‘무선LAN’의 안전한 사용을 위한 보안대책

NCSC-TR050020

국가사이버안전센터
National Cyber Security Center

'무선LAN' 보안 취약성 고찰

① 무선LAN 보안 기술 동향
② 무선LAN 보안 취약성
③ 무선LAN 보안 대책

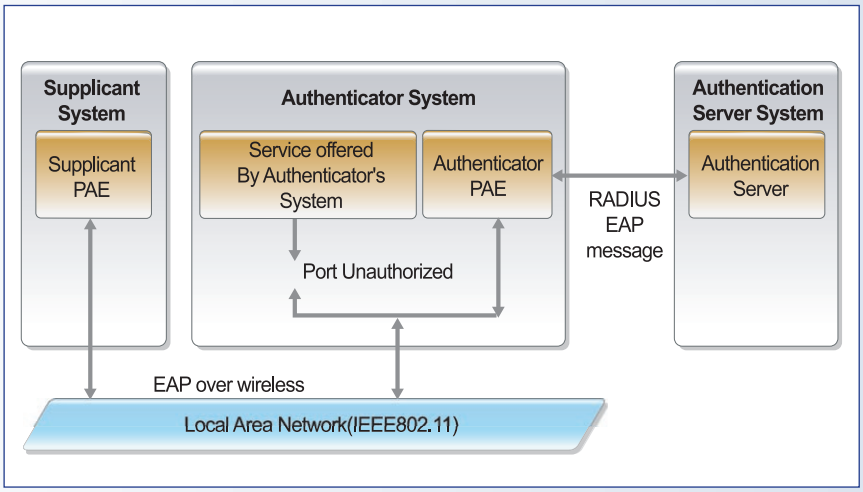
국가보안기술연구소 ▌최명길박사, mgchoi@inje.ac.kr

1. 서론

무선랜은 무선랜 표준에 따라 상이한 취약점을 가지고 있다. 이 글에서는 802.1X의 보안 취약점 및 WAP의 보안 취약점을 중심으로 서술한다.

2. 802.1x 개요

IEEE 802.1x는 무선랜을 목적으로 개발되지 않았지만, 무선랜 적용이 가능한 형태로 변하고 있다. IEEE 802.1x는 기존 802.3 미디어와 달리 매체를 공유하면서도 점대점(Point-to-Point) 형식의 연결을 취하고 있다. 또한, 물리적으로 같은 전송 매체를 사용하지만, 액세스포인트(AP)와 단말기를 결합한 가상의 포트 개념을 사용한다. 마치 유선상의 스위치 포트와도 같은 개념이다. 즉, 각 단말 결합상태를 인증(Controlled)과 비인증(Uncontrolled) 상태로 정의하여 액세스포인트 접근을 제어한다. (Monthly 사이버 시큐리티 7월호 참조)



[그림 1] IEEE 802.1x의 구조

[그림 1]과 같이 IEEE 802.1x 규격은 사용자(Supplicant), 인증자(Authenticator), 인증 서버(Authentication Server) 등 3 종류의 개체로 구성된다. 사용자(Supplicant)는 인증자가 요구하는 인증 정보를 요청 받고, 사용자 식별 정보(User Credential)을 전달한다.

인증자는 사용자에게 인증 정보를 요구하고, 전달 받은 인증 정보를 인증 서버에 전달한다. 또한 인증자는 사용자의 접속 포트 상태를 관리하며 인증 결과에 따라 포트를 인증 상태 혹은 비인증 상태로 설정한다. 인증 서버는 인증 서비스를 제공하는 개체로서 사용자 식별 정보를 사전 형태로 가지고 있다. 인증 서버는 논리적으로 인증자와 역할이 분리되지만 물리적으로는 인증자와 분리될 필요가 없다. IEEE 802.1x 규격은 사용자, 인증자, 인증 서버간의 전체적인 인증 메커니즘을 규정하고 있으며, 사용자와 인증자 사이에서는 확장 가능한 인증 프로토콜(Extensible Authentication Protocol, 이하 EAP)을 MAC 계 에서 사용한다.

