무선 랜 카드 Monitor Mode와 WPA2 복호화를 통한 무선 네트워크 감청에 관한 연구

전인표 조동민 명의정 김현우 이재우 정다안*

*KITRI Best of the Best

Study on Monitoring Wireless Network by using WiFi USB Adapter Monitor Mode and WPA2 Decryption

In-Pyo Jeon Dong-Min Jo Eui-Jung Myeong

Hyun-Woo Kim Jae-Woo Lee Da-an Jeong*

*KITRI Best of the Best

요 약

요약

I. 서론

스마트폰 및 태블릿 PC의 영향을 받아 공공시설 및 가정을 중심으로 다양한 무선랜 환경이 만들어지기 시작하였다. 무선랜은 유선랜에 비해 저렴하고 편리하다는 이유로 현재 널리 보급되어 사용되고 있다. 특히 지하철과 같은 공공시설 및 카페에서 제공하는 'WiFi'의 이용이 크게 증가하고 있으며, 이에 따라 보안상의 문제들이 발상해고 있다.

대중적인 사용을 목적으로 개방된 환경에서 제공되는 무선랜의 특징상 다양한 형태의 보안 위협이 발생할 수 있다. 이로 인해 무선 AP에서는 보안 강도에 따라 WEP, WPA, WPA2 등의 인증/암호화 기술을 제공하고 있으며, 안전한 이용을 위해 WPA2 설정을 권고하고 있다. 하지만 이러한 보안 권고에도 불구하고 암호화된 통신을 사용하지 않거나 공격자가 기존의 'WiFi'에 공유된 암호를 알아내어 복호화 할 경우 개인정보 유출 및 해킹으로 인한 2차 피해가 우려 된다. 추가적으로 현재 발견되고 있는 공중 무선랜의 취약점은 '무선 AP 공격 및 해킹' 또는 '불법적인 무선 AP 설치' 로 인한 사례들이 대부분이다.

본 논문에서는 현재 보안상 안정을 위해 사용권장되고 있는 WPA2의 취약점과 전파를 이용한다는 무선랜 특성상의 취약점을 이용한 네트워크 감청에 대한 연구를 다루고 있다.

II. 관련 연구

2.1 무선 랜 카드 Mode

2.1.1 Managed Mode

기본 설정 값으로, Station에서 AP로 통신할 때 사용된다.

2.1.2 Ad-Hoc Mode

Station 간의 직접적인 통신에 이용된다.

2.1.3 Master Mode

Station이 마치 AP처럼 인식되도록 한다. 예를 들어 스마트폰 테더링 등이 있다.

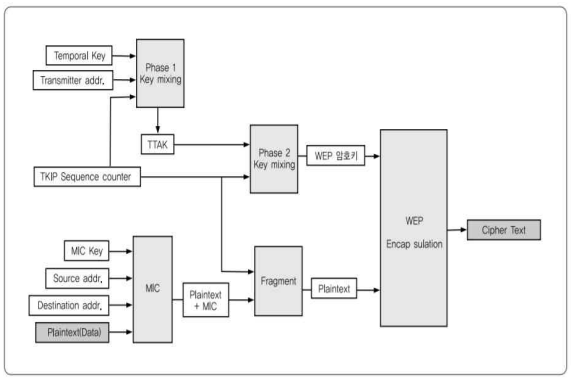
2.1.4 Monitor Mode

Data를 직접적으로 주고받지는 못하지만 Wireless Packet을 수집할 수 있따.

2.2 WPA2(WiFi Protected Access2) 보안 메커니즘

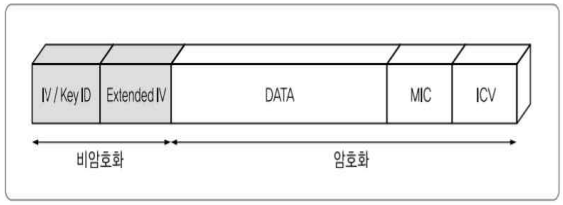
WPA2 암호화의 경우 이전의 WEP, WPA 암호화에 비해 무선 장비와 단말기 간의 가상 인증 기능을 제공하는 EAP(Extensible Authetication Protocol)오 같은 검증된 보안기술들이 포함되어 보다 강화된 인증/암호화 기능을 제공한다. WPA2에서는 이번 버전과의 호환성을 위해 TKIP(Temporal Key Integrity)와 CCMP 두 가지 방식의 암호화를 사용한다.

