무선랜 보안 가이드

2008. 11

행정안전부
MINISTRY OF
PUBLIC ADMINISTRATION
AND SECURITY

KISA 한국정보보호진흥원
Korea Information Security Agency

이 가이드는 무선랜을 안전하게 사용하는데 도움이 되고자 작성되었습니다.

이 가이드의 작성을 위하여 다음 분들께서 수고하셨습니다.

2008년 11월

책 임 자 :	한국정보보호진흥원	KISC	본 부 장	**이명수**
참여연구원 :		해킹대응팀	팀 장	**최중섭**
			선임연구원	**서진원**
			선임연구원	**김영백**
			주임연구원	**이동련**
			주임연구원	**한단송**
			주임연구원	**주필환**
			연 구 원	**박문범**
			연 구 원	**전은국**
외부전문가 :	서울여자대학교			**김형종**
	컴퓨터프로그램보호위원회			**신동명**

Contents

Contents

표 목차

그림 목차

제1장 개 요

Korea Information Security Agency

제1장 개 요

무선랜은 사용의 편리함으로 인해 점차 많은 분야에 걸쳐 활용되고 있다. 무선랜의 가장 큰 장점은 무엇보다도 이동성에 있다고 할 수 있다. 국내 유선 인터넷 서비스는 '06년을 기점으로 포화상태에 있지만, 무선 인터넷 사용자는 꾸준한 증가세를 보이고 있다.

하지만 무선랜은 많은 장점과 동시에 무선 서비스의 특성 상 존재하게 되는 다수의 보안 취약점을 가지고 있으며, 이런 문제점을 해결하기 위해 다양한 보안관련 기술이 개발 및 적용되고 있다. 하지만 그에 반해 무선랜 사용자의 보안인식은 여전히 부족한 상태로, 매년 개인정보유출 등의 보안사고가 반복적으로 발생하고 있는 상황이다.

앞으로 현실화될 유비쿼터스 환경에서는 무선랜이 중요한 부분을 차지하게 되며, 현재도 백화점, 대형 할인마트, 주유소 등 일상생활의 여러 분야에서 무선랜이 사용되고 있다. 그만큼 무선랜의 보안은 점차 중요한 이슈로 다뤄지게 될 것으로 예상되며, 무선랜 사용자들도 일정 수준의 보안 수칙에 대해 숙지하여 피해를 예방할 수 있도록 해야한다

본 가이드에서는 무선랜에 대한 현황과 더불어 무선랜에서 발생할 수 있는 주요 취약점을 먼저 언급하고, 그에 대한 보안 가이드를 무선랜 사용자 및 관리자에게 제시하는 것을 목적으로 하였다.

제2장 무선랜 구성요소

제1절 무선랜의 유형과 구성요소

Korea Information Security Agency

제2장 무선랜 구성요소

무선네트워크 표준에는 서비스 범위와 네트워크의 구성 등에 따라 다수의 무선 네트워크의 분류가 정의되어 있다. 본 장에서는 간략히 무선네트워크의 서비스 범위에 따른 분류에 대해 먼저 알아보고, 주요 구성요소에 대해 알아보도록 한다.

제1절 무선랜 유형과 구성요소

1. 무선 네트워크 유형과 무선랜 기술 표준

가. 무선 네트워크 유형

무선랜의 기술적 위치를 설명하기 위해 본 장에서는 무선 네트워크 구조의 유형들을 제시하고자 한다. 〈표 1〉은 데이터 전송의 범위에 따른 무선 네트워크의 3가지 구조이다.

[표 1] 무선 네트워크 구조별 특징 요약

무선 네트워크구조	내 용	사용예제
WPAN	단거리 Ad Hoc 방식 또는 Peer to Peer 방식	– 노트북간의 데이터 전송이나 핸드폰과 헤드셋과 같이 한 쌍을 이루는 무선 단말기에 사용 – 블루투스는 마우스와 키보드에서 유선 라인을 대신해 사용됨
WLAN	유선랜의 확장개념 또는 유선랜의 설치가 어려운 지역으로의 네트워크 제공	– WLAN은 임시 사무실과 같은 환경에서 유선랜 구축으로 인해 발생하는 불필요한 비용소모를 줄임
WMAN	대도시와 같은 넓은 지역을 대상으로 높은 전송속도를 제공	– 대학 캠퍼스와 같이 넓은 지역에서 건물간의 무선 연결 기능을 제공

WPAN(Wireless Personal Area Network)은 별도의 무선 장비가 필요 없는 소규모의 무선 네트워크 형태로서 개인 사용자간의 단거리 네트워크 구성에 많이 사용되고 있다. 일반적으로 별도의 물리적인 연결 없이 적은 수의 무선 단말기간의 통신에 사용되며, 간단하게는 사용자간 무선 단말기의 정보 공유와 전송, 노트북과 마우스와 같은 주장비와 주변기기의 연결, 그리고 특정화된 소규모 지역 내에서의 무선통신에 사용되는 기술을 말한다. 최근에는 소규모 사무실이나 일반 가정의 홈 네트워킹에 많이 이용이 되고 있으며, 특히 USN(Ubiquitous Sensor Network) 환경에 적합한 기술로서 많이 활용될 것으로 예상된다.

WLAN(Wireless Local Area Network), 즉 근거리 무선통신은 전파를 정보의 전송매체로 이용하여 가까운 거리에 있는 각종 정보처리 기기들 간에 정보를 교환하게 하는 기술을 말하며, 사무실이나 학교와 같이 한정된 지역에서 사용되며, 기존 구성되어 있던 유선랜의 일부를 대체하고 있다. 본 가이드는 WLAN의 안전한 관리 및 활용에 목적을 두고 있다.

WMAN(Wireless Metropolitan Area Network)은 도시 규모의 지역 내에서 무선 광대역 접속기능을 통해 사용자간 연결 기능을 제공한다. IEEE 802.16 표준을 통해 정의되어 있으며, 일반적으로 WiMAX라는 이름으로 불려진다. WiMax는 고정 WiMax와 이동 WiMax가 있으며, 국내에서 상용기술로 활용되고 있는 Wibro 기술은 Mobile WiMAX로서 2005년 12월, IEEE 802.16-2005 표준으로 제정되었다.

나. 무선랜 주요 표준

무선랜 기술은 802.11x 표준으로 제정되어 발전되어 왔다. 여기서는 802.11의 주요 표준 및 보안 기능에 대하여 간략히 설명하고자 한다. 〈표 2〉는 무선랜의 주요 표준들이다.

[표 2] 무선랜 주요 표준 요약

무선랜표준	표준 제정시기	주파수대역	데이터속도 (최대)	서비스 범위 (실내~외부)
802.11	1997	2.4 GHz	2 Mbps	20~100M
802.11a	1999	5 GHz	54 Mbps	35~120M
802.11b	1999	2.4 GHz	11 Mbps	38~140M
802.11g	2003	2.4 GHz	54 Mbps	38~140M
802.11n	2009[예정]	2.4~5 GHz	300 Mbps	70~250M

● IEEE 802.11/a/b/g

최초의 무선랜 표준인 802.11은 1997년 제정되었다. 802.11에서는 2,4GHz 대역을 사용하는 세 가지 전송방법(ISM – Industrial, Scientific, Medical)에 대해 정의하고 있다. 1999년에는 802.11의 개선된 변조기술과 무선전송 방법이 포함된 802.11a와 802.11b 두 가지의 표준이 발표되었다.

802.11 표준에서 중요한 내용으로는 WEP(Wired Equivalent Privacy) 암호화 방식을 들 수 있다. 무선랜용 기본 암호화 방식인 WEP은 전송되는 무선 Lan에 연결된 무선 AP와 무선 단말기 간에 주고받는 무선 전송데이터를 2개의 장비가 약속한 공유 비밀 키와 임의로 선택되는 IV(Initial Vector) 값을 조합한 64비트 또는 128비트의 키를 이용해 전송 데이터를 암호화함으로서 보안을 강화하는 방식을 말한다.

802.11b는 1999년 제정된 무선랜 표준으로서, 802.11 규격을 기반으로 개발되어 802.11과 같은 2.4GHz 주파수 대역을 사용하며, 최대 11Mbps의 전송속도를 지원한다. 전송속도의 경우, CSMA/CA 기술을 사용하므로 실제 전송속도는 최대 6-7Mbps 정도로 떨어지게 되며, 이는 모든 802.11 무선 표준에서 동일하게 적용되는 사항이다.

802.11a는 802.11과 802.11b와는 달리 5GHz의 주파수 대역을 사용하며, 최대 54Mbps의 전송속도를 제공한다. 주파수 대역이 달라 802.11과 802.11b와는 상호 호환성이 없으나, 2.4GHz 대역처럼 블루투스와 같은 다른 무선기기의 영향을 받지 않는 이점을 가지나, 5GHz 대역은 통신위성이 지상과 교신할 때 이용하

는 대역이기도 하여, 국가에 따라 옥외이용이 금지되어 있으며, 국내에서도 전파법에 의해 이용이 규제가 되다 사용이 허용된바 있다. 802.11a의 경우 최대 200m의 전송거리를 가진다.

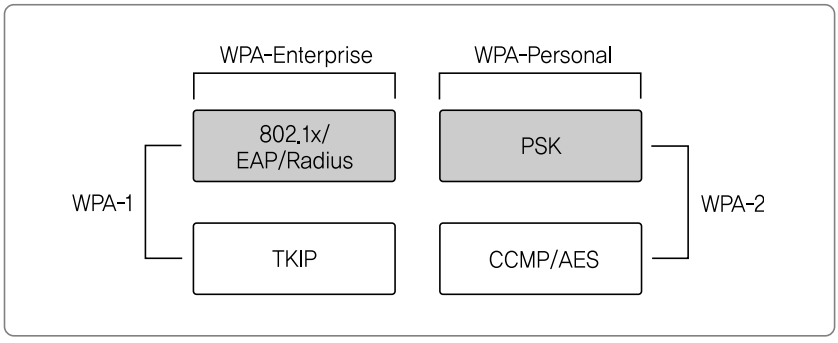
802.11g는 2003년 발표된 표준으로 802.11b와 같은 2GHz의 주파수 대역을 사용하지만, 전송방법의 수정을 통해 속도는 802.11a와 같은 최대 54Mbps를 지원한다. 802.11b와 호환을 이루면서도 속도의 향상을 가져와 현재 가장 널리 쓰이고 있는 표준이다.

● IEEE 802.11i/WPA2

802.11i는 802.11이후 여섯 번째 무선 표준으로 2004년에 제정되었다. 무선장비와 단말기간의 가상 인증기능을 제공하는 EAP(Extensible Authentication Protocol)의 도입 등 검증된 보안기술들이 포함되어, 보다 강화된 인증과 데이터 암호화 기능을 제공한다.

802.11i에는 WPA-1과 WPA-2 규격이 포함되어 있는데, 이는 암호화 방식에 따라 분류된 것으로 WPA-1은 TKIP(Temporal Key Integrity Protocol)을, WPA-2는 CCMP 암호화 방식을 사용하는 것으로 정의되어 있다.

또한, WPA 규격은 WPA-개인과 WPA-엔터프라이즈로 각각 규정되어 있는데, 이는 무선랜 인증방식에 사용되는 모드에 따라 구분되어 진다. WPA-개인은 PSK 모드를 사용하는 경우를, WPA-엔터프라이즈는 Radius 인증 서버를 사용하는 경우를 말한다.



[그림 1]
802.11i의 규격과
규격별 인증/
암호화 방식

PSK 인증방식은 인증 서버가 설치되지 않은 소규모 망에서 사용되는 방식으로, 무선 AP는 무선 단말기가 자신과 동일한 비밀키(PSK)를 가지고 있는지 802.1x에 규정된 EAPoL-Key 프레임을 활용하여 4웨이 핸드셰이킹 절차를 통해 확인하여 인증을 수행한다. 인증이 성공되는 경우에는 임시 암호 키를 256비트의 PSK로부터 생성하여 사용한다. 보통 이 PSK는 RFC2898의 PBKDF(Password-Based Key Derivation Function)V2 알고리즘에 의해 패스워드로부터 생성되며, 무선구간 보호용 암호키 생성을 위한 PMK(Pairwise Master Key)를 위하여 "PMK :=PSK"가 사용된다. 즉 미리 설정된 PSK로부터 유도되는 임시 비밀 키인 PMK를 생성한 후, 이 값을 무선 AP도 가지고 있는지 확인하고, 동일한 값을 가지고 있는 것으로 확인되면 무선랜이 활성화된다.

무선 전송데이터 암호화 방식 중, TKIP(WPA-1) 방식은 WEP의 취약점을 해결하기 위해 제정된 표준으로서, EAP에 의한 사용자 인증결과로부터 무선 단말기와 무선 AP 사이의 무선 채널 보호용 공유 비밀 키를 동적으로 생성하여 무선구간 패킷을 암호화 한다. CCMP(WPA-2)는 128비트 블록 키를 사용하는 CCM(Counter Mode Encryption with CBC-MAC)모드의 AES 블록 암호 방식을 사용한다.

현재의 무선랜 표준으로서는 802.11i가 가장 보안에 안전한 방식으로서, WPA 인증방식은 별도의 무선 인증 서버를 사용하지 않는 일반 가정이나 소규모 사무실 환경에서의 가장 효율적인 보안 강화방안이다.

- IEEE 802.11n

이론적으로 300Mbps의 처리율을 갖도록 IEEE 802.11을 개선하기 위한 표준으로 추진되고 있으며, 2009년도에 완료될 예정이다. 802.11n에서 고려하는 성능의 향상은 하드웨어적으로는 MIMO 안테나 및 수신 장치의 사용을 통해서 이루고자 한다. 또한, 소프트웨어적인 노력으로는 새로운 코딩 방법을 제안하고 있다.

2. 무선랜 네트워크 유형

802.11 무선 표준에서는 무선랜의 구성에 따라 2개의 구성유형이 제시되고 있다. 첫 번째는 infrastructure 모드로, 무선AP와 무선 단말기로 구성되는 방식이고, 두 번째는 무선 단말기 사이의 직접 통신이 이뤄지는 Ad Hoc 모드이다.