3. IEEE 802.1x 보안 취약성

EAP-MD5의 프로토콜은 CHAP(Challenge Handshake Authentication Protocol)을 EAP에서 구현한 것으로 [그림 2]와 같다. EAP-MD5는 서버가 난수를 송신하면 클라이언트는 사용자 패스워드와 MD5 해쉬 함수를 이용하여 응답값을 전송한다. 서버는 송신한 난수와 서버에 저장된 사용자 패스워드를 이용하여 응답값을 생성한 후 클라이언트가 전송한 응답값과 비교하여 인증한다.

EAP-MD5는 동적 암호화 키를 생성할 수 없으므로 WEP 암호화를 하지 않거나, 암호화할 경우에는 정

적 WEP 키를 사용한다. 따라서 IEEE 802.1x 규격이 적용되지 않은 상태에서 발생할 수 있는 모든 형태의 도청 공격이 가능하다.

IEEE802.1x에서 EAP-MD5를 이용할 경우 가능한 공격은 다음과 같다.

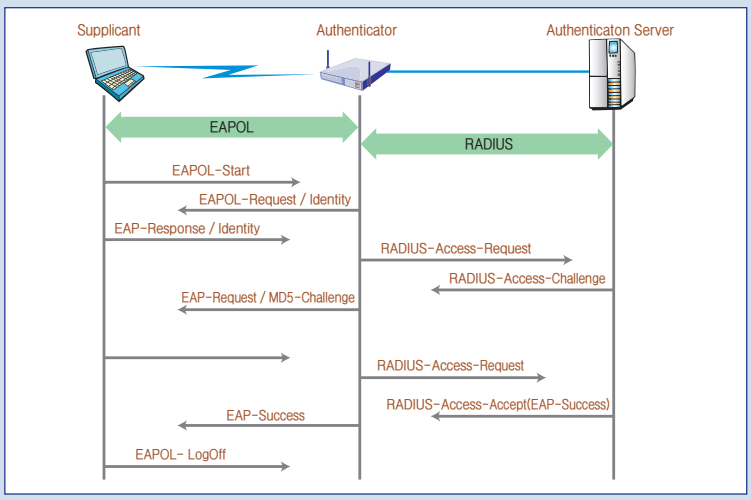
가. 오프라인 브루트-포스 공격(Off-line Brute-Force Attack)

[그림 2]와 같이 'EAP-Request/Identity' 메시지에 대한 응답 메시지인 'EAP-Response/Identity'는 사용자 ID를 전송한다. 따라서 공격자는 무선 구간을 도청하면 사용자 ID를 획득할 수 있다. 사용자는 (1)과 같이 서버가 생성한 난수값(CHN: Challenge Number), 비밀번호(PWA:password)를 MD5 함수로 해쉬값을 생성하여 EAP-Response로 송신한다.

$$RES_{PN} = HashMD5(EAP\ Identifier || PW_A || CHN) \text{ --- (1)}$$

공격자는 이 메시지를 도청하면 RES_{PN}값을 얻을 수 있다. 공격자는 EAP 패킷 형식의 일부인 EAP ID를 쉽게 도청할 수 있다. 공격자는 사용자 A의 비밀번호인 PW_A를 알 수 없다. 그러나 공격자가 PW_A 값을 추측해서 RES_{PN}값을 계산하여 획득한 RES_{PN}과 실제 RES_{PN}값이 일치하면 사용자의 PW_A와 공격자가 추측한 PW_A는 일치한다. MD5 함수가 단방향 해쉬함수로 공격자가 획득한 RES_{PN}과 계산한 RES_{PN}의 값이 일치할 때 사용자의 PW_A와 공격자가 추측한 PW_A가 일치하지 않는 경우는 확률적으로 거의 0에 가깝다.

현재 MD 크랙과 같은 MD5 알고리즘 브루트포스 공격은 8자리 숫자 패스워드의 경우 1분 이내 크래킹이 가능하고, 영문자, 소문자, 숫자가 섞여 있는 경우 8자리 이하의 패스워드는 약 1주 정도가 소요된다.



[그림 2] EAP-MD5 메커니즘

나. 중간자 공격 및 의인화 공격

EAP-MD5의 인증 프로토콜은 양방향 인증을 제공하지 않는다는 단점이 있다. 즉, 서버는 사용자를 인증하지만 사용자는 서버를 인증하지 않는다. 따라서 공격자가 단방향 인증의 단점을 이용하여 중간자 공격(Man-in-the Middle Attack)과 의인화(Impersonation) 공격을 할 수 있다.

