Journal of the Korea Academia-Industrial cooperation Society
Vol. 13, No. 4 pp. 1839-1848, 2012

http://dx.doi.org/10.5762/KAIS.2012.13.4.1839

Wi-Fi를 이용한 스마트폰에서 사전 공격에 안전한 WPA-PSK 프로토콜

박근덕[1], 박정수[2], 하재철[2*]
[1]호서대학교 컴퓨터공학부, [2]호서대학교 정보보호학과

A Secure WPA-PSK Protocol Resistant to Dictionary Attack on Smartphone Communication Using Wi-Fi Channel

Geun-Duk Park[1], Jeong-Soo Park[2] and Jae-Cheol Ha[2*]
[1]**Division of Computer Engineering, Hoseo University,**
[2]**Dept. of Information Security, Hoseo University**

요 약 최근 스마트폰에서는 Wi-Fi 통신 기술을 이용한 인터넷 서비스가 활성화 되어 있으며 스마트폰 사용자와 무선 AP(Access Point)간의 전송 데이터 보호를 위해 WPA 보안 프로토콜을 사용하고 있다. 하지만 WPA-PSK 프로토콜의 경우 사전 공격(dictionary attack)에 매우 취약한 특성을 보이고 있다. 따라서 본 논문에서는 WPA-PSK에서 발생하는 사전 공격을 방어할 수 있는 안전한 WPA-PSK 프로토콜을 제안하고자 한다. 제안 프로토콜에서는 Diffie-Hellman 키 합의 기술과 PSK(Pre-Shared Key)의 비밀 속성을 접목하여 암호화키를 생성하도록 설계하였기 때문에 사전 공격은 물론 외부자의 의한 중간자 공격(Man-In-The-Middle attack) 그리고 Rogue AP 위장 공격도 방어할 수 있다.

Abstract Recently, smartphone communications using Wi-Fi channel are increasing rapidly to provide diverse internet services. The WPA security protocol was used for data protection between user and wireless AP. However, WPA-PSK protocol was known to be weak to the dictionary attack. In this paper, we proposed a secure WPA-PSK protocol to resist the dictionary attack. Since the proposed method was designed to generate a strong encryption key which is combined the Diffie-Hellman key agreement scheme with secrecy property of PSK(Pre-Shared Key), we can protect the Wi-Fi channel from Man-In-The-Middle attack and Rogue AP impersonation attack.

Key Words : WPA-PSK, Dictionary Attack, MITM Attack, Rogue AP Impersonation Attack

1. 서론

최근에는 스마트폰의 빠른 보급과 이동 통신망의 발달로 인해 시간과 장소에 상관없이 인터넷 서비스를 사용할 수 있게 되었다. 스마트폰을 사용하는 사용자에게는 3G, LTE, WIBRO 등 다양한 이동 통신망이 제공이 되는데 현재 3G 통신망을 주로 이용하고 있다. 이외에도 학교, 지하철, 백화점, 회사, 카페 등에 설치된 Wi-Fi(WLAN)를 통한 무선 접속 기술도 제공되고 있다[1]. Wi-Fi망은 고속이면서 보통 무료로 제공되기 때문에 보통 3G 이동통신망을 이용하다가도 Wi-Fi망으로 전환하여 인터넷 서비스를 이용할 수 있다. 스마트폰 이외에도 인터넷 전화기, IPTV 등 인터넷을 사용하는 IT 기기가 등장함에 따라 가정에서도 무선 공유기를 설치하여 Wi-Fi를 사용하고 있다.

그러나 Wi-Fi 무선 네트워크는 유선과 달리 전파 통신

이 논문은 2011년도 호서대학교의 재원으로 학술연구비 지원을 받아 수행된 연구임.(2011-0267)
*Corresponding Author : Jae-Cheol Ha
Tel: +82-10-4330-6886 email: jcha@hoseo.edu
접수일 12년 01월 25일 수정일 12년 03월 15일 게재확정일 12년 04월 12일

을 하기 때문에 Airodump, Kismet과 같은 무선 네트워크 스니핑 툴을 사용한 메시지 도청에 취약하다[2]. 따라서 IEEE에서는 무선 네트워크에서 유선과 동등한 보안을 제공하기 위해 WEP(Wired Equivalent Privacy)라는 보안 프로토콜을 도입하였다[3]. 그러나 2001년 초에 WEP에 사용되는 RC4 알고리듬의 취약점으로 인해 비밀키가 노출될 수 있음이 밝혀졌다[4,5]. 그 후 2003년에 WEP 보안을 위한 대안으로 IEEE에서는 WPA(Wi-Fi Protected Access)이라는 보안 프로토콜을 발표하였다[6].

WPA에는 OllehWiFi, LG U+ Zone, T WiFi Zone과 같이 통신 사업자가 제공하는 별도의 인증 서버를 두어 사용자를 인증하는 방식이 있으며, 집, 소규모 회사, 공공장소, 카페 등에서 사전에 공유된 키를 이용하여 사용자를 인증하는 방법으로 나누어지게 된다. 이 중에서 사전에 공유된 키를 이용하는 방법을 WPA-PSK(Pre-Shared Key) 방식이라 부른다.

WPA-PSK을 이용하여 무선 보안을 제공할 때에는 무선 공유기에 사전 공유키가 설정되어 있어야 한다. 현재 출시되는 공유기는 기본적으로 WPA-PSK 보안 정책을 사용하도록 되어 있다. 통상 제품 출하 시 기본 패스워드가 설정되어 있지만 사용자가 고유의 패스워드로 재설정하여 사용하고 있다. 그런데 무선 공유기의 패스워드가 노출되면 전송 데이터가 도청당할 수가 있기 때문에 이 패스워드가 데이터 기밀성을 유지하는 핵심이 된다. 특히, 패스워드의 길이가 너무 짧거나 공격자가 유추하기 쉬운 패스워드를 사용한다면 사전 공격(dictionary attack)에 의해 패스워드가 쉽게 노출될 수 있다[7]. 또한 Wi-Fi 무선 네트워크에서는 도청된 정보를 이용하여 불법적인 제 3자가 정당한 사용자의 세션 ID를 가로채 정당한 사용자로 위장하여 로그인을 하는 세션 하이재킹 공격이 가능하다[8].