가. Infrastructure 모드(Client/Server)

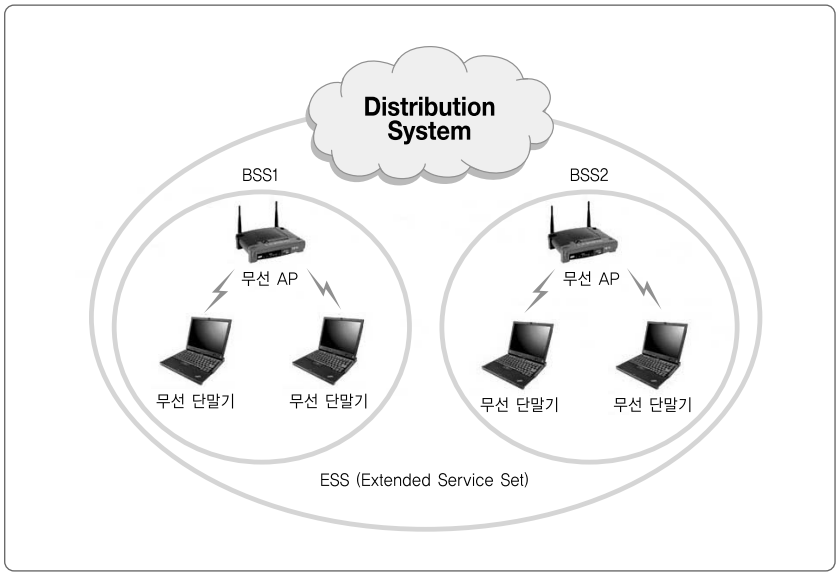
Infrastructure 무선랜은 1개 이상의 무선 AP로 구성되고, 무선 AP는 기업용 백본 라인 또는 개인용 초고속 인터넷 라인 등에 연결되어 통신이 이루어지게 된다. ad hoc 무선랜은 개별 무선 단말기 사이에서 통신이 이루어지는 무선랜으로, 최근에는 다양한 무선 단말기가 보급되고 있어 많이 이용되는 유형이다. Infrastructure 모드에서는 단말기 간의 직접적인 통신은 불가능하며, 반드시 무선 AP를 경유하여 통신이 가능하다.

하나의 무선랜은 다수의 무선 AP로 구성될 수 있으며, 무선 AP 1개와 다수의 무선 단말기로 구성된 무선랜의 최소 규모를 BSS(Base Service Sets)이라고 한다. 본 방식에서의 무선통신은 주어진 전력(Power Output) 범위 하에서 얼마나 멀리 신호가 전달될 수 있느냐에 따라 그 한계가 주어지며, 무선 접속 범위를 확장하기 위해서는 셀룰러 이동통신 시스템과 유사한 마이크로 셀을 이용하며, 사용자는 어떠한 지점에서도 항시 하나의 AP와 마이크로 셀에 연결되어 있다.

〈그림 2〉은 2개의 BSS를 포함하는 1개의 DS(Distribution System)으로, DS는 다수의 무선 AP의 연결을 통한 네트워크의 확장을 통해 임의의 크기와 복잡성을 가진 무선 네트워크 생성이 가능한데, 802.11 표준에서는 이렇게 다수의 BSS를 가지는 네트워크를 ESS(Extended Service Set)이라고 정의한다.

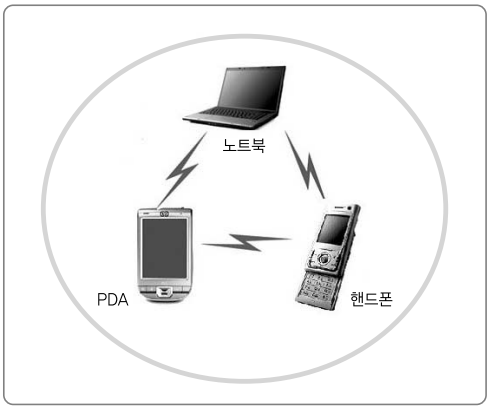
추가적으로 대부분의 무선랜이 내부의 유선랜과 연동을 통해 구성되는 것이 일반적인 형태이므로, 최초 무선랜 구축 시 무선랜을 통한 인트라넷의 접근 가능성을 고려하여 접근제한에 대한 정책과 함께 실제 접근차단을 막기 위한 보안장비의 설치도 같이 고려하도록 한다.

[그림 2] Infrastructure 모드의 구성



나. Ad hoc 모드 (Peer to Peer)

[그림 3] ad hoc 모드의 구성



Ad hoc 모드는 무선 AP를 이용하지 않고, 단말기간의 설정을 통해 통신이 이뤄지는 모드를 말한다. Ad hoc 모드의 장점은 무선단말기를 보유한 사용자끼리 별도의 추가 장비 없이도 무선 접속이 가능하다는데 있어, 통신 인프라가 없거나 구축하기 곤란한 상황에서,

[표 3] Ad hoc 네트워크의 활용 환경

활용환경	활용사례
통신 인프라 구축이 곤란한 상황/조건	– 전쟁, 재난 구조(화재, 태풍 등), 광범위한 범위에 걸친 센싱(환경오염/산불 감시)
기존 기간망의 한계 보완	– 특정조건 하에 이동 노드가 집중되는 장소 및 환경 – 홈 네트워크 내에서 다양한 이 기종 노드 간 통신 지원 – 유연한 멀티캐스팅 서비스를 통해, 이 기종 노드간 화상회의/미팅지원

이동 노드들 간의 자율적인 경로 설정과 수정이 가능하다. 〈표 3〉은 Ad hoc 네트워크의 활용 환경이다.

Ad hoc 네트워크는 보다 유연한 사용 환경을 제공하지만, 구조적으로 여러 가지 문제를 가지고 있다. 개방된 네트워크의 형태로 인해 보안에 근본적으로 취약한 구조를 가지고 있기 때문에 기기 각각의 보안설정과 접근제한이 적절히 이뤄지지 않을 경우 정보유출 등의 문제가 발생할 수 있다. 또한 제한된 하드웨어 사용으로 인하여 Infrastructure 모드에 비해 성능과 전원의 사용에 제한을 받을 수밖에 없다.

기본적으로 Ad hoc 네트워크의 보안은 다른 통신 네트워크에서 요구되는 것과 동일하지만, 다른 통신 단말기를 신뢰할 수 없는 상황이므로 암호기술에 의한 보안에 의존한다. 따라서 노드간의 신뢰할 수 있는 관계를 형성하고, 암호화를 위한 키(Key)를 Ad hoc 네트워크 전반에 분배하는 것이 주요과제이다.

Ad hoc 네트워크에서는 주로 공개키(Public Key) 암호 기술을 사용한다. 예를 들어 Ad hoc 네트워크 내 A, B, C라는 그룹이 각각 존재한다고 할 때, 그룹 A의 대표 노드가 서버 노드 역할을 하며 신뢰 위임(Trust Delegation) 절차를 주도한다. 그 후 각각 그룹의 대표 노드들은 자기 그룹이 정한 공개키를 다른 그룹과 교환하며 그룹 간 신뢰관계를 형성하게 된다. 이 같은 방식은 임의의 Ad hoc 네트워크에서 신뢰를 분배하는 역할을 담당하는 프로토콜로 일반화 할 수 있다.

Ad hoc 네트워크에서의 라우팅은 노드가 네트워크 내에서 이동하기 때문에 노드 간 패킷을 라우팅 하는 문제가 중요한 이슈가 된다. 그런데 기존 라우팅 프로토콜은 트래픽이 아무런 영향을 받지 않는 경우에도 변화에 반응을 보이고, 네트워크상의 모든 노드의 경로를 유지하기 위해 주기적으로 컨트롤 메시지를 보내야 한다.

이를 위해서는 Ad hoc 네트워크 같이 노드 이동성이 심한 경우 전원이나 링크 대역폭 등 부족한 자원들이 더 자주 소모되는 단점이 있다. 이에 대한 대안으로 설정된 것이 반응경로(Reactive Route)이다. 이 방식을 통해 패킷 라우팅이 반드시 필요한 경우에만 노드 간 루트가 성립되도록 할 수 있다.

이를 위해서는 Ad hoc 네트워크 같이 노드 이동성이 심한 경우 전원이나 링크 대역폭 등 부족한 자원들이 더 자주 소모되는 단점이 있다. 이에 대한 대안으로 설정된 것이 반응경로(Reactive Route)이다. 이 방식을 통해 패킷 라우팅이 분명히 필요한 경우에만 노드 간 루트가 성립되도록 할 수 있다.

3. 무선랜 주요 구성요소

가. 무선 단말기(Station)

[그림 4] 무선 단말기 제품들

무선 단말기는 무선랜의 가장 마지막에 위치하게 되는 장비로서, 실제 무선랜을 이용하는 사용자가 무선랜의 접속에 이용하는 장비를 말한다. 주요 무선 단말기의 종류로는 노트북, PDA, 핸드폰 등이 있다. 무선 단말기가 무선랜에 접속하기 위해서는 무선랜이 요구하는 SSID(Service Set Identifier, 이하 SSID), 인증 및 무선 전송데이터 암호화 등의 설정을 충족하여야 한다.

나. 무선 AP(AP)

[그림 5] 무선 AP 제품

무선 AP는 기존 유선랜의 가장 마지막에 위치하여 무선 단말기의 무선랜 접속에 관여한다. 무선 AP는 무선랜의 보안에도 많은 비중을 차지하는 중요한 장비로서, 무선 단말기의 접속에 필요한 관련 설정 값을 갖는다.

무선 AP의 서비스 범위는 무선AP가 지원하는 무선 표준에 따라 달라지며, 사용된 무선 표준에 따라 사용할 수 있는 무선랜의 인증방식과 무선 전송 데이터 암

호화 방식을 설정할 수 있다.

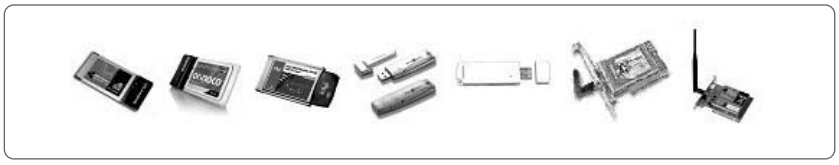
다. 무선 브릿지

무선 브릿지는 2개 이상의 무선랜을 연결하는 장비로서, 물리적으로 떨어져 있는 2개의 무선랜에 각각 위치하여 동작하게 된다. 무선랜의 특성 상 2개의 브릿지 사이에는 전파의 전송을 방해하는 물체가 존재하지 않아야 한다.

[그림 6] 무선 브릿지 제품

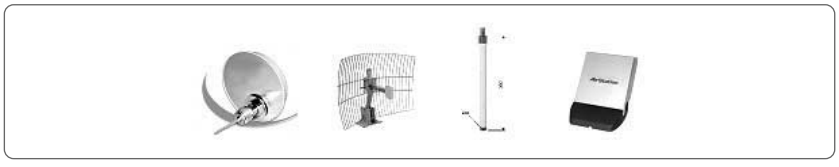
라. 무선랜 카드 및 무선랜 안테나

무선랜 카드는 무선 통신을 위한 전파를 송수신하는 장비로 무선랜 단말기와 무선랜 AP에서 사용하며 PCMCIA용, USB용, PCI용이 있다.



[그림 7] 무선랜 카드

무선랜 안테나는 무선 전파를 더 멀리 송수신하기 위해서 사용한다. 무선랜 안테나를 사용하면, 무선랜 전파를 더 멀리까지 전송할 수 있으나 늘어난 전파 전송 범위 안에서 무선랜 데이터에 대한 도청과 감청의 위험이 더 높아질 수 있는 단점이 있다. 무선랜 안테나는 방향성이 있는 지향성 안테나와 방향성이 없이 사방으로 전파를 송수신하는 무지향성 안테나가 있다.

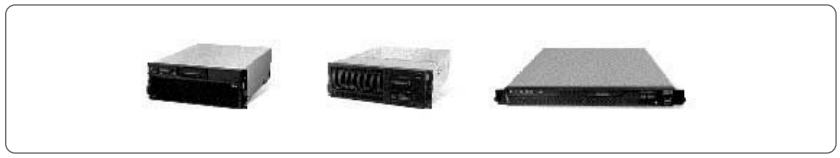


[그림 8] 무선랜 안테나

마. 사용자 인증서버

사용자 인증 서버는 무선랜 사용자의 인증을 하기 위한 인증키를 관리하고, 인증키가 없는 비인가 사용자의 접속을 차단하는 역할을 한다.

[그림 9] 사용자 인증 서버



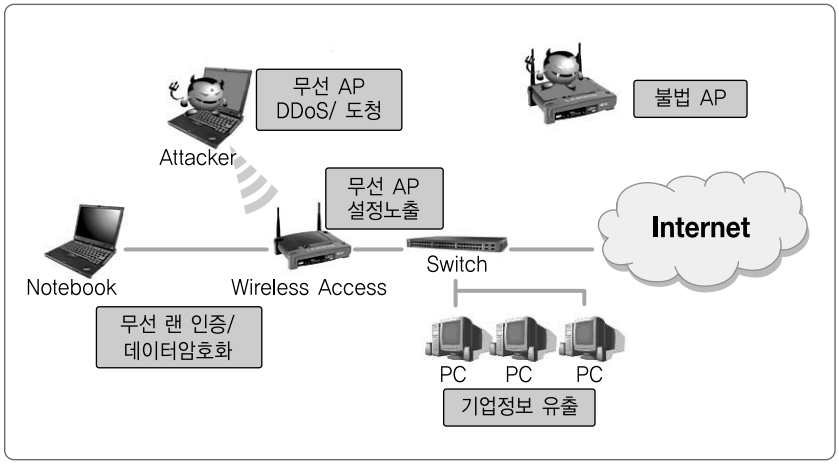
제3장 무선 서비스 주요 보안 취약성과 대응기술

Korea Information Security Agency

제3장 무선랜 서비스의 주요 보안 취약점

무선랜은 기존 유선랜의 확장 개념에서 가정 또는 일반 사무실 환경에서 사용되는 경우가 많아, 대부분이 기존의 유선랜에 무선 AP를 연결한 후, 클라이언트에 무선 랜카드를 장착하여 접속하는 형태로 구성되고 있다. 따라서 유선랜과 무선랜의 분리는 전혀 고려되지 않는 경우가 많으며, 이로 인한 보안 상 문제점이 존재하게 된다.

[그림 10] 무선랜의 취약 지점



무선 인터넷 서비스의 취약점은 크게 무선 네트워크 접속 시 인증 과정에서의 문제점과 무선 전송데이터의 암호화 취약점으로 나눌 수 있다.

최초 무선랜 표준안인 IEEE 802.11에서는 별도의 무선랜 인증과 전송 데이터에 대한 암호화는 포함되어 있지 않았다. 이로 인해 초기 무선랜은 별도의 인증절차 없이 접속이 가능하였고, 평문 데이터가 전송되었다.