중간자 공격은 사용자와 인증 서버간 트래픽을 중간에서 가로채는 방식이다. 중간자 공격은 트래픽을 가로채는 시점이 중요하다. 공개 인증(Open Authentication) 모드에서 동일한 ESSID를 사용하는 여러 대의 AP가 존재할 경우 사용자는 전파 환경이 더 나은 AP로 접속한다. 따라서 공격자는 가장(Rogue) AP를 이용해 중간자 공격을 시도한다. 사용자는 공격자 AP를 자신이 접속해야 할 AP로 착각하여 접속하고 EAP-MD5 프로토콜의 인증 절차를 진행한다. 공격자는 자신이 설치한 AP로부터 전송되는 데이터를 실제 사용자가 접속해야 하는 AP로 접속한다. 최종적으로 실제 AP로부터 인증 성공 메시지를 받고 네트워크에 대한 접근 허락을 받으면 공격자는 사용자에게 인증 실패 메시지만 전달한다. 이러한 방식으로 공격자는 사용자 ID와 패스워드를 모르는 상태에서도 네트워크에 접근할 수 있다. 그러나 중간자 공격은 무선에서는 큰 효과가 없을 수 있다. 사용자와 공격자간 무선 환경의 차이가 있어야 하며, 공격자가 네트워크 접근 권한을 획득했다 하더라도 사용자는 인증을 위해 재시도하는 경우가 많다. 따라서 공격자는 인증 재시도 방지 메커니즘을 사용해야 한다.

의인화 공격은 중간자 공격에 비해 현실적으로 가능성이 높은 공격 방법이다. 중간자 공격과 비슷하지만 차이점은 사용자로부터 데이터만 수집하여 실제 ID와 패스워드를 공격한다는 것이다.

다. 반복 공격(Replay Attack)

공격자는 무선 구간 트래픽을 가로채 사용자 ID와 EAP ID, 챌린지 난수값, MD5 응답값을 사전으로 만든다. 사전이 완성되면 공격자는 서버에 접속하여 인증을 시도한다. 공격자는 인증을 위해 EAP-Response/Identity 메시지를 전송하고, 서버가 전송하는 EAP-Request/MD5 챌린지 값을 사전에서 검색한다. 만약 사전의 데이터와 일치하는 데이터가 존재하면, 공격자는 일치하는 데이터를 사용하여 인증 시도를 하여 서버에 접속한다.

라. 서비스거부공격(DoS)

서비스 거부 공격은 공격자가 단말이나 네트워크의 사용 가능한 자원을 독점하여 사용자가 자원을 사용할 수 없게 한다. EAP 프로토콜의 메시지를 이용하면 서비스거부공격을 할 수 있다. 사용자는 인증 성공 여부를 알기 위해서 EAP 메시지를 서버로부터 전송 받는다. 그러나 EAP 메시지는 무결성 기능을 제공하지 않는다. 따라서 공격자는 AP로 위장하여 EAP 실패 메시지를 사용자에게 전송하여 서비스 이

용을 방해 할 수 있다.