최근 WPA-PSK에 대한 사전 공격에 대응하기 위해 Diffie-Hellman 키 합의 기법(key agreement)[9]을 활용하여 암호화키를 생성하는 방법이 Mano 등에 의해 제안되었다[10]. 하지만 이 방법의 경우 Diffie-Hellman 키 합의 프로토콜의 취약점인 중간자 공격(Man-In-The-Middle attack, MITM attack) 문제를 그대로 내포하고 있다[11]. 즉, 무선 네트워크의 사용자와 AP(Access Point) 사이에 공격자가 위치하여 통신 정보를 중계하는 역할을 함으로써 전송 데이터를 그대로 도청할 수 있다. 또한 합의된 암호화키가 사전 공유키(PSK : Pre-Shared Key)와 연관이 없기 때문에 Rogue AP 위장 공격(Rogue AP impersonation Attack)을 당할 수 있다[12]. 따라서 Mano 등의 프로토콜은 완벽한 보안을 제공하지 못한다.

따라서 본 논문에서는 WPA-PSK에서 사전 공격뿐만 아니라 중간자 공격과 Rogue AP 위장 공격을 방어할 수 있는 안전한 WPA-PSK 프로토콜을 제안하고자 한다. 이 방식은 통신을 위한 세션 키를 생성하는데 사전 공유키를 사용함으로써 사전 공유키를 알지 못하는 제 3자에 의한 중간자 공격을 방어하고 Rogue AP 위장 공격을 예방할 수 있다. 또한 제안 프로토콜은 안전성 제공을 위해 추가되는 계산량과 데이터 전송량이 최소화되도록 설계하였다.

2. 무선 네트워크 보안 프로토콜

2.1 WEP

무선 네트워크는 유선 네트워크와 다르게 통신 메시지가 외부에 노출되기 때문에 보안 프로토콜이 필수적으로 요구되었다. 이러한 요구에 따라 1999년 에 발표된 무선 네트워크 표준 IEEE 802.11b에 보안 프로토콜이 포함되었다. 이 보안 프로토콜을 유선과 동등한 보안성을 제공한다는 의미로 WEP(Wired Equivalent Privacy)라 명명되었으며, AP에서 사전 공유키를 이용하여 사용자를 인증하는 방법을 채택하였다. 그러나 2001년 초, 무선 네트워크에서 보안을 제공했던 WEP는 WEP에서 사용되는 RC4의 키 스케줄링 알고리듬과 초기 벡터 사용법의 취약점으로 인해 비밀키가 복구되는 문제가 발생하였다[4,5]. 이러한 보안 취약점을 보완하기 위해 IEEE 802.11 위원회에서는 WEP의 대안으로 WPA를 발표하였다.

2.2 WPA

WPA는 WiFi-Alliance에서 개발하고 있던 무선 보안 프로토콜로서 IEEE 802.11 위원회에서 승인되어 IEEE 802.11i 문서에 포함되어 있다. WPA는 무선 네트워크에서 안전성을 제공하기 위해 사용자 인증 방식, 키 교환 방식, 암호화 알고리듬 등을 정의하고 있다. WPA의 사용자 인증 방식은 미리 공유된 키인 PSK를 이용하여 사용자를 인증하는 방법인 WPA-Personal과 RADIUS 서버와 같은 인증 서버를 별도로 두어 사용자를 인증하는 방법인 WPA-Enterprise로 나눌 수 있다.

IEEE 801.11i에는 제공하는 무선 보안 프로토콜은 표 1에서 보는 바와 같이 크게 WPA-1과 WPA-2로 분할되는데 두 버전은 인증방식은 동일하나 사용하는 암호 알고리듬이 다르다. 즉, WPA-1은 TKIP(Temporal Key Integrity Protocol)을 사용하고, WPA-2는 CCM(Counter mod with CBC-MAC) 모드로 운용되는 AES 암호 알고리듬을 사용한다[13-15].

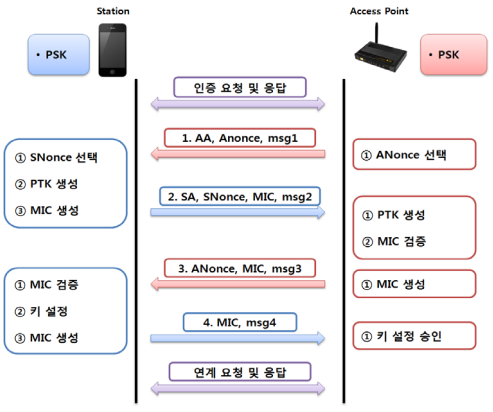
[표 1] WPA의 인증 방식과 암호 알고리듬
[Table 1] Authentication and encryption algorithm of WPA

구분	인증 방식	암호 알고리듬
WPA-1	PSK or Radius 인증 서버	RC4-TKIP
WPA-2	PSK or Radius 인증 서버	AES-CCMP

TKIP는 기존 WEP에서 사용한 보안 프로토콜을 기반으로 키 값의 난수 발생 영역을 확장하였고 데이터 무결성을 위해 CRC-32를 사용하였다. 그러나 WPA-1에서는 여전히 RC4 암호 알고리듬을 사용하고 있고 별도의 키 관리 기법을 제공하지 않고 있어 WEP가 가지고 있던 기본적인 취약성을 대부분가지고 있다.

CCMP-AES는 TKIP를 보완하기 위해 만들어진 암호 프로토콜로 AES 암호 알고리듬을 이용하여 강력한 암호 기능을 제공한다. 암호화 과정에서 MAC 헤더의 일부인 추가 인증 데이터(Additional Authentication Data)를 입력으로 포함시켜 위조 공격을 예방하며 패킷 번호(Packet Number)를 이용하여 재생 공격(replay attack)을 방어한다.

