼 수 있다.

이러한 강력한 암호화를 기반으로 한 보안 서비스 영역에 대해 기존의 와이파이 보안 프로토콜 등과 WPA3 를 비교해 보면 그림 2 와 같이 요약될 수 있다.



[그림 2] 이전 보안 프로토콜과 WPA3 의 주요 보안 서비스 Spec 비교

이 외에도 WPA3 에는 흥미로운 보안 기능들이 추가 되어 있다.

첫번째로 WPA3 은 특정 횟수의 로그인 시도 실패 후 인증을 차단하는 Brute-Force 공격에 대한 보호 기능을 제공한다.

두번째로, WPA3 은 공공 개방형 Wi-Fi 네트워크에 향상된 보안 기능을 제공한다. WPA3 은 연결 시 암호가 입력되지 않은 경우에도 액세스 포인트와 사용자 간의 데이터를 암호화하는 개별화 된 데이터 암호화를 사용한다. 이는 사용자가 네트워크 접근 패스워드를 설정하지 않아도 공공네트워크 영역에서 보호 받을 수 있는 기능이다.

셋째로는 Amazon Echo, Google Home, Smart Door Locks, Smart Thermostats 등과 같은 디스플레이 인터페이스가 없거나 제한된 IOT (Internet of Things) 장치에 대한 보안 구성 과정을 단순화하여 쉬운 인터페이스를 제공한다는 점이다. 이러한 추가적 보안 기능을 요약하면 표 1 과 같다.

개선된 영역	내용	핵심사항
Brute-Force 공격 대응	무차별 공격 시도를 감지 네트워크로부터 통지	특정 횟수의 로그인 시도 실패 후 로그인 차단
공개된 네트워크에서의 프라이버시 보호	공개된 네트워크의 사용자가 개인별 암호화 적용	네트워크 패스워드 설정 불필요
Easy Configuration	스마트폰으로 탭하거나 QR 코트 스캔 등으로 접근권한 설정	IoT 기기 핵심

[표 1] WPA3 의 추가된 보안 기능들

WPA3 의 주요 동향

- ✓ 2018 년 01 월 와이파이얼라이언스 CES 에서 WPA3 발표
- ✓ 2018s 년 02 월 퀄컴은 802.11.ax 와 WPA3 를 적용한 와이파이칩 출시
- ✓ 2018 년 05 월 퀄컴은 향후 출시될 모바일 장치와 모든 와이파이 네트워킹 인프라 제품에 대해 와이파이 얼라이언스(Wi-Fi Alliance)의 3 세대 보안 제품군 WPA3(Wi-Fi Protected Access 3)을 칩셋으로 지원할 계획발표

아직은 지원되는 기기가 미흡하지만 빠른 시간 내에 WPA2 를 대체하고 안전한 와이파이 네트워크 사용을 지원할 것으로 보이며 향 후 출시 예정인 TLS1.3 과 같이 보다 안전한 네트워크 보안을 위해 역할을 할 것으로 보인다.

"끝"

Reference

1) http://www.zdnet.co.kr/news/news_view.asp?artice_id=20180521091417&type=det&re=
2) https://www.wi-fi.org/
3) https://www.copperpodip.com/
4) http://www.itworld.co.kr/news/107806