2.2.1 TKIP 암호화 방식



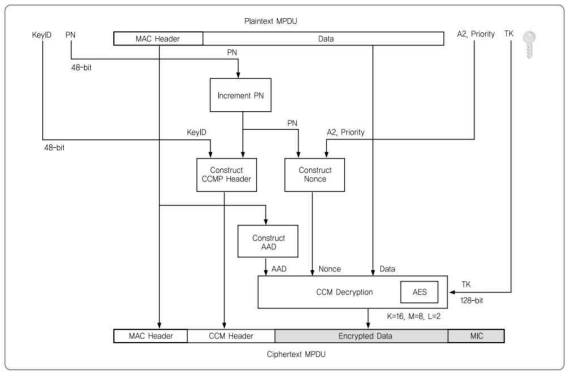
[그림 1] TKIP 암호화 절차

TKIP 암호화 방식은 WEP의 취약점을 해결하기 위해 제정된 표준으로서, EAP에 의한 사용자 인증결과로부터 무선 단말기와 무선 AP사이의 무선 채널 보호용 공유 비밀 키를 동적으로 생성하여 무선 구간 패킷을 암호화 한다. 무선 AP는 무선 단말기가 자신과 동일한 비밀 키를 가지고 있는지 802.1x에 규정된 EAPoL-Key 프레임을 활용하여 4-Way Handshake 절차를 통해 확인하여 인증을 수행한다. 인증이 성공된 경우, PSK로부터 임시 암호 키(PMK)를 생성하여 해당 값을 무선 AP도 가지고 있는지 확인되면 무선랜이 활성화 된다. TKIP는 암호화뿐만 아니라, MIC를 적용하여 전송하려는 데이터의 무결성도 강화하고 있다.



[그림 2] TKIP로 암호화된 패킷 구조

2.2.2 CCMP 암호화 방식



[그림 3] CCMP 암호화 절차

CCMP 암호화 방식은 128비트의 블록 키를 사용하는 CCM(Counter Mode Encryption with CBC-MAC)모드의 AES 블록 암호 방식을 사용하여 데이터의 비밀성과 무결성을 보장한다. CCMP는 TKIP와 키관리 등에 있어서 유사하지만 128비트의 대칭키와 48비트의 초키벡터를 이용하여 차별화된다. 이미 전문가들의 많은 검토를 통해 안정성이 입증된 AES를 기반으로 하기 때문에 현재의 무선랜 표준으로서는 가장 보안에 안정한 방식이다.

2.2.3 WPA2 보안 취약점

문제는 이러한 인증 과정 자체가 별도의 암호화가 되어 있지 않다는 것이다. 따라서 무선 패킷 수집을 통해 4-Way Handshake 과정의 초기 인증패킷만 수집된다면 복호화가 가능하다.

2. 3 IEEE 802.11 프로토콜

(1) 개요

무선 LAN에서 데이터를 송수신하기 위해서는 IEEE에서 정의한 802.11 프로토콜을 따라야 한다. IEEE 802.11 프로토콜은 무선랜 환경에서 주로 데이터링크 계층과 물리 계층 위에서의

전송 방식에 대해 정의되어 있으며, 계속해서 메커니즘이 효율성을 갖도록 보완되고 있다.

(2) 802.11 MAC 프레임

IEEE 802.11 프로토콜에서 데이터링크 계층이 갖는 데이터를 MAC 프레임이라고 하며, 일반적인 구조는 [그림]과 같다.

무선 LAN은 통신 과정에서 상황에 따라 여러 프레임 유형을 사용하는데 그 유형은 각각 관리 프레임, 제어 프레임, 그리고 데이터 프레임 3가지로 구분된다. 각 유형은 기본 프레임 구조의 Frame Control 필드의 2바이트 값 중 맨 앞 subtype 4비트 값 이후 2비트 Type 값으로 구분하며 00일 경우 관리 프레임, 01일 경우 제어 프레임, 10일 경우 데이터 프레임을 말한다. 각 유형에 대한 설명은 다음과 같다.

802.11 관리 프레임

관리 프레임은 무선 단말(이하 스테이션)과 Access Point(이하 AP)사이의 초기 통신을 확립하기 위한 관리용 프레임을 말한다. AP와의 연결과 관련된 결합 요청, 결합 응답 프레임, 프로브 요청, 프로브 응답 프레임, 비콘 프레임, 그리고 인증 프레임 등이 이에 해당한다.