무선 네트워크를 이용하여 전송되는 데이터를 암호화하여 전송할 때에는 무엇보다도 암호화키가 가장 중요하다. WPA-PSK는 그림 1과 같이 암호화에 사용되는 키인 PTK(Pairwise Transient Key)를 생성한다.



[그림 1] WPA-PSK 프로토콜
[Fig. 1] WPA-PSK protocol

WPA-PSK에서는 AP 개통 시 설정된 8~63바이트인 패스워드 PW(PassWord)를 사용하여 미리 공유된 키 PSK를 생성한다. PSK를 생성하는 방법은 (식 1)과 같다. 여기서 PBKDF2는 패스워드 기반 키 유도 함수(Password-Based Key Derivation Function) V2를 의미하며 SSID(Service Set IDentifier)는 AP의 고유 ID를 나타낸다.

$$PSK=PBKDF2(PW,SSID,SSID길이,4096,256) \quad (1)$$

PBKDF2는 키 생성 함수로서 입력을 4096번의 해쉬(Hash) 수행 후 256비트의 결과를 출력한다. PSK는 AP 및 PW를 알고 있는 사용자에 의해 생성되며 PW를 알고 있는 사용자를 내부 사용자 혹은 정당한 사용자라 한다. 사용자에 의해 계산되어 얻어진 PSK는 암호화 통신을 위한 대칭키인 PTK를 생성하기 위해 사용된다. PTK를 생성하기 위해서 그림 1과 같은 4단계 핸드쉐이크 과정(4-way handshake)을 거쳐서 얻은 파라미터들과 PSK를 이용하여 (식 2)와 같이 계산한다. 이 때 PTK는 PRF(Pseudo Random Function) 함수를 이용하여 생성되며 512비트의 출력을 갖는다. 여기서 Station은 사용자의 장비를 의미하며 AP와 주고받는 난수를 SNonce와 ANonce로 표기하였다.

$$PTK = PRF\text{-}512(PSK, \text{“Pairwise key expansion"}, Min(AA, SA) \| Max(AA, SA) \| Min(SNonce, ANonce) \| Max(SNonce, ANonce)) \quad (2)$$

또한, WPA-PSK 프로토콜에서는 메시지 인증 코드인 MIC(Message Integrity Code)이라는 정보를 교환하면서 PTK의 무결성을 검사하게 되는데 MIC를 생성하는 방법은 (식 3)과 같다.

$$MIC = HMAC(PTK, \text{전송되는 파라미터들}) \quad (3)$$

HMAC로 사용되는 해쉬 함수는 MD5나 SHA1을 사용할 수 있으며, SHA1을 사용할 경우 160비트 중 128비트만을 사용한다. “전송되는 파라미터들”은 MIC이 전송될 때 같이 전송되는 파라미터들로 메시지나 임시 정보(nonce)를 의미한다. 즉, MIC은 전송되는 파라미터의 무결성과 정상적으로 PTK가 만들어졌는지를 판단하는 기준이 된다.

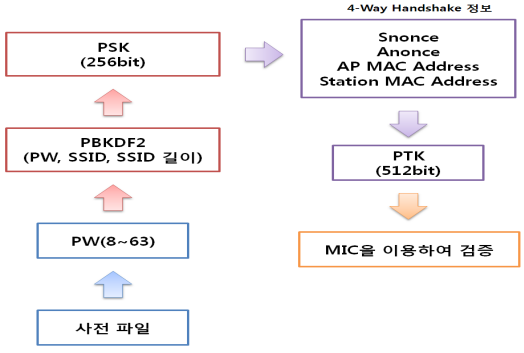
3. WPA-PSK에 대한 사전 공격

3.1 사전 공격

WPA-PSK 사전 공격은 AP와 사용자들이 공유하는 패

스워드를 사전 파일을 이용하여 찾아내는 공격으로 WPA-PSK를 이용하여 무선 네트워크를 구성할 때 패스워드를 짧게 설정하거나 추측하기 쉬운 값으로 설정을 하였다면 아주 쉽게 패스워드를 추출할 수 있다. 즉, 2장의 (식 1)과 (식 2)를 이용하여 생성되는 PSK와 PTK는 안전해 보이지만 사전 공격에 취약하다. 그 이유는 그림 1에서 보는 바와 같이 PTK를 생성할 때 사용되는 파라미터 중 패스워드를 제외한 나머지 파라미터가 무선 채널상에 모두 노출되기 때문이다. 따라서 공격자는 패스워드 하나만 사전에서 추측하여 특수한 검증식을 만족하는지 확인하면 된다. WPA-PSK에서 공격자는 패스워드가 맞는지 검사하기 위해 4단계 핸드쉐이크에서 전송되는 MIC을 이용한다. WPA-PSK 사전 공격은 그림 2와 같이 요약할 수 있으며 아래와 같은 절차에 따라 수행된다.

① 공격자는 무선 스니핑을 통해 4단계 핸드쉐이크 과정에서 교환되는 모든 정보를 도청한다.
② 공격자는 사전 파일에 있는 추측된 단어를 이용하여 PSK를 생성한다.
③ 생성된 PSK와 도청한 파라미터들을 이용하여 PTK를 생성한다.
④ PTK의 일부분은 MIC의 해쉬키로 사용되기 때문에 생성된 PTK의 해쉬키로 MIC을 생성한 후 도청한 MIC 값과 비교한다.
⑤ 만약에 같다면 PSK를 생성할 때 사용된 단어가 AP와 Station간의 패스워드가 된다. 같지 않다면 다른 사전의 단어를 이용하여 단계 2부터 4까지를 반복한다.