IEEE 802.11b에서 처음으로 무선 전송 데이터의 암호화에 대한 내용이 포함되었는데, 802.11b에서 정의된 WEP(Wired Equivalent Privacy)은 클라이언트

와 무선 AP 사이의 구간에 적용되어 무선 전송데이터의 암호화를 통해 유선랜 수준의 보안을 제공한다. 하지만, 이 또한 취약점이 발견되어 간단한 도구를 이용해 암호화 key값을 알아내는 것이 가능한 상황이다.

이 외에도 무선 AP에 대한 서비스 거부 공격, 불법 AP를 통한 데이터 유출 가능성 등 다양한 무선 서비스에 대한 취약점이 존재한다. 본 장에서는 무선랜의 기술적 보안 취약점과 관리적 차원의 물리적 취약점에 대해 기술하고 있다.

제1절 무선랜의 보안 취약점 분석

1. 무선랜의 물리적 보안 취약점

가. 무선 장비의 물리적 보안 취약점

무선랜을 구성하는데 있어 중요한 역할을 하는 무선 AP의 경우, 원활한 서비스의 제공을 위해 외부에 노출된 형태로 위치하게 되는 것이 일반적이다. 이러한 무선 AP는 장비가 외부로의 노출로 인해 비인가자에 의한 장비의 파손 및 장비 리셋을 통한 설정 값 초기화 등의 문제가 발생할 수 있다. 〈표 4〉은 무선 장비의 물리적 보안 취약점의 대표적 유형들이다.

[표 4] 무선 장비의 물리적 보안 취약점의 유형

유 형	내 용
도난 및 파손	- 외부 노출된 무선 AP의 도난 및 파손으로 인한 장애 발생
구성설정 초기화	- 무선 AP의 리셋버튼을 통한 장비의 초기화로 인한 장애 발생
전원 차단	- 무선 AP의 전원 케이블의 분리로 인한 장애발생
LAN 차단	- 무선 AP에 연결된 내부 네트워크 케이블의 절체로 인한 장애발생

무선 AP로 연결되는 유선 네트워크 케이블에 대한 보안도 무선 AP와 마찬가지로 철저해야 하는데, 무선 AP로 연결된 네트워크 케이블이 내부 네트워크로 접근하는 하나의 수단으로 이용될 수 있기 때문이다. 따라서 기본적으로 무선 AP의

설치장소는 외부의 비인가자가 접근할 수 없는 위치에 설치를 하도록 하며, 부득이한 경우, 별도의 시설 설치를 통해 외부로부터 접근이 불가능하도록 철저히 보호하여야 한다.

나. 무선 단말기의 물리적 보안 취약점

무선 단말기는 무선랜 서비스를 구성하는 주요 요소 중의 하나로서 무선랜 사용업체의 필요조건에 따라 여러 형태의 무선 단말기가 존재할 수 있다.

무선 단말기의 유형 중 이동성을 가진 노트북, PDA 등의 경우, 항상 분실의 위험성이 존재하게 되는데 이 경우, 저장 데이터의 유출은 물론 무선랜의 내부 보안 설정이 함께 유출될 가능성이 존재하게 된다.

따라서, 무선 단말기의 경우 업무시간 이외에는 반드시 정해진 장소에 보관 하도록 하고, 보관 시에는 단말기의 전원을 종료하여 외부 비인가자의 오용을 사전에 차단하도록 한다. 또한 무선 단말기의 최초 사용 시 로그인 절차 등을 적용하여 비인가자의 접근을 차단하도록 한다.

2. 무선랜의 기술적 취약성

무선랜은 공기를 전송매체로 사용하는 서비스의 특성 상 많은 취약점이 존재하게 된다. 또한 불특정 다수의 신호수신이 가능함으로 인해 도청이 가능하고, 무선 전파를 전송하는 무선 장비에 대한 공격이 가능하다. 또한 유선랜에서 존재하는 여러 가지 공격 기법이 사용가능하다.

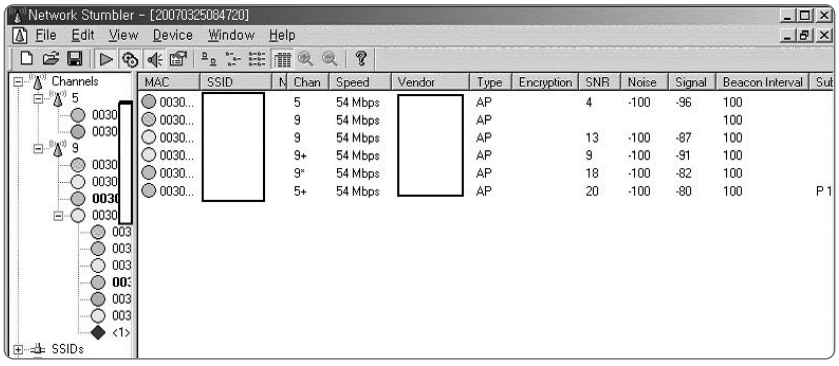
가. 도청

무선랜의 가장 근본적인 문제점이라고 할 수 있는 것이 바로 도청이다. 무선 AP에서 발송되는 전파의 강도와 지형에 따라 서비스가 필요한 범위 이상으로 전달될 수 있으며, 이 경우 외부의 다른 무선 클라이언트에서 무선 AP의 존재여부를 파악할 수 있고 더불어 전송 무선 데이터의 수신을 통한 도청이 가능하게 된

다. 이 경우, 만일 무선 데이터가 암호화 되어있지 않은 경우 모든 전송 데이터를 볼 수 있어 심각한 문제가 발생하게 된다.

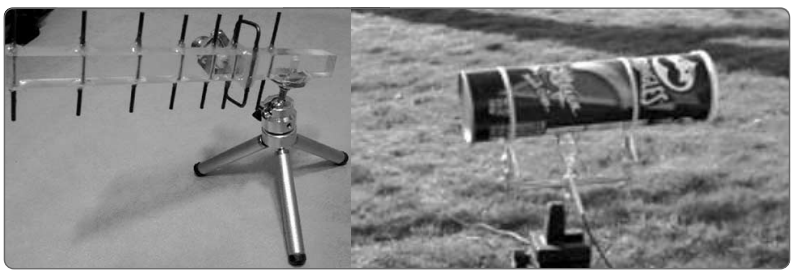
도청은 기본적으로 무선랜 카드가 탑재된 클라이언트는 모두 이용 가능하며, 일반적으로 암호 해독에 이용되는 프로그램을 위한 노트북과 신호 수신을 위한 안테나 등이 사용된다.

무선 전송데이터의 도청에 이용되는 별도의 S/W는 인터넷을 통해 손쉽게 구할 수 있는데, 이를 이용해 탐지되는 무선랜의 기본적인 구성을 파악할 수 있다. 다음 〈그림 11〉은 대표적인 무선랜 분석 S/W인 Net Stumbler의 화면으로 무선랜의 구성요소인, SSID 정보, 무선랜 암호화 방식정보, 무선랜의 속도, 신호감도 등의 정보를 확인하는 화면이다.



[그림 11] Netstumbler를 이용한 무선랜 구성정보의 수집

이러한 S/W와 함께 원거리에서도 〈그림 12〉와 같은 무선랜의 신호를 탐지하기 위한 별도의 무선 통신 수신안테나를 이용하여 미약한 무선 신호를 증폭시켜 무선랜의 전송데이터를 무단으로 취득하게 된다.



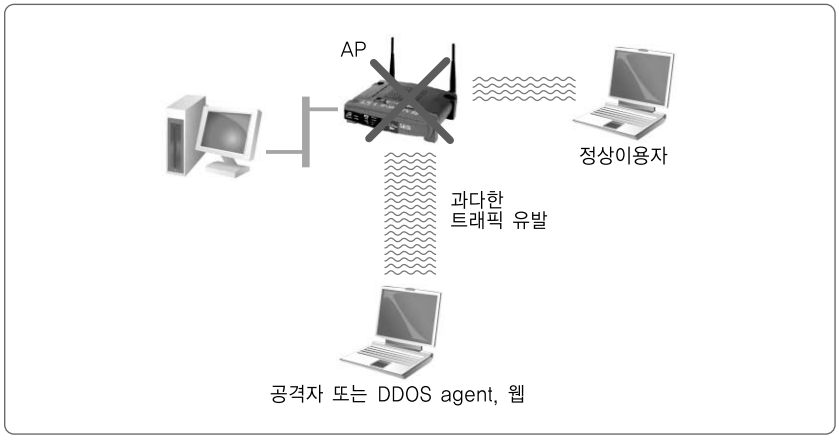
[그림 12] 무선 통신 수신용 안테나의 예

나. 서비스 거부

서비스 거부란 무선 서비스를 제공하는 무선 AP 장비에 대량의 무선 패킷을 전송하는 서비스 거부 공격을 통해 무선랜을 무력화하는 것을 말한다. 또한, 무선랜이 사용하는 주파수 대역에 대해 강한 방해전파를 전송하는 것도 통신에 영향을 주게 된다.

무선 클라이언트와의 통신을 위해 설정된 SSID를 포함한 "Probe Request" 메시지를 브로드케스트로 전송하게 된다. 이 신호를 수신한 무선 AP는 해당 클라이언트가 접속하는 것을 허용한다면 "Probe Response" 메시지를 회신하게 된다. 이러한 과정에서 다량의 request 메시지를 무선 AP로 전송하는 경우, response 메시지 회신 동작의 반복으로 인해 다른 무선 단말기의 접속이 불가능하게 된다.

[그림 13] 무선랜에 대한 DD●S 공격

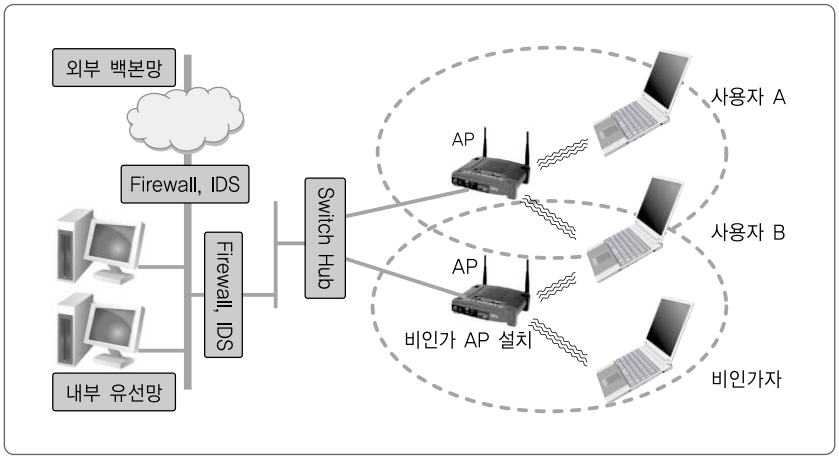


이러한 무선 AP에 대한 서비스 거부 공격은 실제 내부 네트워크로의 침입으로까지 발전되지는 않지만, 백화점과 같이 실시간으로 무선랜을 이용해 주요 업무가 이루어고 있는 경우, 공격으로 인해 발생되는 무선랜의 중지는 치명적인 결과를 가져올 수 있게 된다.

이와 같이 무선랜 자체를 이용해 회사의 중요업무를 수행하는 경우에는, 서비스 중지 시 대체할 수 있는 별도의 유선랜을 준비하여 만일의 경우에 대비하는 것이 반드시 필요하다.

다. 불법 AP(Rogue AP)

공격자가 불법적으로 무선 AP를 설치하여 무선랜 사용자들의 전송 데이터를 수집하는 것으로, 불법 AP의 설치유무를 탐지하는 것은 어렵지 않으나 무선의 특성 상 정확한 불법 AP의 위치를 파악하는 것은 쉽지 않은 일이다. 일부 무선 보안 솔루션에서는 다수의 무선 AP를 이용해 불법 AP의 무선 강도 등을 참고로 대략적인 불법 AP의 위치정보를 제공하고 있기는 하나 실제 정확한 위치를 파악하고 제거하기는 어려울 수 있다.



[그림 14] Rouge AP 예

불법 AP의 경우, 별도 전원연결이 필요하므로 무선랜이 적용된 사무공간의 철저한 관리를 통해 불법 AP가 설치되지 않도록 관리를 하는 것이 가장 중요한 부분이다. 또한 불법 AP의 설치여부에 대해 보안정책내 별도의 항목을 추가하여 주기적으로 무선랜 서비스 지역에 대한 점검을 진행하여 불법 AP가 설치될 수 있는 위험성을 줄여야 한다.

라. 무선 암호화 방식

무선 데이터 암호화 방식으로 많이 사용되고 있는 WEP(Wired Equivalency Protocol)은 전송되는 MAC 프레임들을 40비트의 WEP 공유 비밀 키와 임의로 선택되는 24비트의 Initialization Vector(IV)로 조합된 총 64비트의 키를 이용

한 RC4 스트림 암호화방식으로 보호한다.

기본적으로 무선 클라이언트와 무선 AP는 동일한 패스워드 문장으로부터 4개의 고정된 장기 공유키를 생성한 후 이들 중에서 하나를 선택하여 암호 및 인증에 활용한다. 문제는 선택된 공유키의 KEY ID와 IV값을 평문으로 상대방에게 알려줘야 하기 때문에 WEP키가 추출될 수 있는 약점이 존재한다.

■■■ WEP 인증방식의 문제점

- 짧은 길이의 초기벡터(IV)값의 사용으로 인한 IV값의 재사용 가능성 높음
- 불완전한 RC4 암호 알고리즘 사용으로 인한 암호키 노출 가능성
- 짧은 길이의 암호키 사용으로 인한 공격 가능성
- 암호키 노출로 인한 무선 전송데이터의 노출 위험성

WPA/WPA2의 경우에도 초기 무선랜에 접속하는 인증단계에 사용되는 Pre-shared 키 값(PSK)을 무선 전송패킷의 수집을 통해 유추해낼 수 있는 취약점이 존재하는 것으로 알려져 있으나, WEP과는 달리 무선 데이터 전송 시 고정된 키 값을 이용해 무선 전송데이터를 암호화 하지 않으므로 단순히 무선 전송 데이터 패킷의 수집을 통해서는 무선 전송데이터의 암호화 키 값을 유추해낼 수는 없다.

WPA/WPA2의 무선 AP와 무선 단말기간의 인증에 PSK 또는 802.1x/EAP 인증방식을 이용한다. PSK 인증방식의 경우, 별도의 인증 서버가 설치되어 있지 않은 소규모 망에서 사용되는 인증방식으로서, 초기 인증에 사용되는 PSK 값을 이용해 4-웨이 핸드쉐이킹(4-way handshaking) 과정을 통해 무선 AP와 무선 단말기가 동일한 값을 가지고 있는지 확인하게 된다.