802.11 제어 프레임

제어 프레임은 스테이션과 AP 사이의 연결을 유지하는 역할을 한다. AP가 데이터를 수신했을 때 수신한 데이터에 대한 Ack를 보내며 지속적으로 스테이션과 AP사이의 데이터의 전송 상황을 얻어 데이터의 송수신을 조절한다. 대표적으로 Ack 프레임이 여기에 해당한다.

802.11 데이터 프레임

데이터 프레임은 스테이션과 AP사이의 실제 데이터를 주고받기 위한 프레임 규격이다. QoS data 프레임이나 data 프레임같이 데이터를 담은 프레임들이 여기에 속한다..

(3) 802.11b/g/n/ac의 대역폭과 주파수

물리 계층에서 단말간 데이터 송수신을 바라보았을 때, 무선 LAN 환경에서 두 단말 간에 서로 통신을 하기 위해서는 주파수 및 대역폭 환경을 서로에게 맞게 동기화 해주어야 한다. IEEE 802.11 표준은 802.11b ~ 802.11ac 순으로 보완되어왔는데 물리 계층에 있어서 그 주파수와 대역폭이 점진적으로 개선되어 왔다. 현재 가장 최신의 표준은 802.11ac이며 주파수 대역은 2.4GHZ 대역과 5GHZ를 혼용하고 있고 채널 당 대역폭도 20MHz ~ 160MHz으로 여러 대역을 모두 허용함으로써 이용량이 많아져가는 무선 랜 환경에 대비하고 있다. 각 표준에 대한 전송속도와 주파수 정보는 [표 1]과 같다.

표준	주파수	채널 당 대역폭	최고 전송 속도
802.11b	2.412GHz	20MHz	11Mbps
802.11g	2.412GHz	20MHz	54Mbps
802.11n	2.412GHz, 5.17GHz	20MHz, 40MHz	약 600Mbps
802.11ac	2.412GHz, 5.17GHz	20MHz, 40MHz, 80MHz 160MHz	약 1.3Gbps

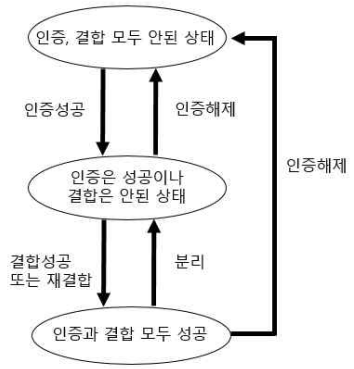
[표 1] - 각 표준별 주파수 및 대역폭 정보

(4) 802.11 비콘 프레임

IEEE 802.11 관리 프레임에 속하는 프레임으로써, 주로 공유기의 기능을 하는 AP가 STA에게 자신의 존재를 알리기 위해서 주기적으로 발생하는 프레임을 말한다. 프로토콜 상에서의 데이터 값을 살펴보면, Frame Control 필드에서의 맨 앞 subtype 4비트 값이 1000 에 해당하며, 그 뒤 2비트 Type 값은 비콘 프레임이 관리 프레임에 속하므로 00 값에 해당한다. 그 뒤 2비트 값은 일반적으로 00이기 때문에 일반적으로 비콘 프레임에서 Frame Control 필드의 맨 앞 1바이트 값은 0x80에 해당한다. AP는 자신이 사용할 주파수 대역을 정한 후 해당 주파수 대역에서 비콘 프레임을 주기적으로 송신한다. 무선 단말인 STA는 이 때 여러 주파수 대역에서 여러 AP 가 존재할 수 있으므로 모든 채널을 호핑해가며 프레임을 감지한다. 비콘 프레임이 감지되었으면 AP의 정보를 보여주며 그 신호의 세기에 따라 사용자에게 원활한 환경의 AP 순으로 보여준다. 따라서 특정 장소에서 AP의 존재를 확인하기 위해서는 비콘 프레임을 감지한다.

(5) 802.11 상태 구분

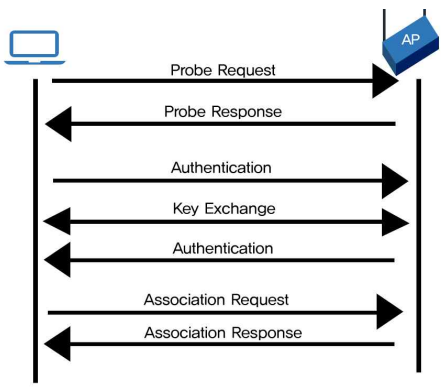
802.11 무선 단말 간에는 인증이나 결합 여부에 따라 3가지 상태가 존재하며 각 상태별로 전달되는 프레임의 유형이 다르다. 상태 간의 다이어그램을 그리면 그림과 같다.