[그림 2] WPA-PSK 프로토콜 사전 공격
[Fig. 2] Dictionary attack on WPA-PSK protocol

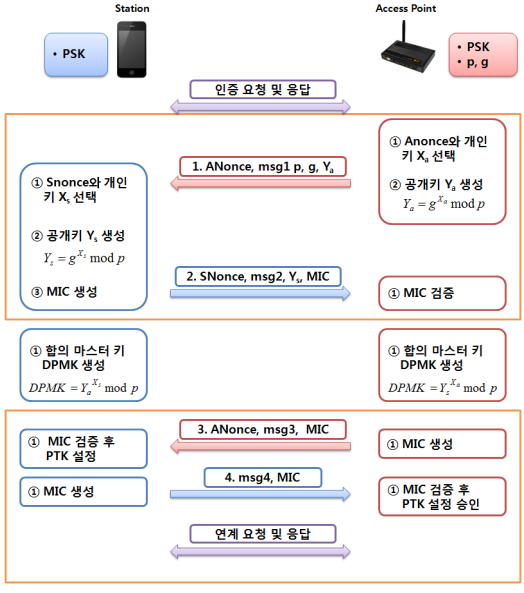
이러한 사전 공격은 WPA-PSK에서만 적용이 가능하며 WPA-Enterprise에서는 인증 서버로부터 사용자 인증 후 PMK(Pairwise Master Key)를 발급을 받기 때문에 사전 공격 자체가 불가능하다.

3.2 Mano 등의 사전공격 대응 방법

WPA-PSK 사전 공격을 방어하고자 2006년 Mano 등은 WPA-PSK의 4단계 핸드쉐이크 과정에서 Diffie-Hellman 키 교환을 사용한 대응 방법을 제안하였다. Mano 등이 제안한 방법은 그림 3과 같다. 이 방법의 핵심은 Diffie-Hellman 키 합의를 통해 DPMK(Dynamic Pairwise Master Key)를 만들고 이를 이용하여 (식 4)와 같이 PTK를 생성하고자 하는 것이다.

PTK = PRF-512(DPMK, “Pairwise key expansion", Min(AA, SA) || Max(AA, SA) || Min(SNonce, ANonce) || Max(SNonce, ANonce) (4)

원래 이 대응 방식은 내부자의 도청공격, 외부자의 사전 공격이나 전수조사 공격(brute-force attack)을 방어할 목적으로 제안되었다. 그림 3에 제시된 프로토콜을 살펴보면 외부자의 공격을 막기 위해 PTK를 생성하는데 사용되는 DPMK를 Diffie-Hellman 키 합의에 의해 생성한다. 따라서 X_a와 X_s를 알지 못하는 공격자가 DPMK 값 $g^{Xs \cdot Xa} \bmod p$를 계산하는 것은 이산대수 문제(discrete logarithm)에 근거하여 불가능하다. 따라서 이 프로토콜은 암호화키인 PTK를 노출하지 않으므로 결국 사전 공격을 방어할 수 있다.



[그림 3] Mano 등의 WPA-PSK 프로토콜
[Fig. 3] WPA-PSK protocol of Mano et al.

그러나 이 방법은 2가지의 취약점을 내포하고 있다. 첫 번째, Diffie-Hellman 키 합의가 가지고 있는 근본적인 문제인 중간자 공격을 가지고 있다. 공개키에 대한 별도의 인증 기법이 존재하지 않는 한 결국 사전 공유키를 알지 못하는 외부 공격자에 의해 중간자 공격을 통한 세션 하이재킹 등이 가능하다는 문제가 존재한다.

두 번째, 합의 마스터키인 DPMK 생성 시 DPMK와 PSK는 서로 관련성이 없기 때문에 Rogue AP 위장 공격이 가능하다. Rogue AP 위장 공격이란 공격자가 Rogue AP(불법적인 AP)를 정상적인 AP로 위장하여 사용자를 접속시킨 후 정보를 해킹하는 공격이다. 사용자가 Rogue AP를 이용하여 인터넷 서비스를 이용한다면 공격자는 모든 통신 메시지를 도청할 수 있다. 스마트폰이 이 공격에 더욱 위험한 이유는 스마트폰에서는 AP와 연결을 할 때 신호 세기가 가장 높은 것과 자동 연결을 하기 때문이다.

Rogue AP 위장 공격 시나리오는 다음과 같다.

① 공격자는 정상적인 AP와 정보(SSID, 암호화 방식)가 같은 Rogue AP를 생성하여 정상적인 AP로 위장한다.

② Station은 Rogue AP를 정상적인 AP로 판단하고 Rogue AP에 접속 요청을 한다.

③ Station의 접속 요청에 의해 Rogue AP는 키 합의를 위한 4단계 핸드쉐이크 과정을 수행한다.

④ Rogue AP는 그림 4와 같이 4단계 핸드쉐이크 과정 중에 2 단계에서 AP의 MIC 검증부분을 검증 없이 통과한다.

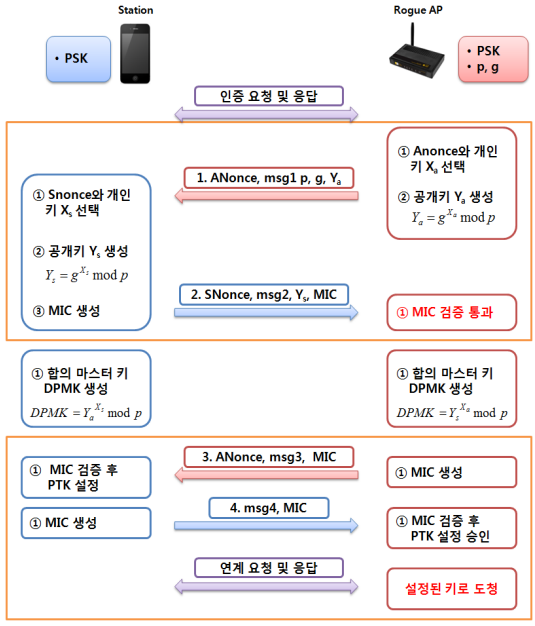
⑤ 암호화 통신을 위한 합의 마스터키 DPMK를 생성하게 되는데 이 DPMK는 PSK와 연관성이 없기 때문에 PSK를 모르는 Rogue AP에서도 DPMK를 생성할 수 있다.