■■■ PSK 인증방식 절차

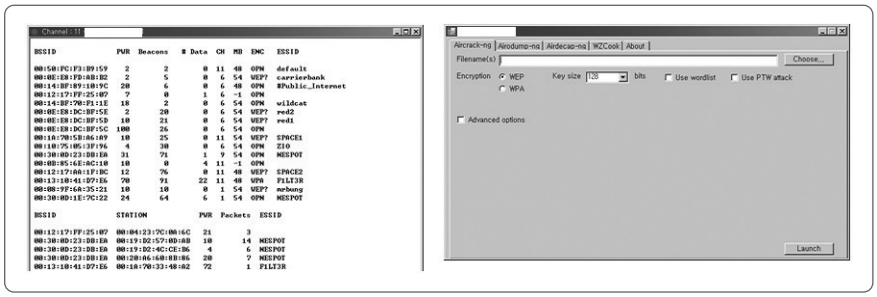
① 무선 단말기는 PSK와 함께 암호화 방식을 선택한 후, 요청메시지에 담아 개방 시스템 방식으로 무선 AP로부터 인증 후 연결
② PSK를 PMK로 직접 설정하고, EAPoL-Key 프레임을 사용한 4 웨이 핸드쉐이킹 과정을 통해 무선 단말기와 무선 AP간 임시키를 설정하고 검증.
③ PMK 확보여부가 인증되면, 무선 단말기와 무선 AP가 동일한 PSK를 가진 것으로 인증

문제는 이러한 인증 과정에서 별도의 암호화가 되어 있지 않아 무선 패킷 수집을 통해 비밀키 값을 유추하는 것이 가능하다는데 있는데, 기존 WEP 암호화 방식의 공격과 마찬가지로 4-handshake 과정의 초기 인증패킷만을 수집하여 준비된 사전파일을 사용하여 고정된 PSK 값의 유추가 가능하다.

하지만 PSK 값의 유추 작업이 항상 가능한 것은 아니며, 일반적으로 사용되는 단어를 사용하거나, 짧은 자리수의 암호를 사용하는 경우에만 가능하다. 실제 WPA와 802.11i 관련 문서에서는 최소 20자 이상의 비밀키를 사용하도록 권고하고 있으나 대부분의 일반 사용자는 짧은 자리 수의 암호나 일반 단어를 사용하는 경우가 대부분이어서 이러한 취약점에 노출되게 된다.

이러한 WEP과 WPA/WPA2 취약점 공격도구는 인터넷을 통해 쉽게 구할 수 있기 때문에 개인 사용자 또는 소규모 무선랜을 사용하는 중소업체의 경우, 공격 대상 무선 네트워크 주변에서 패킷 수집 작업을 통해 무선 전송데이터 암호화에 취약점을 악용할 수 있다.

따라서 보다 안전한 무선랜의 운영을 위해서는 WEP의 사용보다는, WPA/WPA2를 사용하되 가능한 긴 길이의 비밀키를 설정하거나, 추가적인 인증 서버의 운영이 권고된다.



[그림 15] 무선 암호화 인증 공격 도구

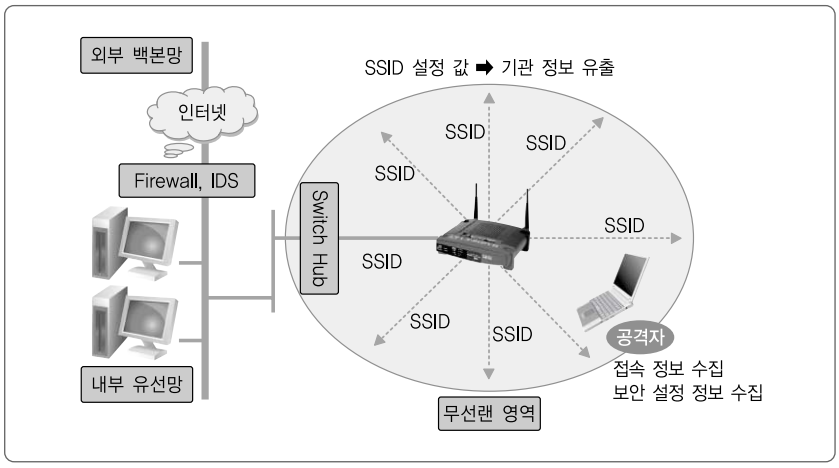
마. 비인가 접근

(1) SSID 노출

기본적으로 무선랜에서 사용되는 기본적인 인증방식은 개방형 인증 방식, 즉 별도의 인증절차 없이 무선 AP와의 연결이 이루어지는 방식이다. 무선 AP에 별

도의 무선 전송데이터의 암호화 방식이나, 인증절차가 설정되어 있지 않은 경우에는 무선 전송데이터의 모니터링을 통해 SSID 값을 획득하고, 획득한 SSID 값을 무선 단말기에 설정하는 것만으로 무선랜으로의 불법적인 접속이 가능하게 된다.

[그림 16] SSID 값을 이용한 공격정보 수집



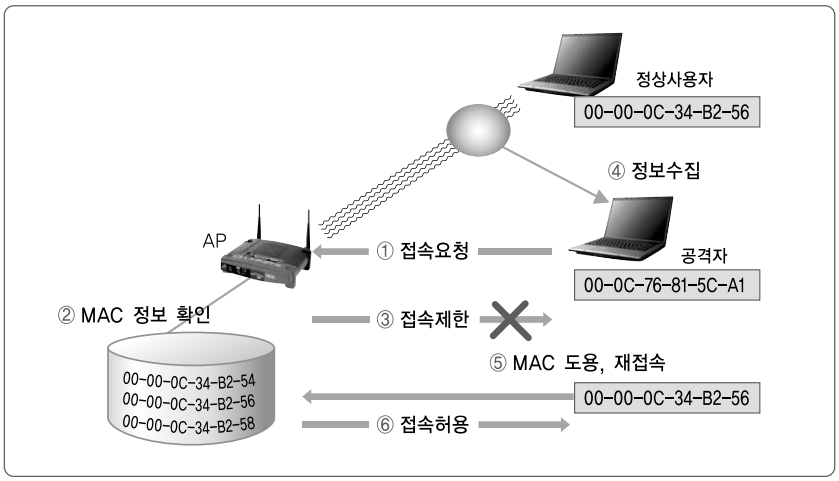
일반적인 무선 AP의 경우, SSID 값을 broadcast 하도록 설정되어 있어, SSID 값을 이용해 공격에 필요한 정보의 수집이 가능하며, 별도의 공격기술이나 도구의 사용이 없이도 공격에 필요한 기본적인 정보의 수집이 가능하다.

(2) MAC 주소 노출

무선랜 환경에서 접근제어를 위해서 MAC 주소 필터링을 적용하기도 한다. 즉, 무선 전파를 송수신하는 무선랜 카드에 부여된 MAC 주소 값을 이용하여 무선랜 서비스의 접속을 제한하는데 활용하는 것이다. 이러한 MAC 주소 필터링은 간단한 접근제어 방식이면서 공격의 위험을 줄이는데 효과적이다. 또한, 네트워크 규모와 관계없이 적용될 수 있는 보안 메커니즘으로 무선랜뿐만 아니라, 유선 네트워크에서도 많이 활용되고 있는 방법이다. 하지만, MAC 주소 필터링은 공격자가 정상사용자의 MAC 주소를 도용함으로써 쉽게 무력화되고 있는 실정이다.

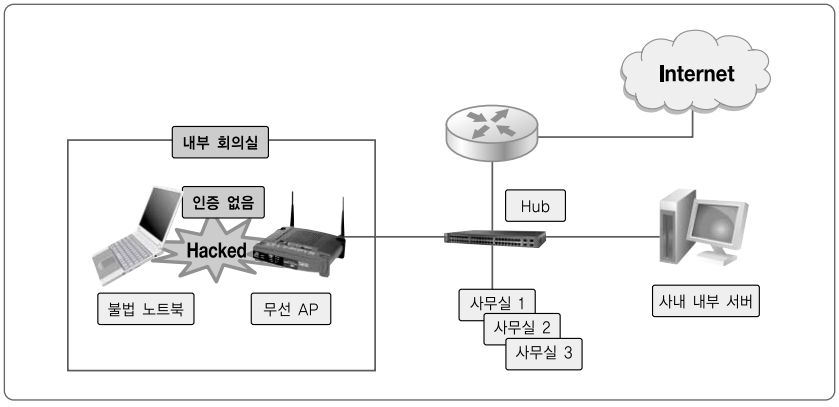
아래 〈그림 17〉에서는 공격자에 의해 정상사용자의 MAC 주소가 도용되어, AP에 설정된 MAC 주소 필터링을 무력화 시키며 접속 요청을 시도하는 모습을 나타

내고 있다. 즉, 공격자가 자신의 접속 요청이 제한당하고 있음을 인지하고, 정상 사용자와 AP 사이의 신호를 분석하여 정상 사용자의 MAC 주소를 알아낸 후, 자신의 MAC 주소를 정상 사용자의 MAC 주소로 위조하여 접속을 재요청하고 있다. 이 경우 AP는 정상 사용자의 접속 요청으로 여기고 접속을 허용하게 된다.



[그림 17] 무선랜 분석 도구를 이용한 MAC 주소 도용

실제, 별도의 무선랜 보안설정을 하지 않은 개방형 인증방식을 사용하는 곳은 우리 주변에서 쉽게 확인할 수 있으며, 만일 〈그림 18〉과 같이 이러한 무인증 무선 AP가 회사 내의 유선 네트워크에 연결되어 있는 경우, 별도의 인증절차 없이 직접 내부의 서버와 자료에 접속을 할 수 있게 되어 심각한 보안상의 문제가 발생하게 된다.



[그림 18] 개방형 인증 무선 AP를 이용한 사내 네트워크 접속사례

3. 무선랜의 관리적 취약성

가. 무선랜 장비 관리 미흡

무선랜을 운영하는 대부분의 기관에서는 사용하는 AP의 개수 정도만 파악하고 있어, 실제로 장비가 파손되거나 도난당하여 무선랜 서비스를 제공하지 못하고 있어도 이를 파악하지 못하는 경우가 발생할 수 있다. 이를 방지하기 위해, 기관에서 사용하는 무선랜 장비인 AP와 무선랜 카드 등에 대한 장비 운영현황과 사용자 현황 등을 파악하여야 한다. 뿐만 아니라, 무선랜 장비에서 제공하는 기본 값 혹은 초기 값을 사용하고 있는 곳이 많아, 공격자의 표적이 되고 있다. 특히, 보안설정을 위해 사용하는 WEP 등도 장비에서 제공하는 초기 값을 사용하고 있어 보안에 매우 취약한 것으로 드러나 있다.

나. 무선랜 사용자의 보안의식 결여

무선랜 운영 기관에서 마련한 보안정책과 보안기능을 사용하지 않는 사용자가 있으면, 전체 기관의 정보보호에 허점이 발생하기 마련이다. 사용자의 정보보호 무관심으로 인해 무선랜 단말기에 보안기능을 미설정하거나, 무선랜 정보보호를 위해 사용하기로 정한 보안기능을 사용하지 않는 경우가 많은데, 이렇게 무선랜 보안기능을 설정하지 않은 사용자는 공격자의 표적이 될 수 있다. 또한, 사용자들이 정보보호에 대한 인식 부족으로 기관에서 설정한 보안설정 값이나 암호키 값을 협력업체 직원이나 외부 방문객들에게 노출시키는 경우도 발생한다. 이러한 경우가 발생하면 보안 관리자가 설정해 놓은 정보보호에 관한 노력이 한순간에 무너질 수 있고, 이로 인해 외부인의 침해가 발생할 수 있다. 사용자의 부주의로 인한 비인가 AP의 설치 및 운영 등은 앞에서 설명한 것처럼 공격자가 내부 망을 침투할 공격통로로 악용될 소지가 있어, 이로 인한 많은 피해가 발생할 수 있게 된다.

무선랜을 사용하는 기관에서는 관리자뿐만 아니라, 무선랜을 사용하는 사용자도 항상 보안에 관심을 갖고 무선랜을 사용해야 한다. 아무리 잘 수립된 보안정책

과 이를 적용하기 위한 보안 장비가 있다하더라고 막상 사용자가 이를 따르지 않으면 무용지물이 되기 때문이다.

다. 전파관리 미흡

무선랜을 설치하여 운영하는 기관의 대부분은 유선 네트워크 관리자가 무선랜도 관리하고 있는 경우가 많다. 이러한 경우에, 유선 네트워크 관리자가 무선랜에서 사용하는 전파 특성을 파악하지 못하는 경우가 많다. 즉, 전파 자원의 관리 미흡으로 인해 무선랜 환경에 취약성이 발생한다. 이러한 취약성에는 다음과 같은 것들이 있다.

우선, AP의 전파 출력 조정을 하지 않아 기관 외부로 무선랜 전파가 유출되는 경우이다. 기관 외부로 전파가 도달되면, 기관외부에서 공격자에 의한 공격이 발생할 수 있다. 이러한 경우에는 반드시 기관 내부와 외부에서 전파 출력을 측정하여, 적절한 무선랜 서비스 영역을 제공할 수 있도록 해야 한다.

다음은 무선랜 채널설정이 미흡한 경우로, 무선랜은 중심 주파수를 기준으로 하여 3개 채널까지 전파 간섭을 일으키고 있다. 즉, 주파수 간섭이 발생하지 않도록 채널을 설정하기 위해서는, AP를 설치하여 설정할 때, 설치한 AP에서 수신되는 인근 AP의 채널과 3개 이상 떨어뜨려 사용할 채널을 선택하여야 한다.

제2절 사용자 인증 취약성과 대응기술

본 절에서는 무선랜 사용자 인증 메커니즘이 갖고 있는 취약성을 분석해 보고, 각 취약성의 대응방법을 알아본다. 앞 절에서도 설명한 것처럼 무선랜은 전파가 도달되는 거리에 있는 모든 사람들이 접속을 시도할 수 있다. 비인가자의 접속허용으로 인한 내부망의 침해사고를 미연에 방지하기 위하여 강력한 사용자 인증이 반드시 적용되어야 한다.