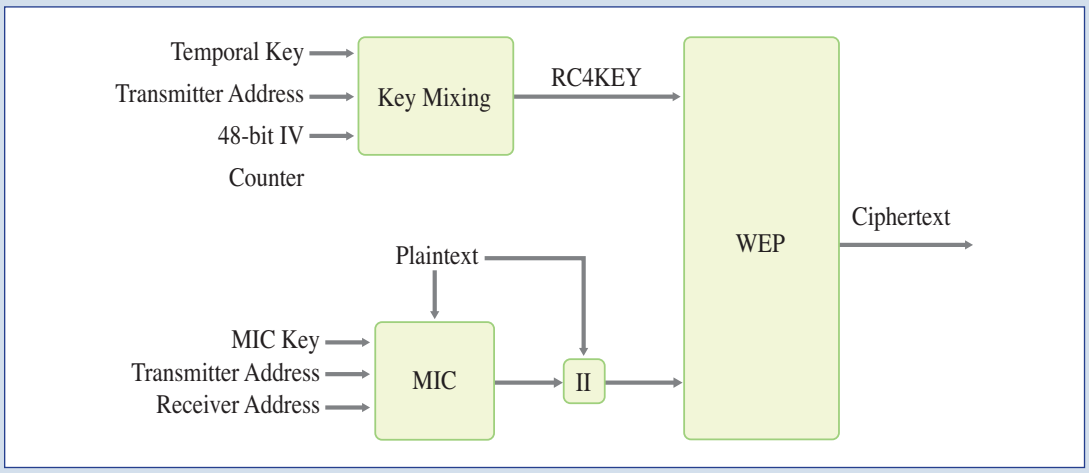
사용자는 통신 시작/종료 시 EAP-Logoff 및 EAP-Start 메시지를 서버에 전송한다. 공격자는 사용자로 가장하여 EAP-Logoff 및 EAP-Start 메시지를 AP에 전송하여 서비스 이용을 방해한다. EAP 패킷의 ID공격은 8비트를 사용하여 AP가 동시에 연결할 수 있는 세션은 255개이다. EAP 공격자는 AP에 255개 이상의 연결 요청 패킷을 전송하여 사용자의 AP 접속을 방해한다.

4. WPA 취약점

무선랜 보안 알고리즘인 WEP은 초기값(Initial Vector), 키 스트림 재사용, 키관리 방식, 무결성 취약점 등을 가지고 있다. 최근 802.11 WG 그룹은 Wi-Fi Protected Access(WPA)라는 보안 프로토콜을 제안하였다. 이 프로토콜은 WEP의 보안 취약점을 보완한다. WPA는 키 재사용 방지 및 키 분배를 위해 키 해쉬 함수 MIC와 802.1X 기반 키관리 방법을 사용한다. 그러나 WPA는 AP와 단말간에 사전에 공유한 키를 사용함으로 사전 공격 등에 취약하다. WPA의 취약성에 아래와 같다.

가. WPA의 임시키(Temporal Key) 해쉬 취약성

[그림 3]은 WPA 암호화(TKIP; Temporal Key Integrity Protocol) 과정이다. 키 해쉬 함수에 16바이트의 임시키(Temporal Key), 6바이트 송신자 주소(Transmitter Address)와 48비트 초기값(Initial Vector)를 입력하면, 16바이트 RC4키가 출력된다. 48비트 초기값은 시퀀스 카운터로 동작하며 한 사이클이 지나면 증가한다. 16바이트 RC4키는 WEP 프레임에 사용되며 1개 패킷마다 변경된 Perpacket



[그림 3] TKIP 암호화 과정

Key을 생성한다. 초기값 카운터는 재사용공격(Replay Attack) 방지를 위해 사용되며, 수신측은 수신한 초기값 카운터가 이전에 수신한 패킷 초기값보다 작으면 패킷을 기 한다. MIC는 메시지 무결성 보장을 위해 사용된다. [그림 3]과 같이 MIC의 입력은 MIC키, 송신자 및 수신자 주소, 메시지 등이며 출력은 MIC-Tag를 결합한 메시지이다.

1) 키 혼합(Key Mixing) 함수

TKIP(Temporal Key Integrity Protocol)은 임시키 해쉬(Temporal Key Hash)라고 정의된 키 혼합 함수를 사용한다. [그림 4]와 같이 키 혼합 함수의 입력값은 임시키(TK), 송신자 주소(Transmitter Address), 48 비트 초기값(IV)이며, 출력값은 128비트 WEP 키이다. 128비트의 WEP키 중 24비트는 초기값으로부터 유도된다. 48비트의 초기값 중 LS(Least Significant) 16 비트를 IV16, 32 MSB(Most Significant Bit)는 IV32라 한다. 키 혼합 함수는 아래와 같은 2단계로 요약할 수 있다.