⑥ Station과 Rogue AP에서 생성한 DPMK는 같게 되므로 Station과 Rogue AP간의 통신이 가능해진다. 결국 Station은 Rogue AP인지 모르고 네트워크를 사용하게 되므로, 공격자에게 모든 통신 메시지가 도청 당하게 된다.

Mano 등의 프로토콜에서 Rogue AP 위장 공격이 가능한 이유는 PSK가 연관되지 않는 DPMK를 생성하므로 공격자가 의도한 AP를 만들어 통신할 수 있기 때문이다. 즉, 정당한 핸드쉐이크 과정에서 얻어진 파라미터들로 Rogue AP는 Station이 가진 DPMK를 생성할 수 있는 것이다.

4. 제안하는 사전 공격 대응 프로토콜

본 논문에서는 기존 WPA-PSK 프로토콜에서 발생되는 사전 공격을 방어하고, Mano 등의 프로토콜에서 문제가 되었던 외부 공격자에 의한 중간자 공격과 Rogue AP 위장 공격을 방어하는 향상된 WPA-PSK 프로토콜을 제안하고자 한다. 제안하는 프로토콜에서 사용할 표기는 다음 표 2와 같다.



[그림 4] Rogue AP 위장 공격
[Fig. 4] Rogue AP impersonation attack

[표 2] 표기법
[Table 2] Notations

표기	설명
p	소수, $512 \le p \le 1024$
q	(p-1)의 소인수, 160비트
h	$1 < h < (p-1)$ 사이의 정수
g	원시근, $h^{(p-1)/q} \bmod p > 1$
X_a	AP의 임시 개인키, $1 < X_a < q$
Y_a	AP의 임시 공개키 $Y_a = g^{PSK \cdot X_a \bmod q} \bmod p$
X_s	Station의 임시 개인키, $1 < X_s < q$
Y_s	Station의 임시 공개키 $Y_s = g^{PSK \cdot X_s \bmod q} \bmod p$

위의 공격들을 방어할 수 있는 WPA-PSK 프로토콜 설계 기준의 핵심을 정리하면 다음과 같다.

① 사전 공격을 방어하기 위해 공격자가 전송 메시지를 도청할 수 있어도 PSK를 검증할 수 있는 정보는 전송되지 않아야 한다.
② 암호화된 메시지를 복호할 수 없도록 내부자라도 PSK로부터 사용자와 AP간에 합의된 세션키를 구할 수 없어야 한다.
③ Mano 등의 프로토콜 취약점인 외부자에 의한 중간자 공격과 위장 공격을 방어하기 위해서 합의 마스터키 생성 방식이 개선되어야 한다.
④ 세션키 합의를 위해 추가되는 계산량과 통신량이 최소화 되도록 한다.

위의 설계 기준을 만족할 수 있는 방법은 사용자나 AP가 자신의 공개키를 계산할 때와 합의 마스터키를 생성할 때 PSK 정보를 포함하도록 해야 한다. 그러면서 Diffie-Hellman 방식을 이용하여 세션키를 합의해야 한다. 제안한 프로토콜을 도식화한 것이 그림 5이다.

그림 5처럼 Diffie-Hellman 키 합의 기법을 응용하여 키 합의를 수행한다. 즉, 두 통신자의 공개키를 계산할 때 자신의 개인키와 PSK를 곱한 후 멱승(exponentiation)을 수행한다. 그러나 개인키와 PSK를 곱한 값이 커지게 되면 멱승 연산량이 늘어나므로 안전도를 해치지 않는 범위 내에서 지수(exponent)를 위수(order) q로 모듈러 연산을 먼저 하여 계산량을 감소시킨다. 소수 q는 안전도와 계산량을 고려하여 160비트로 사용한다. 또한, 합의 마스터키를 생성할 때 추가적으로 PSK를 포함시킴으로써 Rogue AP 위장 공격을 방어할 수 있도록 설계 하였다. 그리고 DPMK는 256비트 이어야 하기 때문에 키 합의를 통해 얻어진 DK(Dynamic Key)를 해쉬하여 DPMK로 사용한다. 제안한 프로토콜을 단계별로 설명하면 다음과 같다.

■ 1단계 :(AP-->Station) ANonce, p, q, g, Y_a

① AP는 키 합의에 사용될 개인키 X_a와 난수 ANonce를 생성한다.
② 다음 수식과 같이 공개키 Y_a를 생성한다.

$$E_a = (PSK \cdot X_a) \bmod q$$

$$Y_a = g^{E_a} \bmod p$$

③ AP는 공개 파라미터 ANonce, p, q, g와 공개키 Y_a를 전송한다.

■ 2단계 : (Station-->AP) SNonce, Y_s, MIC

① Station은 키 합의에 사용될 개인키 X_s와 난수 SNonce를 선택한다.
② 다음 수식과 같이 공개키 Y_s를 생성한다.

$$E_s = (PSK \cdot X_s) \bmod q$$

$$Y_s = g^{E_s} \bmod p$$

③ 합의키 DK를 계산한다.

$$DK = Y_a^{(PSK \cdot X_s) \bmod q} \bmod p$$
$$= g^{(PSK^2 \cdot X_a \cdot X_s) \bmod q} \bmod p$$

④ DK를 해쉬하여 256비트 DPMK를 생성한다.
DPMK = SHA256(DK)
⑤ DPMK, AP MAC 주소, Station MAC 주소, SNonce, ANonce로 PTK를 생성한다.

PTK = PRF-512(DPMK, “Pairwise key expansion", Min(AA, SA) ‖ Max(AA, SA) ‖ Min(SNonce, ANonce) ‖ Max(SNonce, ANonce) (5)

⑥ PTK를 해쉬키로 하여 메시지에 대한 MIC를 생성하고, 공개 파라미터 SNonce, 공개키 Y_s, MIC을 전송한다.

MIC = HMAC(PTK, 전송되는 파라미터들) (6)

■ 3단계 : (AP-->Station) ANonce, MIC

① AP는 합의키 DK를 계산한다.

$$DK = Y_s^{(PSK \cdot X_a) \bmod q} \bmod p$$
$$= g^{(PSK^2 \cdot X_s \cdot X_a) \bmod q} \bmod p$$

② DK를 해쉬하여 256비트 DPMK를 생성한다.
DPMK = SHA256(DK)
③ DPMK, AP MAC 주소, Station MAC 주소, SNonce, ANonce로 PTK를 생성한다.