인증과 결합이 모두 되지 않은 상태에서 인증을 요청할 경우 인증(Authentication) 프레임을 보내는데, WPA2와 같은 보안 프로토콜을 사용할 때에는 키교환 과정이 이루어진다. 반면 보안 프로토콜을 사용하지않은 Open Mode와 같은 상태라면 인증 과정은 그대로 존재하나, 키교환은 이루어지지 않는다. 인증이 성공하였으면 결합 요청(Association Request) 프레임을 보내 결합에 성공한다. 인증과 결합이 모두 성공한 상태에서 데이터를 교환하고 있을 때, 분리(Disassociate) 프레임을 주고받게 되면 연결이 두 번째 상태로 돌아가게 되며, 특별한 이유가 아닌 이상 재결합한다. 반면 같은 상태에서 두 단말이 연결을 끊고자 하는 경우 인증 해제(Deauthentication) 프레임을 받게되면 첫 번째 상태로 돌아가게 되며 이는 연결이 끊어졌음을 의미한다.

(6) 결합 과정

일반적으로 사용자가 무선 단말을 가지고 AP에 연결하려고 할 경우 사용자 인터페이스에서 발견된 AP를 선택한 후 PSK만 적어주고 연결 요청을 한다. 이 과정에서 무선 단말(STA)과 AP는 특정 프레임들을 주고 받으며 위에서 설명한 인증과 결합을 하게 된다. [그림] 과 같다.



사용자의 단말(STA)에서 발견된 AP가 여전히 존재하는지 확인하기 위해 처음에는 프로브 요청(Probe Request) 프레임에 연결하고자 하는 AP의 SSID를 담아 브로드캐스트로 보낸다. AP는 프로브 요청 프레임에 담긴 SSID가 자신의 SSID와 일치하면 프로브 응답(Probe Response) 프레임을 보낸다. 프로브 응답 프레임을 무사히 받은 STA는 AP에게 인증 프레임을 보내게 된다. 인증 프레임을 받은 AP는 자신이 사용하고 있는 보안 프로토콜에 따라 키교환 과정을 가지게 되며, WPA2 프로토콜의 경우 EAPOL 프로토콜을 통해 키교환을 한다. 키교환 과정에서 AP가 STA을 인증된 사용자라고 판단하였을 경우 인증 프레임을 보내 인증 상태 진입에 성공하게 되고, 마지막으로 결합 요청(Association Request) 프레임과 결합 응답(Association Response)프레임을 주고받아 결합하면 최종적으로 연결에 성공하게 된다.

3. WPA2 복호화 및 감청

3.1 환경 구성

(가) 시나리오

스테이션 A가 존재하고, 무선 AP가 있다. 스테이션 A는 이 무선 AP에 접속하여 인터넷을 이용하고 있다. 해당 무선 AP는 WPA2 프로토콜을 사용하며 우리는 PSK를 안다고 가정하고, A의 패킷을 감청하기로 한다.

(나) 운영체제

일반적인 사용자도 쉽게 이용할 수 있는 Ubuntu 16.04를 사용하였다.

(다) AP 설정

PJHS라는 SSID를 가지며 각 채널이 20MHz의 대역폭을 가지는 2.412GHz의 주파수 대역에서 9번째 채널을 사용하고 있도록 설정하였다. 개인용 WPA2 프로토콜을 사용하고 있으며 AES 암호화 방식을 사용하도록 설정하였다.

(라) 무선 랜카드

무선 패킷을 감청하기 위해서는 랜카드를 관리 모드(managed mode)에서 모니터 모드(monitor mode)로 전환해주어야 하는데 기존의 컴퓨터가 가지고 있는 무선 랜카드를 모니터 모드로 전환할 경우, 인터넷을 이용하기 어렵다. 따라서 기존 랜카드로는 인터넷을 이용하면서 동시에 무선 패킷을 감청하기 위해 모니터

모드(monitor mode)용 무선 랜카드를 따로 사용하였으며 TP-Link의 TL-WN727N 모델을 이용하였다. 본 문서에서 본 랜카드의 인터페이스 이름은 'wlan1'으로 한다.