1. SSID 설정과 폐쇄시스템 운영

가. SSID 설정을 통한 접속제한

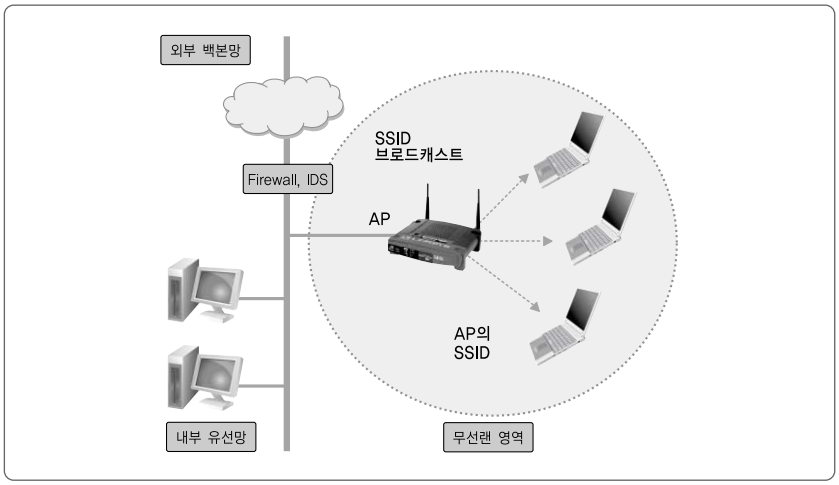
SSID는 AP가 제공하는 무선랜 서비스 영역을 식별하기 위해 사용하는 ID이다. 무선랜 서비스에 접속하려고하는 사용자는 현재 자신의 위치에서 접속이 가능한 무선랜 서비스를 식별해야 한다. 무선랜 장비인 AP는 SSID 신호 브로드캐스트하여 무선랜 서비스가 제공되고 있음을 접속을 원하는 사용자에게 알린다. 사용자는 AP가 보내온 SSID를 이용하여 연결을 원하는 무선랜 서비스에 접속을 시도한다.

무선랜 서비스를 식별하기 위한 SSID에 관한 사항을 좀 더 자세히 살펴보면, 무선랜 환경은 사용자의 접속 편의와 무선랜 서비스 식별을 쉽게 하기 위해서 SSID 값을 무선랜 서비스를 제공하는 기관의 이름이나, 읽고 기억하기 쉬운 값으로 설정하고 있다. 무선랜 장비인 AP는 자신이 제공하는 무선랜 서비스 영역을 좀 더 많은 사용자에게 알려, 자신의 서비스를 이용할 수 있도록 하고 있다. 이를 위하여, AP는 자신이 제공하는 무선랜 서비스를 식별하기 위한 식별자인 SSID를 브로드캐스트하는 것을 기본설정으로 하고, 이러한 설정은 특정 무선랜 서비스를 이용하고자 하는 사용자에게 SSID 값을 알려 좀 더 쉽게 연결을 시도할 수 있도록 하고 있는 것이다.

하지만, 만일 SSID를 모르는 사용자일 경우에는, 자신이 위치한 곳에서 제공되는 무선랜 서비스에 대한 정보가 없기 때문에 무선랜 서비스에 접속을 시도할 수 없게 된다. 이러한 특성을 이용하여 SSID 설정 방법을 이용하여 가장 단순한 접근제어를 적용할 수 있다. 즉, 무선랜 관리자가 SSID를 브로드캐스트하지 않도록 설정하고, 인가된 사용자에게는 미리 SSID를 알려주어, 알려준 SSID로 연결을 시도하도록 한다면, SSID를 모르는 공격자의 연결 시도를 줄일 수 있다. 하지만, 이러한 단순한 접근제한은 무선랜 분석도구를 이용하여 SSID를 알아냄으로써, 공격자의 접속 요청 시도가 가능할 수 있게 된다.

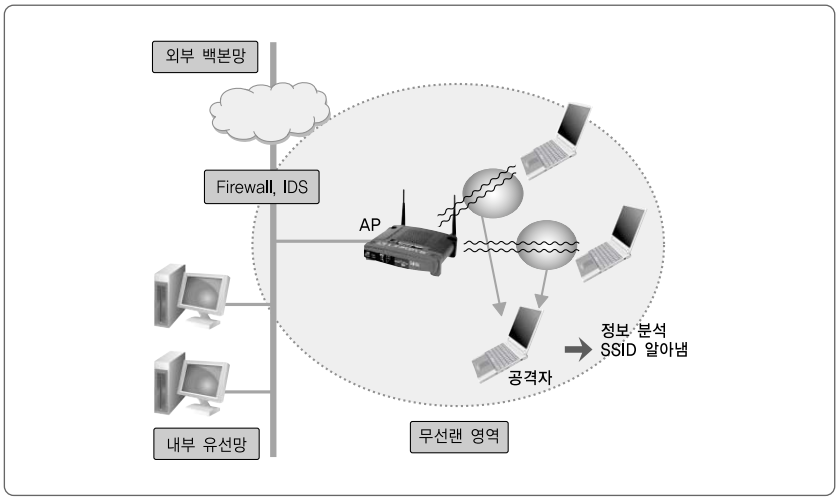
〈그림 19〉와 〈그림 20〉는 공격자가 SSID 값을 알아내는 방법을 나타내고 있

다. 〈그림 19〉의 경우에는 AP에서 SSID를 브로드캐스트하는 경우로, 이러한 경우에는 특별한 기술이 없어도 공격자가 단순히 AP 전파 수신영역 안에만 존재하면, 브로드캐스트하는 SSID 값을 알아낼 수 있다.



[그림 19] AP에서 SSID를 브로드캐스트 하는 경우

〈그림 20〉의 경우에는 AP에서 SSID를 브로드캐스트하지 않고, 숨김 모드로 설정한 경우이다. 이 경우에 공격자는 쉽게 SSID를 알아낼 수는 없지만, 무선 데이터 분석 도구를 사용하여 무선 데이터를 수집 분석하는 과정을 통해서 SSID를 알아낼 수 있다. SSID를 숨김 모드로 사용할 경우에는 공격자에게 SSID를 알아



[그림 20] SSID를 숨김 모드로 설정한 경우

내기 위해서 무선랜 분석도구를 사용하여 일정 시간이상의 무선 데이터를 수집하여 분석하여야 하는 불편함을 준다. 이러한 과정을 통해서 공격자가 공격을 포기하도록 유도한다.

나. 폐쇄시스템 운영

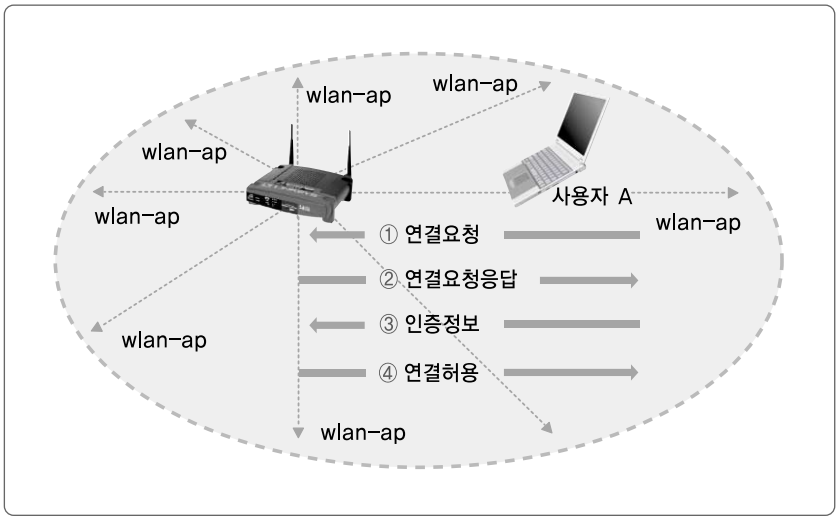
일반적인 의미에서 폐쇄 시스템(Closed System)의 운영이란 네트워크에 개방된 자원이 없도록 관리하는 것을 말한다. 폐쇄시스템 운영의 간단한 예로는, 네트워크에 공유폴더를 생성하지 않는 것이다. 하지만, 많은 사용자들은 운영상의 편의를 위해서 사용자들끼리 서로의 자료에 접근할 수 있도록 공유폴더를 만들어 네트워크상에 개방하고 있다. 보안성의 관점에서 본다면, 공유폴더를 만들어 개방하여 사용하지 않는 것이 가장 좋으나, 꼭 사용해야 할 경우에는 공유폴더에 반드시 접속 가능한 사용자와 암호를 설정하여 사용해야 한다.

무선랜 환경에서 의미하는 폐쇄 시스템이란, SSID 값을 숨김 모드로 놓고, 이와 더불어 접근제한 규칙을 적용하는 것을 말한다. 이제 폐쇄 시스템 운영과 관련된 사항을 무선랜 연결 절차를 통하여 알아보자. 아래 〈그림 21〉은 무선랜의 연결 설정 절차를 나타내고 있다. 아래 〈그림 21〉는 무선랜 서비스를 이용하고자 하는 〈사용자 A〉가 SSID 값이 〈wlan-ap〉인 AP가 제공하는 서비스에 접속하는 절차를 설명하고 있다.

무선랜 〈사용자 A〉가 SSID가 〈wlan-ap〉인 AP에 접속하여 무선랜 서비스를 이용하고자 한다면 우선, 〈사용자 A〉가 무선랜 서비스를 제공하는 AP의 SSID를 알아야 한다. 〈사용자 A〉가 무선랜 서비스를 제공하는 AP의 SSID를 알아내는 방법은 두 가지로 생각해 볼 수 있다. 가장 간단한 방법이면서 현재 많은 무선랜 환경인, 무선랜 AP가 SSID를 브로드캐스트하는 경우를 생각해보자. 이 경우에는 〈사용자 A〉가 AP의 전파 수신영역 안에 있다면, AP가 브로드캐스트하는 신호를 수신하여 SSID 값이 〈wlan-ap〉임을 알아낼 수 있게 된다. 그러나 무선랜 AP가 SSID를 브로드캐스트하지 않는 경우에는 〈사용자 A〉가 AP의 전파 수신영역에 있다고 하더라도, AP가 SSID 값을 브로드캐스트하지 않아 그 값을 알 수가

없게 된다. 이러한 경우에는 무선랜 관리자에게 문의하여 SSID이 〈wlan-ap〉임을 알아내야 한다. 위의 두 가지 방법을 통하여 이용하고자하는 무선랜 서비스의 SSID 값인 〈wlan-ap〉를 알아냈다면, 〈그림 21〉에서 나타내고 있는 것과 같은 절차를 다음과 같이 거쳐서 무선랜 서비스를 이용할 수 있다.

[그림 21] 무선랜 연결 설정 절차



① 〈사용자 A〉는 자신이 이용하고자하는 무선랜 서비스를 제공하는 SSID인 〈wlan-ap〉를 선택하여 연결요청 메시지를 보낸다. 이 단계에서는 AP가 사용하는 채널을 알 수 없음으로, 〈사용자 A〉는 AP의 응답 메시지가 올 때까지, 자신의 연결요청 메시지를 1번 채널부터 14번 채널까지 바꾸어 가면서 계속해서 전송한다.

② AP가 자신이 사용하는 무선랜 채널로 전송받은 연결요청 메시지에 대하여 〈사용자 A〉에게 응답 메시지를 보낸다. 이 단계에는 AP가 자신이 사용하는 채널로 〈사용자 A〉에게 응답 메시지를 보내므로 〈사용자 A〉는 이 응답메시지를 받음으로써, AP가 사용하는 무선랜 채널에 관한 정보를 알게 된다. 앞으로 일어나는 〈사용자 A〉와 AP 사이의 무선 통신은 AP 보내온 응답메시지가 사용하던 채널- AP가 사용하는 채널을 이용하게 된다.

③ 〈사용자 A〉와 무선랜 서비스를 제공하는 AP와 인증을 수행한다. 인증은 무

선랜에서 정한 인증 메커니즘을 이용한다. 사용자 인증에 관한 구체적인 방법은 향후에 좀 더 자세히 알아보기로 한다. 이 단계에서는 인증 메커니즘에서 정한 인증에 필요한 정보들을 주고받는 단계이다.

④ 인증이 성공적으로 이루어지면, 무선랜 AP를 통하여 무선랜 서비스를 이용할 수 있다는 연결 허용 메시지를 〈사용자 A〉에게 전송한다. 이제 〈사용자 A〉는 SSID 〈wlan-ap〉에서 제공하는 무선랜 서비스를 이용할 수 있게 되었다.

⑤ 무선랜을 이용하여 인터넷 서비스를 이용하려면, 유선 네트워크에서와 마찬가지로 〈사용자 A〉의 IP 관련 정보를 설정해야 한다. 무선랜 환경을 이용하여 인터넷을 사용하기 위해서 〈사용자 A〉 단말기에 IP, 서브넷 마스크, 게이트웨이, DNS 등을 설정해야 한다. 하지만, 대부분의 무선랜 환경에서는 이러한 IP 설정의 불편함을 줄이기 위해서 AP에 DHCP(Dynamic Host Configuration Protocol) 기능을 사용하여 자동으로 IP를 부여하고 있다. 이제 무선랜 연결 절차를 마치고, 〈사용자 A〉는 SSID 〈wlan-ap〉를 통하여 무선랜 서비스를 제공받을 수 있게 된 것이다.

만일, AP에서 자신의 SSID 값인 〈wlan-ap〉를 브로드캐스트하도록 설정한 경우에는 AP의 전파 수신영역에 있는 모든 사용자들이 SSID 〈wlan-ap〉를 이용하여 연결요청 메시지를 보내올 것이다. 뿐만 아니라, 무선랜 서비스를 이용하려는 공격자들에게 무선랜 서비스를 제공하는 곳임을 알리는 것과 마찬가지 효과가 발생하게 된다. 즉, SSID의 브로드캐스트는 불필요한 연결요청 메시지를 유발하고, 공격자에게 무선랜 서비스가 제공되고 있음을 알리게 된다. 또한, 공격자들이 사용자 인증 메커니즘의 적용여부 등을 알기 위한 접속시도가 증가하게 되는 등의 취약점이 발생하게 된다.

이러한 취약점을 제거하기 위해서, AP에서는 SSID를 숨김 모드로 설정하여 사용하는 방법을 지원하고 있다. SSID를 숨김 모드로 설정하면, SSID를 모르는

사용자의 접속시도를 현저하게 줄일 수 있다.