PTK = PRF-512(DPMK, “Pairwise key expansion", Min(AA, SA) ‖ Max(AA, SA) ‖ Min(SNonce, ANonce) ‖ Max(SNonce, ANonce) (7)

④ 생성된 PTK로 MIC을 검증한다. 검증 시 올바르다면 다음 과정을 수행하지만 틀리다면 처음부터 다시 시작한다.
⑤ AP는 MIC을 생성한 뒤에 Station으로 전송한다.

MIC = HMAC(PTK, 전송되는 파라미터들) (8)

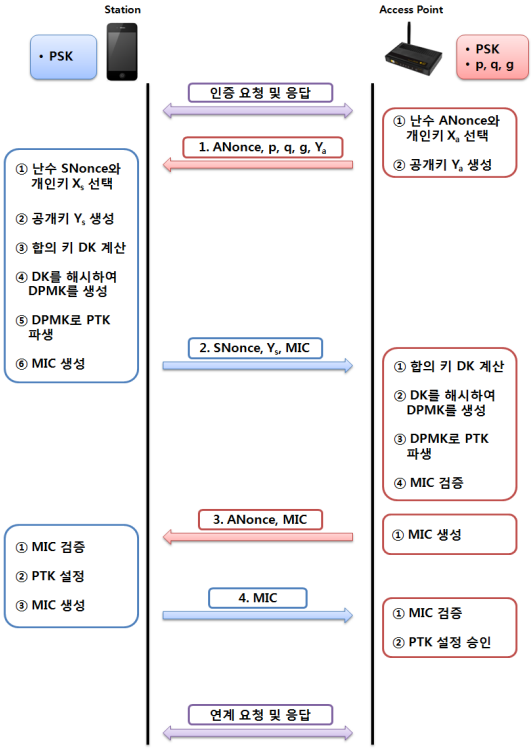
■ 4단계 : (Station-->AP) MIC

① Station은 먼저 MIC을 검증하고 올바르다면 최종적으로 PTK 키를 설정한다.

② Station은 MIC을 생성한 뒤 AP로 전송한다.

③ AP는 먼저 MIC을 검증하고 올바르다면 키 설정을 승인하고 설정된 키인 PTK로 사용하여 암호화 통신을 수행한다.

④ 만약에 같지 않다면 제대로 키 합의가 이루어지지 않은 것이기 때문에 처음부터 다시 시작한다.



[그림 5] 제안하는 WPA-PSK 프로토콜
[Fig. 5] Proposed WPA-PSK protocol

제안 프로토콜에서는 Mano 등의 프로토콜과 다르게 Diffie-Hellman 키 합의로 암호화키를 생성할 때 PSK 정보를 포함시킨다. 즉, Mano 등의 프로토콜에서는 공개키를 생성할 때 두 통신자만의 비밀 정보가 포함되지 않기 때문에 중간자 공격이 가능했던 점을 고려하여 공통의 마스터키 DK를 생성할 때 PSK를 사용함으로써 PSK를 알 수 없는 외부 공격자에 의한 중간자 공격이 불가능하게 된다.

그리고 Rogue AP 위장 공격을 방어하기 위해서는 DK 생성 시 PSK를 멱승을 위한 지수에 포함시킨다. 따라서 DK는 $g^{(PSK^2 \cdot X_s \cdot X_a) \bmod q} \bmod p$가 되어 PSK를 알지 못하는 Rogue AP가 DK를 생성할 수 없게 설계하였다.

또한, Mano 등의 프로토콜에서는 멱승 시 사용된 지수 X_a나 X_s에 대한 크기가 정해져 있지 않으나 소수 p의 길이(약 512비트)가 됨으로 많은 계산 부하가 발생하게 된다. 그러나 제안 프로토콜에서는 사용되는 지수가 $(p-1)$의 약수인 q의 길이(약 160비트)가 되게 함으로써 계산량을 크게 감소시킬 수 있었다.

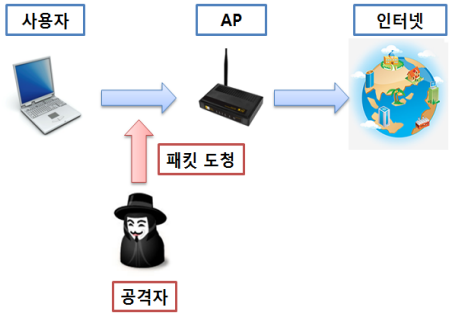
그리고 AP와 사용자는 합의 마스터키인 DPMK를 사용하여 PTK를 생성하고 PTK를 이용하여 MIC를 생성하기 때문에 사전 공격 자체가 불가능하다. 즉, 사전에 있는 단어만 가지고는 DPMK를 예측할 수 없기 때문에 원래 WPA-PSK에 사용했던 사전 공격은 적용이 불가능하다.

5. 사전 공격 실험 및 비교 분석

5.1 일반 WPA-PSK에 대한 사전 공격 실험

본 논문에서는 실험을 통하여 WPA-PSK에 대한 사전 공격이 실제로 가능한지 Wi-Fi 환경에서 실험해 보았다. 공격자는 공격 대상이 되는 특정 AP에 대한 패스워드를 공격하기 위해 그림 6과 같이 사용자와 AP간의 4단계 핸드쉐이크 과정의 내용을 모두 도청 후 저장하였다.

WPA-PSK의 4단계 핸드쉐이크 과정에 대한 패킷을 캡처하기 위해서 Kismet 툴과 Air 패키지를 사용한다. Kismet 툴은 주변 AP에 대한 정보 수집 및 패킷 수집을 할 수 있으며 Air 패키지는 사전 공격, 패킷 수집, 가상 AP 생성 등의 일을 할 수 있다.