P1K=Phase1(TK, TA, IV32) (1단계)
RC4Key=Phase2(P1K, TK, IV16) (2단계)

1단계는 2^{16} 패킷마다 한번씩 수행되며, 입력값은 송신자 및 수신자 주소, IV32이며, 출력은 P1K로서 2단계의 입력값으로 사용된다. 2단계는 P1K, TK, IV16을 입력으로 하며 출력은 128 비트의 WEP 키이다. TK은 8비트 바이트의 배열 [0.15]이다. S 박스는 비선형 함수이며 16비트의 입력과 16비트 출력이다.

2) 임시키 해쉬 공격

공격자는 같은 IV에서 계산한 소수 비트의 RC4 키를 알고 있다고 가정한다. 가정에서 공격자는 쉽게 TK(Temporal Key)를 계산할 수 있어 패킷을 복호화할 수 있다. 이 공격은 2^{32}의 단순한 연산에 의한 복잡도를 가지고 있다. 공격은 TK를 추출하기 위해서 기본적으로 Phase2를 역산한다. P1K 값은 IV32가 변하기 전에는 변화하지 않으므로 추측한 TK값의 오류를 체크할 수 있다.

나. WPA-PSK의 취약점

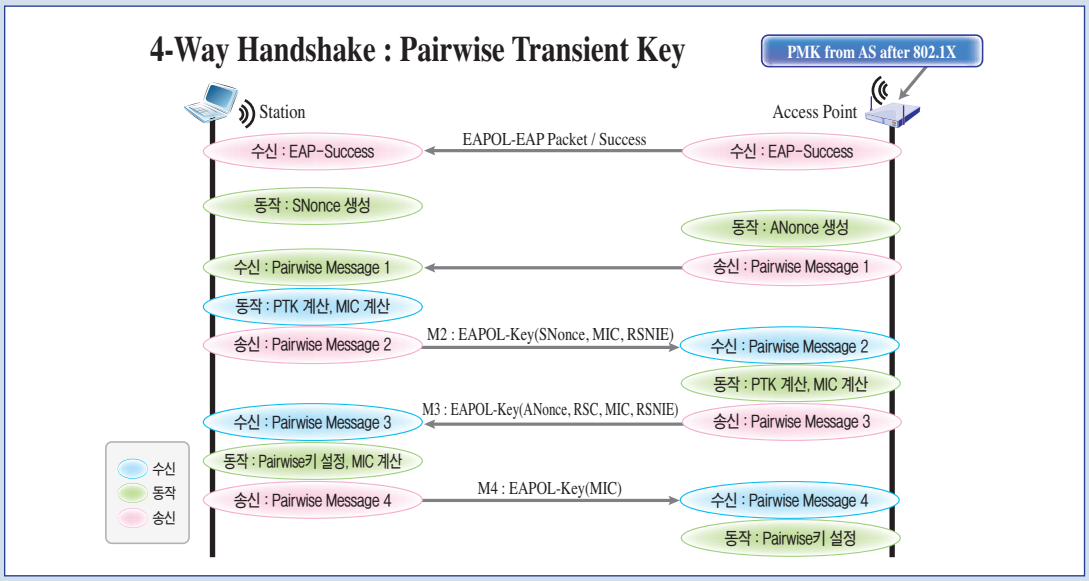
WPA에서 802.1x가 이용되지 않는 곳에서는 PMK(Pairwise Master Key) 대신 PSK(Pre-Shared Key)를 이용한다. PSK는 256 비트이거나 8~63 바이트로 이루어진 패스워드(Passphrase)이다. 각 단말은 자신의 MAC 주소와 연관된 PSK를 가지고 있어야 하나 ESS를 위한 하나의 PSK만을 제공하고 있다. 256비트의 PSK는 아래와 같이 PMK로 이용할 수 있다.

PMK = PBKDF2(passphrase〈PSK〉, ssid, ssidLength, 4096, 256)

PBKDF2는 PKCS #5 v2.0: Password-based Cryptography Standard에서 기술된 키 유도 방법이다. PBKDF2는 패스워드, SSID, 그리고 SSID 길이를 결합한 스트링을 256 비트로 생성하기 위해 4096번 해쉬한다. PTK(Pairwise Transient Key)는 가상난수함수에 PMK, 무선 단말, AP의 MAC 주소, 단말과 AP가 생성한 난수를 결합하여 유도된다.