하지만, 무선랜 기술은 HotSpot 서비스를 원활하게 제공하기 위해서 발전하였다. 즉, SSID를 사용자가 직접 선정하지 않더라도 무선랜 단말기가 알아서 자신에게 보내오는 AP들의 신호를 비교하여 가장 좋은 품질의 신호를 보내오는 AP에 자동으로 접속을 시도하는 방식을 제공하고 있다. 이러한 기술은 무선랜을 이용하고자하는 〈사용자 A〉가 자신이 이용하고자하는 특정 무선랜 서비스를 제공하는 AP의 SSID를 선정하지 않고, SSID를 NULL 값으로 설정하면, 무선랜 단말기가 자동으로 자신에게 강한의 신호를 보내는 AP에 접속을 요청하게 된다. 이러한 접속 요청이 가능함으로 AP의 SSID를 숨김 모드로 설정하여도 접속을 요청하는 사용자들이 생기기 마련이다. 이러한 비인가자들의 접속을 근본적으로 차단하기 위해서 일부 AP에서는 SSID 값을 NULL로 하여 접속을 시도하는 사용자들의 연결요청 메시지에 대하여 접속을 차단하도록 하는 기능을 제공하고 있다. 이렇게 SSID 값을 NULL로 하여 접속을 요구하는 사용자를 차단하도록 AP를 설정하여 운영하는 것을 폐쇄시스템을 구성하여 운영한다고 한다.

이러한 SSID 설정과 관련된 무선랜의 폐쇄 시스템 운영은 네트워크 ID를 스푸핑 할 수 있는 여지는 있으나, WEP을 설정 여부를 알아보려는 연결 시도를 막을 수 있다. 뿐만 아니라, 무선랜에서 폐쇄 시스템을 적용하면 다음과 같은 보안상 장점이 있다.

우선, SSID 숨김으로 설정하고 폐쇄시스템을 운영하면, SSID를 모르는 사용자의 접속 시도가 현저하게 줄고, SSID를 NULL로 설정하여 SSID에 관계없이 연결을 설정하려고 접속 시도를 차단할 수 있는 장점이 있다. 또한, 무선랜 분석 도구인 NetStumbler 등을 이용한 스푸핑을 미연에 방지할 수 있다는 장점이 있다. 뿐만 아니라, 폐쇄 시스템은 구현하기도 쉽고, 운영을 위한 추가의 노력을 요구하지도 않다는 장점도 있다. 다만, 새로운 사용자와 새로운 하드웨어의 적용과 네트워크 시스템 변경 시에 무선랜 환경을 유지 관리해야하는 관리자의 관심이 필요하다.

2. MAC 주소인증

가. MAC 주소 구성

MAC 주소는 네트워크 접속 장비인 랜카드에 부여되는 48bit의 주소 값으로, 랜카드 제조회사가 완성된 랜카드 제품을 출시할 때 하드웨어에 부여하는 값을 말한다. 48bit의 MAC 주소는 24bit의 제조회사 식별 값과 24bit의 제조회사에서 제품 완료시 부여하는 시리얼 번호로 구성된다. 즉, 랜 카드에 부여된 MAC 주소 값을 확인하면 제조회사까지도 알 수 있다. 이러한 특성을 갖는 주소 값으로 MAC 주소 값을 설정하기 때문에 하나의 랜카드에 부여되는 MAC 주소 값은 유일한 값으로 네트워크상에서 네트워크 기기를 식별하는데 사용되기도 한다.

무선랜에서 사용하는 랜카드도 유선 네트워크에서 사용하는 랜카드와 마찬가지로 유일한 값의 MAC 주소를 부여 받는다. 이 값을 이용하여 무선랜 장비인 단말기와 AP를 인증하는데 사용하기도 한다. 대부분 인증절차는 접속을 허용하는 사용자의 단말기가 사용하는 랜카드의 MAC 주소를 사전에 등록하여 놓고, 접속을 요청하는 단말기의 MAC 주소가 사전에 등록한 리스트에 존재하는지의 여부를 이용하여 인증을 하는 것을 말한다. 이러한 방법을 MAC 주소 필터링이라 부르기도 한다. 복잡한 사용자 인증 메커니즘을 적용하는 것이 아니고 단순히 사용하는 랜카드의 주소 값으로만 접속을 허용할 것이지 아닌지 여부를 결정하기 때문에 대부분 접근제한 방법에 적용되기도 한다.

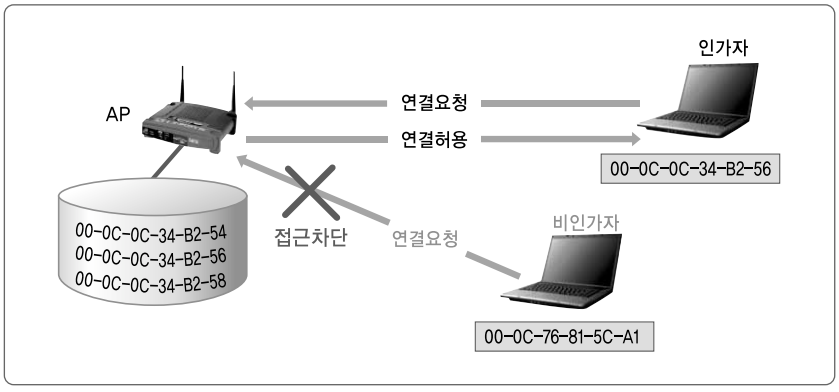
MAC 주소 필터링은 공격의 위험을 줄이는 간단한 방법이면서 네트워크 규모에 상관없이 적용할 수 있는 보안기술로 알려져 있다. 설정 방법 또한 간단하고, 기본적인 공격을 방어하는데 효과적인 방법으로 알려져 있다. MAC 필터링은 무선 네트워크로 진입하는 스위치나 AP 자체에서 설정하여 적용할 수 있다. 현재 나와 있는 많은 종류의 AP에서 지원하는 보안기능이다.

나. MAC 주소인증의 적용방법

(1) AP에 적용하는 경우

아래 〈그림 22〉 은 AP에 MAC 주소인증 기능을 적용한 경우를 나타내고 있다.

무선랜 관리자가 사전에 무선랜 서비스에 접속 가능한 사용자들이 갖고 있는 단말기의 무선랜 카드에 부여된 MAC 주소 값을 조사하여 그 값을 AP에 저장하고, 연결을 요청하는 사용자가 있을 경우에 AP에 저장된 MAC 주소 값과 비교하여 같은 값이 존재하면 연결을 요청한 사용자가 정당한 접속 권한을 갖는 사용자로 간주하여 접속을 허용하고, 그렇지 않는 경우에는 접속을 차단하는 방식이다. 이러한 방식을 제공하기 위해서 AP에 허용하는 사용자들의 MAC 주소에 관한 데이터베이스를 구성하여 관리하여야 한다. 경우에 따라 AP의 저장 능력의 한계로 새로운 사용자 추가에 대한 MAC 주소 추가가 불가한 경우도 발생할 수 있다.



[그림 22] AP를 이용한 MAC 주소 인증 적용방법

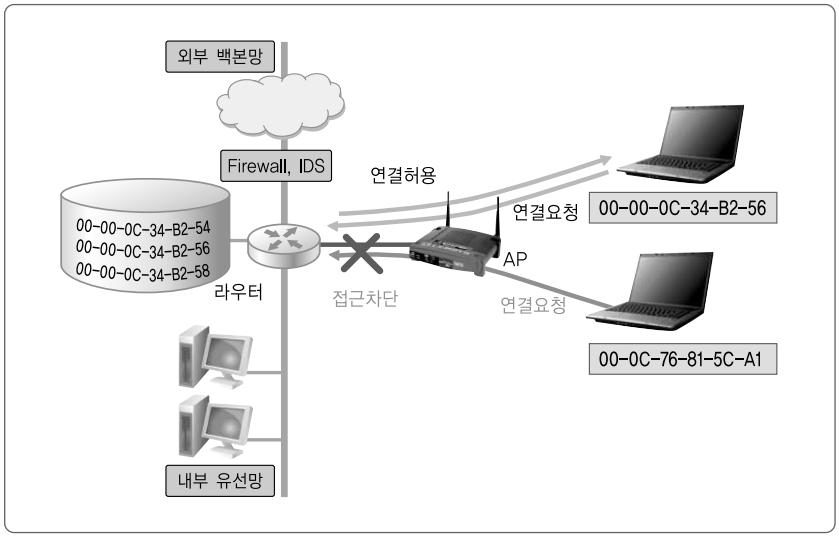
(2) 라우터에 적용하는 경우

아래 〈그림 23〉은 네트워크 장비인 라우터에 MAC 주소인증 기능을 적용한 예이다.

MAC 주소인증 방식을 무선랜 장비인 AP에 적용하는 것이 아니라, 무선랜과 유선 네트워크와의 연결점이 되는 네트워크 장비에 적용하는 것을 말한다. 즉, 유선 네트워크에서 사용하는 장비인 라우터나 스위치 등에 MAC 주소인증 기능을 적용하는 것이다. 이러한 적용방법은 네트워크 장비인 라우터나 스위치에 부하를 가중시킬 수 있다. 즉, 네트워크 장비가 MAC 주소인증 기능을 수행함으로 인해, 네트워크 장비의 고유의 기능인 경로설정과 데이터 전송의 속도가 저하되는 경우

가 발생할 수 있다. 이러한 단점으로 인해 실제로는 네트워크 장비인 라우터나 스위치 등에 MAC 주소인증 기능을 적용하는 예는 그리 많지 않다.

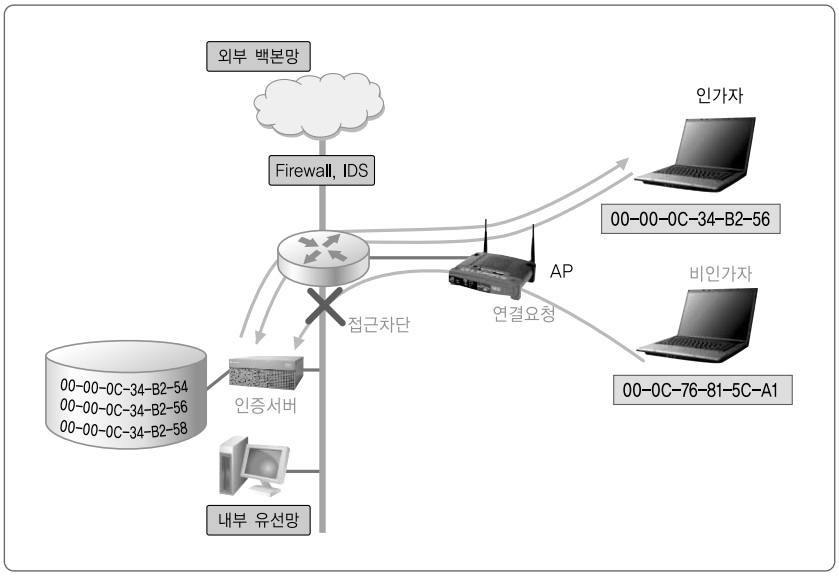
[그림 23] 라우터를 이용한 MAC 주소인증 적용방법



(3) 인증서버에 적용하는 경우

무선랜에서 MAC 주소인증을 적용하는 또 다른 방법은 인증 서버를 이용하는 방법이 있다. 아래 〈그림 24〉은 인증 서버를 이용하여 MAC 주소인증을 적용한 예를 나타내고 있다.

인증 서버를 이용하여 MAC 주소 인증을 적용하면, AP를 이용할 때 발생하는 불편함인 메모리 한계로 인한 MAC 주소 정보 저장의 한계를 극복할 수 있고, 각 AP 마다 유지 관리해야했던 MAC 주소 정보를 인증서버 한 곳에서만 관리해도 됨으로 관리자의 업무 부담을 줄 일 수 있다. 이 방식을 적용하려면 무선랜 환경에 인증 서버를 구축하여 운영해야 함으로 비용이 증가하는 단점이 있다. 하지만, 동적 WEP의 적용이라던가, IEEE 802.1x 표준에서 정의한 보안기능인 EAP 인증기능 등을 사용하려면, 인증 서버가 필요하게 됨으로 인증 서버를 이용한 다양한 보안기능을 추가로 활용할 수 있게 된다.



[그림 24] 인증 서버를 이용한 MAC 주소인증 적용방법

다. MAC 주소 인증의 장점과 단점

앞에서 설명한 방법으로 MAC 주소인증을 적용하기 위해서는, 우선 무선랜 환경에 접속을 허용하는 사용자들의 MAC 주소 인증을 수행하는 장비에 미리 추가하여 설정하여야 한다. 하지만, MAC 주소 인증을 수행하는 장비관리 소홀과 해킹 등의 이유로 장비에 저장되어 있는 MAC 주소정보가 외부로 노출될 수 있다. MAC 주소가 외부로 노출되면, 공격자가 노출된 MAC 주소를 악용하여 무선랜을 통한 침해행위를 발생 시킬 수 있음으로 MAC 주소 정보 관리에 주의하여야한다. 물론, 무선랜 사용자도 자신이 사용하는 무선랜 카드를 분실한다거나, MAC 주소 정보를 다른 사람들에게 알려주는 등, 자신의 MAC 주소가 외부에 노출되는 것을 막기 위해 주의를 기울여야한다.

MAC 주소인증은 무선랜 서비스를 미리 정해진 인가된 사용자에게만 접근할 수 있도록 제공하고 있다. 즉, 간단한 보안설정으로 미리 정해진 사용자에게만 MAC 주소 인증을 통한 접근을 허용하려는 접근제어를 수행하는 것이다. 하지만, 무선랜 장비가 많은 대규모 기관에서는 사용자의 MAC 주소를 관리하기 위한 관리자의 업무가 무척이나 많아진다. 앞에서도 언급한바 있듯이 MAC 주소정보를

사전에 등록하기 위해서는 많은 메모리를 요구하나, 네트워크 장비(AP,라우터, 스위치, 인증서버 등)의 메모리에는 한계가 있어, 많은 수의 MAC 주소를 등록하지 못하는 경우가 발생하게 된다. 이러한 경우에 정당한 사용 권한이 있는 사용자의 접속이 이루어지지 못할 수가 있음으로 MAC 주소인증 방식의 적용을 위해서는 장비마다 적절한 접속 인원을 할당해서 적용해야한다.