(마) 모니터 모드

무선 랜카드가 무선 패킷을 감청하기 위해서는 우선 모니터 모드여야 한다. 무선 랜카드의 기본 설정은 대부분 관리 모드이므로 이를 모니터 모드로 전환해주려면 다음과 같은 명령어를 사용한다.

```
sudo ifconfig wlan1 down;
sudo iwconfig wlan1 mode monitor;
sudo ifconfig wlan1 up;
```

모니터 모드로 전환이 완료 되었으면 iwconfig 명령을 통해 모니터 모드로 전환된 것을 확인할 수 있다.

3.2 AP의 채널 정보 탐색

AP가 이용하는 채널 정보를 확인하여 무선 랜카드가 해당 채널의 패킷만 감지하도록 하여 최대한 AP의 패킷만 감청할 수 있어야 한다. 이를 위해서는 특정 채널에서 우리가 찾는 무선 AP가 존재하는 지를 확인하여야 한다. 즉, PJHS라는 SSID를 가진 AP를 발견해야 한다. 이를 위해서는 무선 랜카드를 해당 AP가 이용하는 채널로 설정해야 한다. 랜카드가 감지하는 채널을 하나씩 바꾸어가며 모든 채널에 대해 tcpdump를 사용하거나 와이어샤크 프로그램을 이용하여 캡쳐한 패킷을 보고 PJHS라는 SSID를 가지는 비콘 프레임을 확인하면 된다. 이 과정을 보다 간단히 하기 위해 airodump-ng를 이용한다. airodump-ng는 무선 랜카드의 감지 채널을 무작위로 호핑해가며 감지한 비콘 프레임에 들어있는 AP의 정보들을 나열해준다. 따라서 모든 채널의 AP의 존재를 파악할 수 있다. airodump-ng를 사용하기 위해서는 다음과 같은 명령어를 이용한다.

```
sudo airodump-ng wlan1
```

해당 명령어를 통해 PJHS라는 AP가 사용하는 채널 정보를 확인할 수 있다. 9번 째 채널을 이용하고 있으므로 다음명령어를 통해 무선 랜카드의 채널을 채널 9로 고정해준다.

```
sudo iwconfig wlan1 channel 9
```

3.3 인증 해제(Deauthentication) 프레임 전송

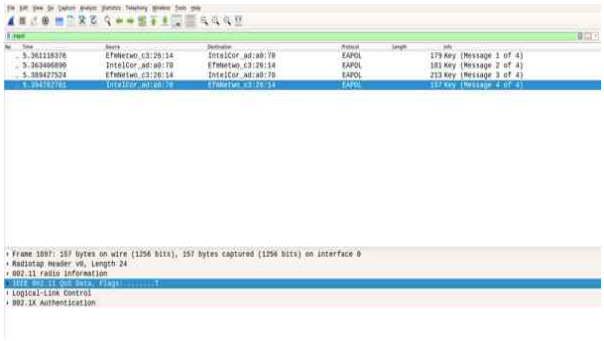
스테이션 A는 이미 무선 AP와 인증과 결합 모두 성공한 상태이다. 따라서 EAPOL 키 교환 과정을 감청할 수 없다. 그렇기 때문에 키 교환 과정을 다시 유도하기 위해서는 이 두 단말간의 인증과 결합이 모두 제거된 상태로 만들어야 하는 문제가 발생한다. 이는 AP에게 스테이션 A가 보낸 것처럼 사칭하는 인증 해제 프레임을 전송함으로써 해결할 수 있다. AP에게 사칭 인증 해제 프레임을 보내는데 성공하게 되면, 스테이션 A는 AP와의 연결이 한 순간 끊어지게 되며, 일반적인 경우 스테이션 A는 바로 다시 AP와 연결을 시도한다. 이 과정에서 키교환을 탈취할 수 있지만 한 순간이므로 스테이션 A의 사용자는 자신의 연결이 누군가에 의해 끊어졌다는 것을 알아차리기 어렵다. 즉, 인증 해제 프레임의 발신자 인증 과정의 허술함 때문에 사용자가 알아차리기 어렵게 사용자의 단말과 AP간의 키 교환을 유도해내 얻어 낼 수 있다.

인증 해제 프레임은 802.11 MAC 프레임에서 관리 프레임에 속하며, Frame Control 필드에서 맨 앞 subtype 4비트 값이 1100인 프레임을 말한다. 인증 해제 프레임은 분리(Disassociate) 프레임과 달리 802.11 프로토콜의 시퀀스 넘버(sequence number)에 종속적이지 않기 때문에 전후 프레임의 시퀀스 넘버(sequence number)를 신경 쓰지 않아도 된다.