1) 내부 PSK 공격(Intra-PSK Attack)

[그림 4]는 EAPOL 메시지를 이용한 4단계 키교환 프로토콜을 나타낸다. 키 교환 프로토콜을 이용한 연결(Associate)을 위해서 무선 단말과 AP는 상대방의 MAC 주소, 난수를 송수신한다. 따라서 공격자는 프레임을 가로채어 PTK를 생성할 수 있다. 공격자가 프레임을 가로채지 못한다면 무선 단말에게 연결 거절(Disassociate) 메시지를 전송한다. 무선 단말이 AP와 접속을 끊은 후 공격자는 단말을 4단계 키교환 프로토콜을 이용하여 AP와 다시 연결(Associate)한다.



[그림 4] PTK 생성을 위한 4단계 핸드세이크

2) 오프라인 PSK 공격(Offline PSK Dictionary Attack)

패스워드는 캐릭터당 약 2.5 비트의 보안 강도를 가지고 있다. 그러므로 n 바이트의 패스워드는 2.5n+12비트의 보안을 가진 키와 동일한 효과를 가지고 있어 패스워드는 비교적 보안 강도가 낮다. 따라서 짧은 길이의 패스워드를 통해 생성된 키들은 사전 공격에 취약하다. 20캐릭터 미만의 길이에서 유추된 키는 사전 공격을 당할 수 있다. 4단계 키교환 프레임의 해쉬값 생성을 위해 PTK를 사용한다. 따

라서 공격자는 해쉬값에 대한 오프라인 사전 공격을 감행할 수 있으며, 8캐릭터 미만의 패스워드는 사용자가 사전에서 쉽게 선택하여 공격을 시도할 수 있다. 이 공격은 WEP 공격보다 쉽게 감행할 수 있다.

5. 결 론

공간으로 데이터를 송신하는 무선랜은 유선랜과 달리 무선전파의 특성을 가지고 있어 여러 가지 공격에 노출되기 쉽다. 현재 상용 무선랜 보안 기술로 널리 알려진 WEP은 RC4 알고리즘을 이용한다. RC4 알고리즘은 IV 의 평문 전송, 키스트림의 단순성 등으로 인해 해킹이 쉽다. 따라서 무선랜 보안 강화를 위해 WPA라는 기술이 대안으로 거론되고 있다. 그러나 WPA-PSK가 짧은 길이의 패스워드로 구성되면, 공격자는 키교환 데이터 프레임을 가로채어 패스워드를 쉽게 알아낼 수 있다.

무선랜 표준화 그룹은 WPA보다 더 강력한 암호 알고리즘인 CCMP 알고리즘을 기본 알고리즘으로 정의하고 있는 RSN 보안 규격을 제정 중이다. 그러나 RSN 보안은 장기적인 관점에서 암호 알고리즘 처리 모듈을 하드웨어 칩셋으로 구현하고 하고 있다. RSN 보안은 칩셋 구현을 통해 사용될 수 있어 상용화에는 상당한 시일이 소요될 것으로 예측된다.

이번 글에서는 상용 무선랜 보안 기술의 취약점에 대해 알아 보았으며 다음 에는 마지막으로 무선랜 보안 대책에 대해서 살펴보도록 한다.

참 고 문 헌

1. 무선랜 WPA 보안 핵심기술, [IT 리포트], 한국기술거래소, 2004.10
2. 무선 LAN 보안 체크리스트, on the net, 2005.3.
3. 무선 LAN 보안 기술, 정보화학회
4. IEEE 802.11을 중심으로 한 무선 LAN 바이블, 세화, 2003.
5. 네트워크 사용자를 위한 무선 LAN 기술강좌, 성안당, 1996.
6. 802.11 Wireless Networks: The Definitive Guide, O'Reilly, 2002.
7. Wireless LANs, SAMS, 2001.
8. 무선 LAN 중심의 모바일 통신 기술, Ohm, 2002.
9. IEEE Std 802.11, Standards for Local and Metropolitan Area Network: Wireless Lan Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999
10. Airsnort, airsnort.shmoo.com
11. Vebjorn Moen, Havard Raddum, Kjell J,Hole: Weakness in the Temporal Key Hash of WPA,
12. Weakness in Passphrase Choice in WPA Interface: http://wifinetnes.com/archives/002452.html