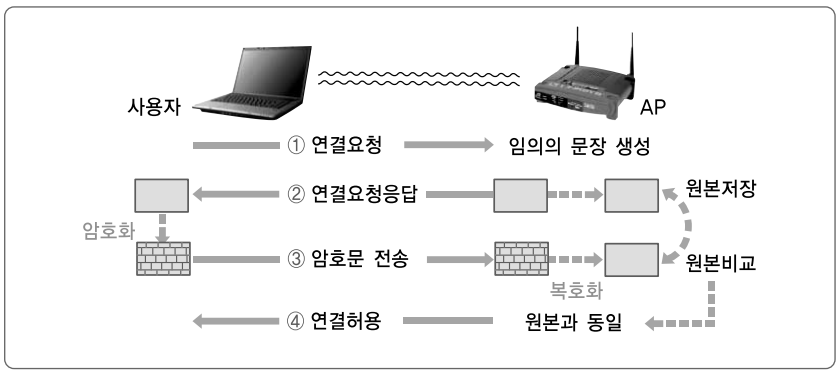
3. WEP 인증 메커니즘

WEP은 앞에서 설명한 것과 같이 유선과 동등한 프라이버시를 제공한다는 목적에서 개발되었고, 데이터 암호화와 사용자 인증, 두 가지 기능을 모두 제공한다. 여기에서는 인증의 측면에서 WEP의 특성을 알아본다. WEP에서 제공하는 사용자 인증은 간단히 설명하면, 서로 같은 공유키를 갖는 사용자들을 정상적인 사용자로 인증하여 통신하는 방법을 제공한다. 이제 WEP 인증 절차와 WEP 인증이 갖는 보안상의 특성을 알아본다.

가. WEP 인증절차

아래 〈그림 25〉은 무선랜 장비인 AP와 사용자간의 WEP 인증을 수행하는 절차를 나타내고 있다.

[그림 25]
WEP 인증절차



앞에서 설명한 것과 같이 WEP의 암호화 방식을 이용하여, 위의 〈그림 25〉과

같이 4가지 절차를 거쳐서 AP와 사용자간의 인증을 수행한다.

① 사용자가 이용하고자 하는 무선랜 서비스의 SSID값을 알아내어, 무선랜 AP에 연결요청 메시지를 전송한다.
② 사용자의 연결요청을 메시지를 받은 AP는 임의의 문장을 생성 원본을 저장하고, 연결요청응답메시지를 이용하여 암호화되지 않은 사본을 전송한다.
③ 연결요청 응답 메시지를 받은 사용자는 AP가 보내온 임의의 문장을, 자신이 갖고 있는 공유키를 이용하여 WEP 암호화를 적용하여 암호문으로 만든다. 완성된 암호문을 AP에 전송한다.
④ 사용자가 자신의 공유키인 WEP키로 만든 암호문을 전송 받은 AP는 AP가 갖고 있는 공유키를 이용하여 암호문을 복호한다. 복호화된 문장과 자신이 저장하고 있던 원본의 문장을 비교하여 같으면, 사용자가 자신과 같은 공유키를 갖는 그룹원임을 인식하고, 연결 허용 메시지를 전송한다. 이러한 방식을 통하여 사용자와 AP가 같은 WEP 키값을 가지고 있다는 것을 인식하게 되고, 같은 키 값을 갖는 사용자들을 정당한 사용자로 인식하여, 무선랜 서비스를 제공한다.

나. WEP 인증 메커니즘의 취약성

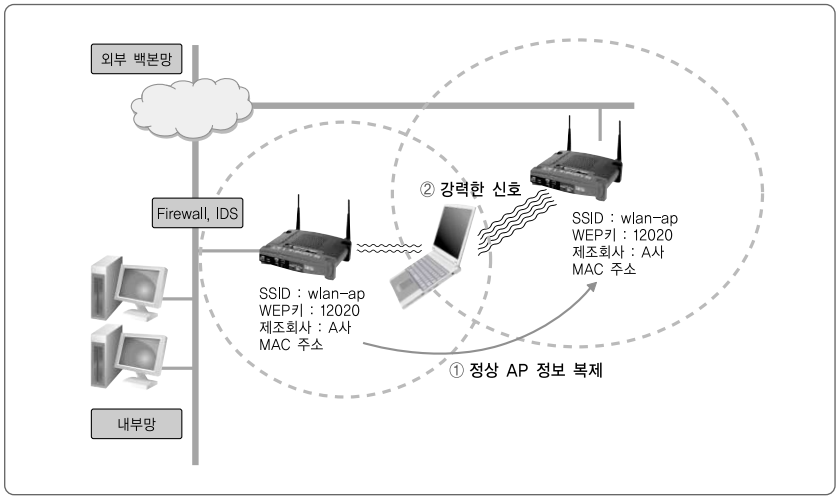
WEP을 이용한 인증 방식은 공유키인 WEP 키를 이용하여 사용자를 인증하는 방식으로 공유키 값을 모르는 사용자는 무선랜 서비스를 이용할 수가 없다. WEP 인증을 적용하는 방식은 아주 간단하다. 우선, AP를 이용한 WEP 인증은 AP와 사용자의 단말기에 같은 값의 WEP키를 설정하여 사용하면 된다. 인증 서버를 이용하여 WEP을 적용할 경우도 마찬가지다. WEP을 이용한 인증은 데이터 암호화와 함께 적용되기 때문에 편리하다. WEP을 적용하여 사용하기만 하면, 사용자 인증과 데이터 암호를 모두 적용할 수 있기 때문이다. 뿐만 아니라, 무선랜 장비에서 WEP을 구현하는 것도 무척이나 간단하고, 인증 절차 또한 간결하여 사용자에게 무척이나 많은 편의를 제공한다.

하지만, WEP을 이용한 사용자 인증은 몇 가지 문제점을 갖고 있다. WEP이 갖는 문제점에 대해서 자세히 알아보기로 한다.

(1) 단방향 인증방식 제공으로 인한 취약성

WEP을 이용한 인증 방식은 앞에서도 알 수 있듯이, AP에서 사용자를 인증하는 단방향 인증 메커니즘을 제공하고 있다. 이러한 단방향 인증 방식은 인증방식이 안전하지 못하여 악의적은 목적으로 운영되는 복제 AP(clone AP : 악의적인 목적으로 정상 AP와 똑같은 설정을 갖도록 복제하여 구성한 AP)로 인한 피해가 발생하게 된다. 아래 〈그림 26〉는 복제 AP로 인해 정상사용자가 접속을 잘 못하여, 피해가 발생하는 경우를 나타내고 있다.

[그림 26] 복제 AP로 인한 피해발생

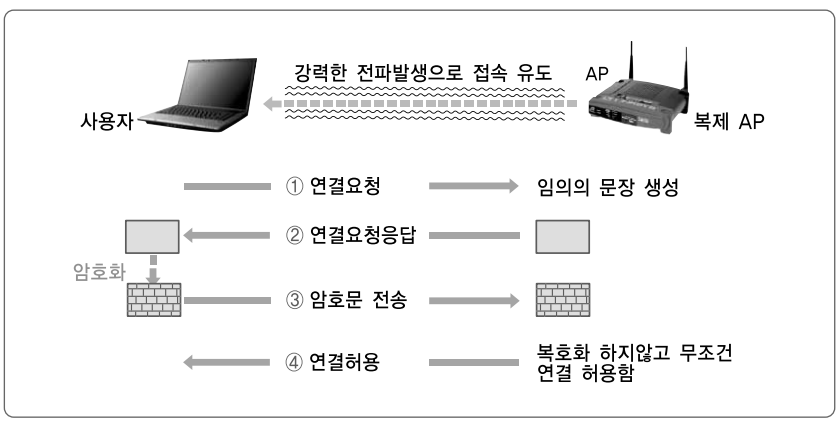


복제 AP를 이용하여 피해는 다음과 같은 절차로 발생하게 된다.

① 공격자가 정상적인 무선랜 환경에서 서비스를 제공하는 AP의 정보를 수집하여 같은 제조회사의 같은 모델을 이용해 정상 AP와 똑같은 설정을 갖는 AP를 복제하여 구성한다.
② 기관 내부에서 무선랜 서비스를 이용하는 사용자나 무선랜에 접속하고자 하

는 사용자는 정상 AP보다 더욱 강력한 전파를 송신하는 복제 AP를 정상 AP로 오인하게 된다. 정상 사용자는 아무런 의심 없이 복제 AP에 접속을 요구하는 메시지를 보내게 되고, 복제 AP는 응답 메시지를 통하여 거짓 인증요구를 한다. 사용자은 복제 AP에 자신의 인증정보를 보내게 되고, 복제 AP는 사용자의 인증정보와는 무관하게 무조건 접속을 허용한다. 이제 정상 사용자는 복제 AP를 이용하여 인터넷 서비스를 사용하게 되며, 이때 복제 AP를 이용한 공격자는 정상 사용자가 이용하는 인터넷 패킷의 정보를 수집하여 개인정보나 금융정보 등을 알아낸다.

이때 만일 정상 AP와 사용자 사이에 WEP 인증을 수행한다면, 정상 AP를 복제한 복제 AP에서도 WEP 인증을 설정하여 수행함으로써, 정상 사용자의 연결을 아무런 의심 없이 처리할 수 있다. 아래 〈그림 27〉은 복제 AP를 이용하여 정상사용자의 접속을 유도하여 WEP 인증 메커니즘을 통과하는 과정을 나타내고 있다.



[그림 27]
복제 AP를
통한 WEP
인증 회피공격

① 복제 AP가 강력한 전파를 발생하여 정상사용자의 접근을 유도한다. 정상 사용자는 양질의 전파가 들어오는 AP가 자신이 사용하고자하는 정상 AP로 인식하고, 연결요청 메시지를 보내게 된다.

② 복제 AP는 정상 사용자가 복제 AP임을 알아채지 못하도록 WEP 인증을 수

행한다. 즉, 임의의 문장을 생성하여 정상 사용자에게 연결요청 응답메시지로 전송한다.

③ 정상 사용자는 자신이 갖고 있는 WEP 키를 이용하여 암호문을 만들어 복제 AP에 전송한다.

④ 복제 AP에서는 WEP키를 모르므로 무조건 연결 허용 메시지를 보내어, 정상 사용자의 접속을 유도한다.

이러한 방식으로 복제 AP를 통한 정상 사용자의 무선랜 연결 설정이 완료되면, 정상 사용자가 송수신하는 패킷을 모니터링 하여, 공격에 필요한 정보를 수집한다.

위와 같은 공격이 가능하게 되는 이유는, 무선랜 서비스 사용자가 무선랜 서비스를 제공하는 AP에 대한 인증을 하지 않았기 때문이다. 다만, AP에게 자신이 WEP키를 갖고 있으며, WEP 메커니즘에 의해 생성된 암호문을 전송함으로써, 자신의 접속이 합법적으로 이루어지고 있다는 것을 간접적으로 알리기만 할 뿐, 자신의 접속여부를 결정하는 AP가 정상적으로 기관에서 설치하여 운영되고 있는 AP인지, 복제되어 공격에 이용되고 있는 AP인지의 여부를 체크하지 않고 있기 때문이다. 이러한 취약점은 단방향 인증 메커니즘을 이용하여 발생하는 것으로, 사용자도 AP가 자신이 접속하고자하는 기관에서 운영되고 있는 AP인지 여부를 확인할 필요가 있다. 즉, WEP은 단방향 인증이므로 비인가 AP, 복제 AP 등에 의한 피해가 발생할 수 있음으로 WEP을 사용하는 기관의 사용자는 무선랜 서비스 이용할 때 항상 조심하여야 한다.

(2) 고정된 공유키 사용으로 인한 취약성

WEP이 갖는 또 하나의 취약점은 무선랜을 사용하는 기관에서 WEP 키 값을 하나의 고정된 공유키를 사용하는 것이다. 무선랜을 사용하는 모든 장비, 즉 AP와 사용자 단말기 등에 동일한 키 값을 설정하여 사용해야 하고, 같은 값을 갖는 키의 사용으로 인해, WEP 키 값이 외부로 유출될 경우에 많은 보안 문제를 일으킬 수 있다.

우선, 무선랜을 사용하는 기관에서 하나의 고정키 값을 설정하여 사용하게 되면, 협력업체 직원, 방문객, 퇴사자 등에 의해서 WEP 값이 외부로 유출될 수 있다. 이러한 위험요소를 줄이기 위해서 WEP 값을 주기적으로 변경하여야 한다. 하지만, 고정된 WEP 키를 변경하는 것은 그리 쉬운 일은 아니다. 기관에서 사용하는 무선랜 장비가 많을 경우에는 더욱 그러하다. 예를 들어 A 기관에서 사용하는 무선랜 장비인 AP가 20대이고, 무선랜 사용자가 100명이라면, 동시에 20대의 AP의 WEP키를 변경하여야 하고, 무선랜 사용자에게 변경된 WEP를 알려주어 변경된 WEP 키값으로 자신의 단말기를 설정하여 무선랜 서비스를 사용할 수 있도록 제공하여야 한다. 하지만, 무선랜을 사용하는 기관의 사용자 대부분은 외근을 하는 경우가 많아 변경된 WEP를 알려주는데 어려움이 발생하기 마련이다.

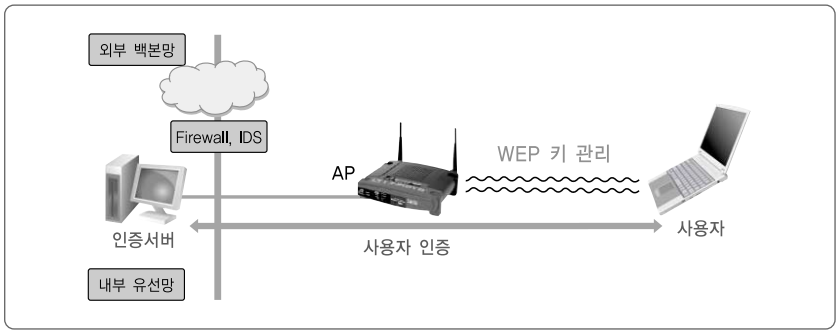
무선랜을 사용하는 기관은 하나의 WEP키를 이용하여 사용자 인증을 수행하기 때문에 WEP키가 외부로 유출될 경우에는 공격자가 습득한 WEP키를 이용하여 접속을 시도하므로 매우 위험하다. 이러한 위험을 줄이기 위해서도, 협력업체 직원이나 방문객에게 WEP키를 알려주었다면, WEP키를 변경하는 일이 꼭 필요하다.

다. 동적 WEP 적용

앞에서 설명한 대로 WEP을 적용하면, 고정된 공유키 값을 사용하게 되어 보안상 여러 가지 문제점이 발생하게 마련이다. 이러한 문제점을 줄이기 위해서 동적 WEP을 적용하여야 한다. 아래 〈그림 28〉은 무선랜 환경에 인증 서버를 적용한 예를 보이고 있다. 아래 〈그림 28〉에서도 알 수 있듯이, 인증서버가 사용자가 접속을 시도할 경우에 인증을 수행하고, 기관에서 사용하는 WEP 키의 설정과 갱신 등의 관리를 수행한다.