인증 해제 프레임의 전송 방법은 C++ pcap 라이브러리를 이용하여 소스 코드를 구성하였다. airodump-ng를 통해 조사한 PJHS라는 AP의 BSSID가 감지되면 감지된 프레임으로부터 확인할 수 있는 A의 mac 주소를 송신자로 하고 AP의 BSSID를 수신자로하여 802.11 인증 해제 프레임을 구성하여 전송하도록 하였다.

3.4 EAPOL 키 교환 탈취

인증 해제 프레임이 성공적으로 AP에게 전송되어 작용하면 802.11 QoS Data 프레임 위에서의 EAPOL 프로토콜 기반의 키 교환을 감지할 수 있다. 4-way handshake이므로 4개의 패킷이 오고가는 것을 확인할 수 있으며 이를 와이어샤크 프로그램을 통해 보면 [그림]과 같다.



여기서 PSK를 통해 PMK를 구성하고 PMK, AP Nonce, STA Nonce, AP mac address, STA mac address를 인자로 PBKDF2-SHA1 함수를 통하여 64바이트 PTK를 얻어낸다. PTK는 KCK, KEK, TK, Tx Key, Rx Key로 구성되며 여기서 주로 복호화에 사용될 데이터는 유니캐스트 데이터를 복호화하는 16바이트 TK 값이다. 해당 값으로 복호화 하면 데이터 프레임의 데이터들을 평문으로 볼 수 있게 된다.

3.5 쿠키 스니핑

802.11 프로토콜은 2계층인 데이터 링크 계층까지의 전송 방식을 규정하였고, 실제로 3 계층에서부터의 데이터의 전송 방식에 쓰이는 프로토콜은 TCP/IP 프로토콜이므로 복호화 된 평문의 데이터 프레임들은 대부분 TCP/IP 프로토콜임을 확인할 수 있다. 따라서 이를 이용해 Python 프로그래밍 언어를 통해 복호화된 패킷에서 HTTP 패킷만 걸러낸 후 쿠키 값을 파싱하여 저장하는 프로그램을 작성하였다. 이 쿠키 값을 즉시 브라우저에 입력시켜 국내 대형 포털 사이트를 접속하면 로그인 세션이 탈취된 것을 확인 할 수 있었다.

Ⅳ. 결론

무선 AP의 경우 자체적으로 보안 설정이 가능하도록 되어 있지만 이용자들의 인식부족 및 편리성 추구로 인하여 보안 설정이 미약한 점이 존재한다. 무선 랜을 통한 개인정보 문제들이 발생하고 있는 상황이기 때문에 무선 랜 보안에 대한 인식제고가 필요해 보인다. 특히, 공공장소 뿐만 아니라 카페, 음식점 등에서 제공하는 무선 랜의 경우 보안설정이 상대적으로 낮을 뿐만 아니라 공격자의 접근이 용이하기 때문에 보안성을 강화하려는 노력이 절실히 필요하다.

본문에서 다루었던 무선랜 보안의 문제점들에 대한 해결책으로는 두 가지 정도를 제안한다.

HTTP(HyperText Transfer Protocol)가 아닌 HTTPS(HTTP over Secure sockets layer)를 사용하여 패킷을 암호화하여야 한다. 웹 개발단계에서부터 보안에 대하여 생각한다면 큰 도움이 될 것이다. 그러나 이는 웹 개발자들이 가져야 할 필수적인 요소는 아니기 때문에 현실적인 어려움이 존재하므로 앞으로의 관심이 필요하다.

둘째, 이용에 번거롭더라도 무선 AP 보안 설정을 WPA2-Enterprise 모드로 해야한다. 별도의 인증서버를 구축해야하는 수고가 필요하지만 접속 아이디, 비밀번호가 동일해도 패킷을 복호화 하는 것이 훨씬 어렵기 때문에 보안성이 상대적으로 매우 높다. 때문에 많은 사람들이 사용하는 공공 무선 네트워크에 인증 서비스를 활성화할 필요가 있다.

[참고문헌]

[1] Korea Communications Commission and Korea Internet & Security Agency, 알기 쉬운 공중 무선랜 보안 안내서, KISA 안내・해설 제2011-14호, 12. 2011.

[2] Korea Communications Commission and Korea Internet & Security Agency, 무선랜 보안 안내서, KISA 안내・해설 제2010-12호, 1. 2010.

[3] http://www.ktword.co.kr/abbr_view.php?nav=2&m_temp1=4898&id=1293

[4] http://www.kalitutorials.net/2014/06/hack-wpa-2-psk-capturing-handshake.html

[5] http://www.aircrack-ng.org/