[그림 6] WPA-PSK 사전 공격
[Fig. 6] Dictionary attack on WPA-PSK

공격 과정을 상술하면 다음과 같다.

① 공격자는 Air 패키지를 이용하여 Airmon-ng 명령으로 무선 어댑터를 Monitor mode로 변경한다. 이

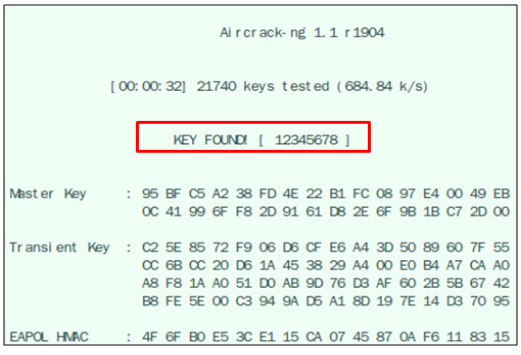
경우 Monitor mode로 변경하면 패킷 수집이 가능한 Promiscuous 모드 상태가 된다.

② Kismet 툴을 이용하여 공격 대상 AP의 정보를 알아낸다. 즉, 사전 공격에 필요한 AP의 MAC 주소, 채널 번호, SSID, 암호화 방식을 알아낼 수 있다.

③ Airodump-ng 명령으로 공격 대상 AP를 스니핑한다. 사용자가 공격 대상 AP로 접속하면 사용자가 목록에 추가되고 통신 내용을 스니핑할 수 있다.

④ 공격자는 스니핑을 수행하여 얻은 패킷에 대해 Aircrack-ng 명령으로 패스워드에 대한 사전 공격을 수행한다.

공격자는 사용자가 사용한 패스워드가 짧거나 쉽게 유추할 수 있는 패스워드라면 그림 7과 같이 패스워드를 짧은 시간 내에 찾을 수 있었다. 실험 결과, 사용자의 패스워드를 찾는 데에는 패스워드의 길이 및 추측성에 따라 차이가 있지만 수초 정도의 시간이 소요되었다. 따라서 패스워드는 사전 공격이 어려운 큰 길이를 사용하거나 패스워드 설정 기준을 준수하여 사용하여야 한다. 그러나 보안 사항을 준수한 패스워드를 사용했다고 해도 사용자가 패스워드를 기억해야하는 한계로 인해 공격시간은 늘어나겠지만 근본적인 방어책이 될 수 없음을 확인하였다.



[그림 7] 사전 공격 실험 화면
[Fig. 7] Experimental dictionary attack

5.2 제안 프로토콜 비교 분석

현재 사용 중인 AP로는 새로운 프로토콜 기능을 제공할 수 없기 때문에 논문에서 제안한 WPA-PSK 프로토콜의 동작 실험은 불가능하다. 본 절에서는 일반 WPA-PSK 프로토콜, Mano 등의 프로토콜, 제안된 프로토콜의 안전성과 효율성을 비교해 보았다. 이를 정리한 것이 표 3이다. 사전공격의 경우 공격이 성공했다는 의미는 패스워드를 알아냈다는 의미이며, 중간자 공격이 성공했다는 것은 중간 공격자가 위장을 통해 두 통신자의 통신 내용을 도청 혹은 세션 하이재킹 등을 할 수 있다는 것이다. 그리고 내부자들끼리는 패스워드를 공유하고 있으므로 PSK를 이미 알고 있다고 가정한다.

일반적인 WPA-PSK 프로토콜은 외부 공격자에 의해 사전 공격이 가능하며, 사전 공격이 성공하면 통신의 도청이나 세션 하이재킹 공격으로 확장할 수도 있다. 또한 내부 공격자의 경우에는 이미 PSK를 알고 있기 때문에 모든 통신 내용을 도청할 수 있다.

Mano 등의 프로토콜은 PTK를 생성하는데 사용되는 DPMK를 Diffie-Hellman 키 합의로 생성을 하기 때문에 외부 공격자에 의한 사전 공격이 불가능하다. 또한, 통신 메시지가 DPMK로 파생된 PTK로 암호화되어 전송되므로 도청도 불가능하다. 하지만 Diffie-Hellman 키 합의를 사용함에 따라 내부자 혹은 외부자에 의한 중간자 공격이 가능하며, DPMK와 PSK의 연관성이 없기 때문에 Rogue AP 위장 공격도 가능하다.

[표 3] 프로토콜 비교
[Table 3] Comparison of the protocol

구 분			일반 WPA-PSK	Mano 등 WPA-PSK	제안한 WPA-PSK
안전성	사전 공격	내부	Known	Known	Known
		외부	O	X	X
	도청	내부	O	X	X
		외부	X	X	X
	중간자 공격	내부	N/A	O	O
		외부	N/A	O	X
	Rogue AP 위장 공격		X	O	X
효율성	추가 계산량		-	멱승 2회 (지수 512비트)	멱승 2회 (지수 160비트)
	추가 통신량		-	p, q, Y_a, Y_s	p, q, g Y_a, Y_s

본 논문에서 제안한 프로토콜은 Diffie-Hellman 키 합의를 사용하되 PSK를 접목하여 사용함으로써 PSK를 모르는 외부 공격자에 의한 중간자 공격을 방어한다. 내부 공격자의 경우 PSK를 이미 알고 있기 때문에 중간자 공격에 대한 방어는 불가능하다. 그러나 내부에서는 전파가 동시에 송·수신되므로 중간 메시지 중계가 필요한 내부자의 중간자 공격은 현실적으로 적용이 어려워 보인다. 그리고 DK 생성 시 PSK를 사용하게 되는 점 때문에 공격자에 의한 Rogue AP 위장 공격도 불가능하다.

일반 WPA-PSK에 비해 제안 프로토콜을 사용함으로써 추가되는 연산량은 약 2회의 멱승 연산이 필요하다.

그러나 Mano 등의 방식에서는 사용하는 지수가 512비트 정도의 큰 정수이므로 계산량이 많아지는 반면, 제안 방식에서는 위수인 소수 q의 길이만큼의 지수를 사용하므로 연산량 증가에 대한 부담을 감소시켰다. 그러나 전송되는 통신량 측면에서는 일반적인 WPA-PSK에 비해 전송 파라미터p, q, g, Y_a, Y_s가 추가되며, Mano 등의 방식에 비해서는 q가 추가되어 전송 정보량은 다소 늘어난다. 제안 방법은 일반 WPA-PSK에 비해 계산량과 통신량이 늘어나지만 내부자의 중간자 공격을 제외한 모든 공격을 방어할 수 있어 안전성이 크게 향상되으며 Mano 등의 방법과 비교해 보면 계산량은 줄어들면서 안전성도 더욱 강화되었다.

6. 결 론

본 논문에서는 소규모 회사나 가정, 카페와 같은 장소에서 제공되는 무선 네트워크인 Wi-Fi상에서 WPA-PSK 프로토콜을 사용할 경우의 보안 취약점을 분석하였다. 현재 사용 중인 WPA-PSK 프로토콜은 패스워드에 대한 사전 공격이 충분히 가능함을 실제 스마트폰 통신 환경에서 실험을 통해 검증하였다. 사전공격에 대한 대응 프로토콜로 제안되었던 Mano 등의 프로토콜은 Diffie-Hellman 키 합의 방식을 그대로 채택하고 있어 외부 공격자에 의한 중간자 공격이 용이하였으며 Rogue AP 위장 공격의 가능성이 존재함을 알 수 있었다.

본 논문에서는 사전 공격, 중간자 공격, Rogue AP 위장 공격을 방어할 수 있는 새로운 WPA-PSK 프로토콜을 제안하였다. 또한 보안성을 강화하기 위해 프로토콜에서 추가되어야 하는 계산량이나 통신량이 최소화 되도록 설계하였다. 제안 프로토콜은 내부자에 의한 중간자 공격은 가능하지만 현실적인 공격 가능성이 매우 적는 점을 고려하면 안전하고 효율적인 무선 보안 프로토콜로 활용할 수 있다.

References

[1] Wi-Fi Alliance, "The State of Wi-Fi® Security Wi-Fi CERTIFIED™ WPA2™ Delivers Advanced Security to Homes, Enterprises and Mobile Devices", pp. 1-15, Wi-Fi Alliance, 2009.

[2] H. Berghel, "Wireless Infidelity I:War Driving", Comm. of the ACM, vol. 47, no. 9, pp. 21-26, 2004.

[3] IEEE Computer Society, "IEEE Std 802.11b-1999", pp. 1-90, IEEE, 1999.

[4] S. R. Fluhrer, I. Mantin, and A. Shamir, “Weaknesses in the key scheduling algorithm of RC4” Proceeding of SAC ’01: Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography. London, UK: Springer-Verlag, pp. 1 – 24, 2001.

[5] A. Stubblefield, J. Ioannidis, and A. D. Rubin, “A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP)”, ACM Transactions on Information and System Security, vol. 7, no. 2, pp. 319-332, 2004.

[6] IEEE Computer Society, "IEEE Std 802.11i-2004", pp. 1-1233, IEEE, 2004.

[7] G. Lehembre, "Wi-Fi security - WEP, WPA and WPA2", pp. 1-14, hakin9, 2005.

[8] D. Welch, S. Lathrop, "Wireless Security Threat Taxonomy", Information Assurance Workshop 2003. IEEE Systems. Man and Cybernetics Society, pp. 76-83, 2003.

[9] W. Diffie and M. E. Hellman, “New directions in cryptography”, IEEE Transactions on Information Theory, vol. IT-22, no. 6, pp. 644 – 654, 1976.

[10] C. D. Mano and A. Striegel, “Resolving WPA Limitations in SOHO and Open Public Wireless Networks”, Wireless Communications and Networking Conference, WCNC 2006, pp. 617-622, 2006.

[11] J. F. Raymond, A. Stiglic, "Security Issues in the Diffie-Hellman Key Agreement Protocol", IEEE Trans. on Information Theory, pp. 1-27, 2000.

[12] I. Martinovic, F. A. Zdarsky, A. Bachorek, C. Jung, J. B. Schmitt, “Phishing in the Wireless : Implementation and Analysis”, IFIP International Federation for Information Processing, vol. 232, pp. 145-156, 2007.

[13] F. M. Halvorsen, O. Haugen, "Cryptanalysis of IEEE 802.11i TKIP", Norwegian University of Science and Technology, June, 2009. Available at http://hirte.aircrack-ng.org/tkip_master.pdf

[14] Y. S. Kang, K. H. Oh, B. H. Chung, K. I. Chung, “Wireless LAN Security Standard IEEE 802.11i", TTA Journal No 99, pp.124-129, June 2005.

[15] Korea Internet and Security Agency, "Wireless LAN Security Guidebook", 2010.

박 근 덕(Geun-Duk Park) **[정회원]**

- 2005년 8월 : 서울대학교 전기컴퓨터공학부 (공학박사)
- 2006년 3월 ~ 현재 : 호서대학교 컴퓨터공학부 조교수

<관심분야>
임베디드소프트웨어공학, 서비스 지향 컴퓨팅, XML 응용

박 정 수(Jeong-Soo Park) **[준회원]**

- 2011년 2월 : 호서대학교 컴퓨터공학과 (공학사)
- 2011년 3월 ~ 현재 : 호서대학교 대학원 정보보호학과 (석사과정)

<관심분야>
스마트폰 보안, 부채널 공격, 무선 네트워크 보안

하 재 철(Jae-Cheol Ha) **[종신회원]**

- 1989년 2월 : 경북대학교 전자공학과 (공학사)
- 1993년 8월 : 경북대학교 전자공학과 (공학석사)
- 1998년 2월 : 경북대학교 전자공학과 (공학박사)
- 1998년 3월 ~ 2007년 2월 : 나사렛대학교 정보통신학과 부교수
- 2007년 3월 ~ 현재 : 호서대학교 정보보호학과 부교수

<관심분야>
정보보호, 네트워크 보안, 부채널 공격