동적 WEP을 사용하려면, 우선 인증 서버를 설치 운영하여야 한다. 또한, 현재 사용하고 있는 AP가 동적 WEP을 지원할 수 있는지 여부를 확인해야 한다. AP에서 802.1x 프로토콜을 지원하는 경우에는 동적 WEP을 사용할 수 있다. 뿐만 아니라, 동적 WEP의 사용으로 인해, 사용자 인증과 키 갱신 등을 위한 패킷의 전

[그림 28] 인증 서버를 이용한 동적 WEP 적용

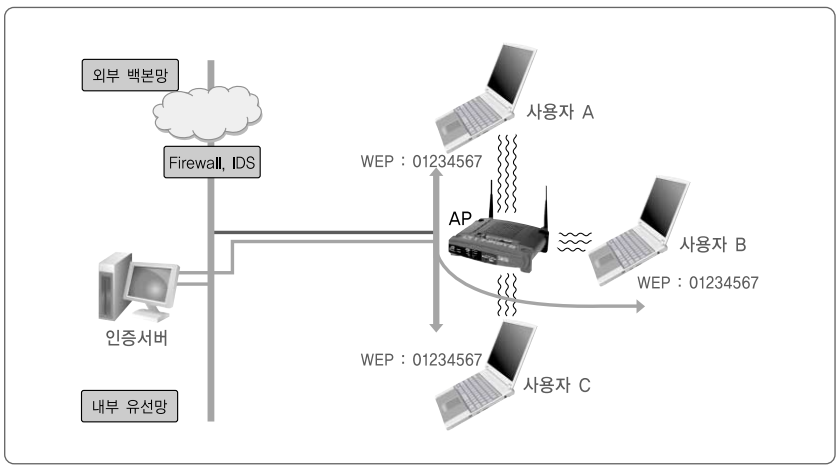


송이 생기게 되므로 AP가 사용자에게 제공하던 데이터 전송률이 낮아지게 되는 경우가 발생하게 된다. 예를 들어, 동적 WEP을 적용하기 전에는 AP가 사용자 30명의 데이터를 원활히 송수신 할 수 있었으나, 이제 동적 WEP을 적용하고 난 후부터는 사용자 30명의 데이터를 빠르고 원활하게 송수신 할 수 없게 된다. 뿐만 아니라, 인증과 키 갱신을 위한 관리 패킷의 증가로 인해 사용자 30명의 연결을 허용하지 못하고 25명 정도만 연결을 허용하는 경우가 발생하기도 한다. 이러한 관리 패킷에 의한 AP의 트래픽 증가로 인해, 무선랜 서비스 제공이 원활하지 못하여, AP를 추가 설치해야 하는 경우도 발생하기도 한다.

동적 WEP은 아래 〈그림 29〉과 같이 연결을 요청하는 사용자별로 WEP 키를 부여한다.

위 〈그림 29〉에서 사용자 A가 연결요청을 하면, 인증 서버가 인증 과정을 수행

[그림 29] 동적 WEP을 적용하여 연결을 설정한 예제



하고 사용자 A에게 WEP 키값을 부여한다. 사용자 B가 연결을 요청하여도 마찬가지로 인증 과정을 수행하여 WEP 키값을 부여한다. 즉, 하나의 연결마다 WEP 키값을 새로 부여하는 것이다. 이렇게 하나의 연결마다 새로운 WEP 키값을 부여하면, WEP 키값의 외부 유출시 피해가 적어지게 된다. 뿐만 아니라, 인증서버는 무선랜 서비스를 이용하는 사용자의 연결에 대한 시간 정보를 관리하여 일정시간 동안 지속적으로 무선랜을 사용하는 사용자의 연결에 대해서는 WEP 키값을 갱신하도록 하고 있다. 이러한 WEP 키값의 갱신은 공격자가 연결 정보를 수집하여 WEP 키값을 크랙하려는 공격을 방지하는데 효과적이다. 공격자가 WEP 키값을 알아내기 위해서 정상 사용자의 무선랜 패킷을 수집하여 분석하는 동안에, 인증서버가 WEP 키값을 갱신하면, 공격자가 정상 사용자의 패킷을 수집하여 WEP 키를 크랙하기 위한 노력을 무력화 시킬 수 있다.

결국, 동적 WEP의 적용은 인증서버의 설치 운영으로 인한 비용증가와 사용자 인증 정보를 전송하기 위한 관리 패킷의 증가로 인해 AP의 사용자 데이터 전송률이 저하되는 경우가 발생하기도 하지만 정적 WEP이 갖는 사용자 인증과 키 관리에 관한 취약성을 효과적으로 줄일 수 있어, 보안성이 향상된다.

4. EAP 인증 메커니즘

WEP을 이용한 인증은 단방향 인증이고, 고정된 공유키 값을 사용하여 인증시 여러 가지 문제점이 있었다. 이러한 WEP 인증의 문제점을 보완하고자 802.1x 표준안에서는 동적 WEP을 제공하였다. 동적 WEP은 인증 서버를 이용하여 사용자 인증과 키 관리를 지원하는 것이다. 하지만, 동적 WEP의 적용도 WEP이 갖던 단방향 인증으로 인한 문제점을 없애지 못 하였고, 인증 서버를 이용하여 연결된 세션의 WEP 키 값을 갱신하도록 설정할 수는 있지만 공격자가 사용자의 패킷을 수집하여 WEP 키를 크랙 하는 공격 자체를 막지는 못하고 있다.

이러한 인증상의 문제점을 해결하고자 802.1x 표준에서는 EAP 인증 기능을 제공하고 있다. 여기에서는 EAP 인증기능에 대해서 알아보고, EAP 인증이 갖는

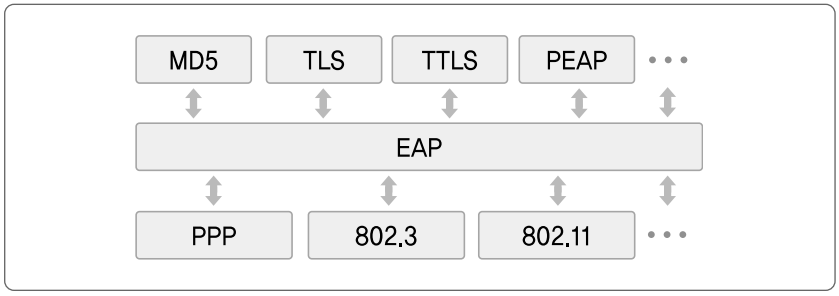
취약성에 대해서도 분석하여 보기로 한다.

가. EAP 개요 및 인증 절차

확장 인증 프로토콜인 EAP는 RFC 2284에 공식적인 명세가 발표되었으며, 초기에는 PPP(point to point protocol)에서의 사용을 위해서 개발되었으나, 현재는 무선랜 표준인 IEEE 802.1x에서 사용자 인증 방법으로 사용되어지고 있다.

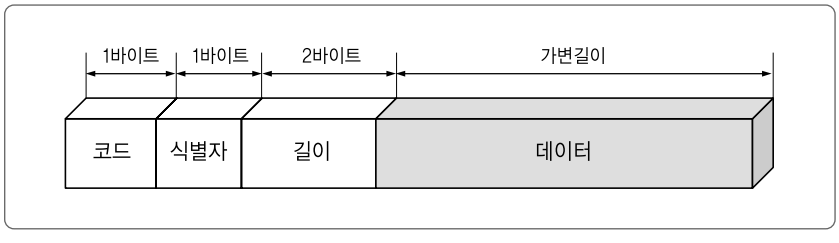
EAP는 어떤 링크에도 접속이 가능한 단순한 캡슐화 개념의 프로토콜이다. 아래 〈그림 30〉는 EAP의 기본 구조를 나타내고 있다. EAP는 모든 링크에 적용될 수 있으며, 다양한 인증 방법을 사용할 수 있도록 설계되었다.

[그림 30] EAP 기본구조



즉, EAP 프로토콜은 위의 〈그림 30〉과 같이, 링크계층 위에서 다양한 종류의 인증 방법을 전송하는 역할을 한다. 이러한 역할을 하기 위한 EAP 프로토콜의 패킷구조는 아래 〈그림 31〉와 같다.

[그림 31] EAP 패킷구조

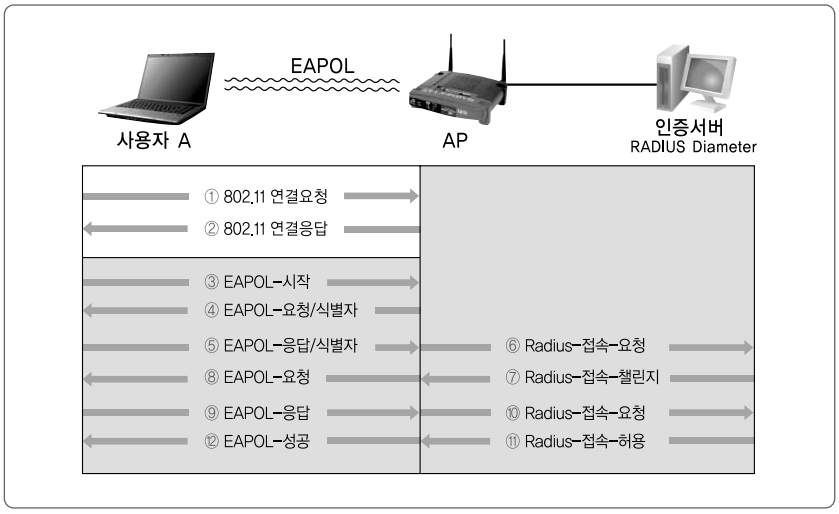


EAP 패킷의 각 필드가 나타내는 정보는 다음과 같다.

- 코 드 : EAP 패킷의 유형을 식별하는데 사용되는 정보
- 식별자 : 요청에 대한 응답을 확인하고자 사용되는 무부호 정수(unsigned integer)이다. 재전송은 동일한 식별자를 이용하고, 새로운 전송은 새 식별자를 사용한다.
- 길 이 : 코드, 식별자, 길이 및 데이터 필드를 포함한 전체 패킷의 길이 정보를 나타낸다.
- 데이터 : 실제로 전송하고자 하는 정보

EAP는 다양한 인증 방법을 제공하기 위해서 코드 필드에서 사용하는 인증 방법을 구분하고, 데이터 영역은 가변 길이로 정의되어 있다.

EAP 프로토콜을 이용하여 무선랜 사용자와 AP, 인증 서버간의 인증을 수행하는 절차는 아래 〈그림 32〉와 같다.



[그림 32] EAP 인증 절차

사용자와 AP 사이에는 EAPOL(EAP over LAN)프로토콜을 통해서 패킷을 전송하고, AP와 인증서버 사이에는 RADIUS(Remote Authentication Dial-in User Services) 프로토콜을 통해서 패킷을 전송한다. 일부에서는 AP와 인증서버 사이의 프로토콜을 RADIUS over LAN이라고 설명하기도 한다. 802.1x에 적용되는 EAP는 자체로써 완전한 실제 인증 메커니즘은 아니다. 실제 인증 방법은 인증서버에 의해서 구현된다. 즉, 802.1x 표준에서 제공하는 EAP는 단순히 연결

을 요구하고, 챌린지를 발부하고 접근을 승인하거나 거부하는 기능을 하고, 실제로 사용하는 인증서(보증서)에 대한 판단은 하지 않는다. 이러한 판단은 인증서버가 수행하게 된다.

EAP를 이용하여 무선랜 연결을 설정하는 절차를 각 단계별로 구체적으로 살펴보면 다음과 같다.

① 무선랜 클라이언트인 사용자 A가 AP에 네트워크 접속을 요구한다.
② AP는 자신이 속해 있는 네트워크에 클라이언트인 사용자 A가 연결을 설정할 때까지 다른 사용자로부터의 네트워크 연결시도를 차단하고, 사용자 A에게 연결 요청에 대한 응답 메시지를 보낸다.
③ 클라이언트인 사용자 A는 AP가 보낸 응답 메시지를 받고 난후에 EAPOL-시작 메시지를 AP에 보내어 RADIUS를 이용한 연결설정을 시작할 것을 알린다. 여기서부터가 EAP를 이용한 사용자 인증 방법의 시작이라고 볼 수 있다.
④ AP는 사용자 A가 보내온 EAPOL-시작 메시지를 받은 후에, EAP-요청 메시지를 사용자 A에게 전송하여, AP 식별자를 보내면서, 사용자 A의 정보를 요구한다.
⑤ 사용자 A는 네트워크에 로그온하기 위해 사용자명과 암호를 입력창을 통하여 입력하여, 사용자 인증을 위한 정보를 AP에 보낸다.
⑥ AP는 사용자에게서 받은 정보를 이용하여 RADIUS서버에 접속요청 메시지를 보내어 상호인증을 요구한다.
⑦ RADIUS서버는 AP에게 사용자 A로 전송할 사용자 인증 챌린지(Challenge) 메시지를 보낸다.
⑧ AP는 RADIUS서버에서 보낸 사용자 인증 챌린지를 사용자 A에게 전송한다.
⑨ 사용자 A는 챌린지에 대한 응답으로서 사용자명과 암호를 단방향(One-way)의 해쉬(HASH)를 사용하여 EAP 응답 메시지를 구성하여 AP에 전송한다.

⑩ AP는 사용자 A에게 받은 정보를 이용하여 RADIUS서버에 Radius-접속요청 메시지를 보낸다.

⑪ 사용자 관리 DB 정보를 사용하여 RADIUS서버는 자신이 보낸 챌린지에 대한 대응 메시지를 생성하여, 사용자 A가 보내온 응답메시지의 값과 비교하여 사용자 A를 인증한다. 이 과정을 역으로 수행하여 사용자 A가 RADIUS서버를 인증하여 사용자 A와의 상호인증을 수행하기도 한다.

⑫ 사용자 A와 RADIUS서버의 상호인증이 성공적으로 완료되면 네트워크 접근을 위한 적당한 사용자의 수준을 정의하고 사용자 A를 구별할 수 있는 WEP키를 결정하여 부여한다.

이제까지는 EAP 프로토콜에 기본적인 동작 원리에 대하여 알아보았다. 앞으로는 EAP를 이용하여 사용자 인증을 수행하는 인증 프로토콜에 대해서 알아보기로 하자. EAP를 이용한 사용자 인증 방법은 EAP-MD5, EAP-TLS, EAP-TTLS, PEAP 등이 있다. 이들에 관하여 좀 더 살펴보자.

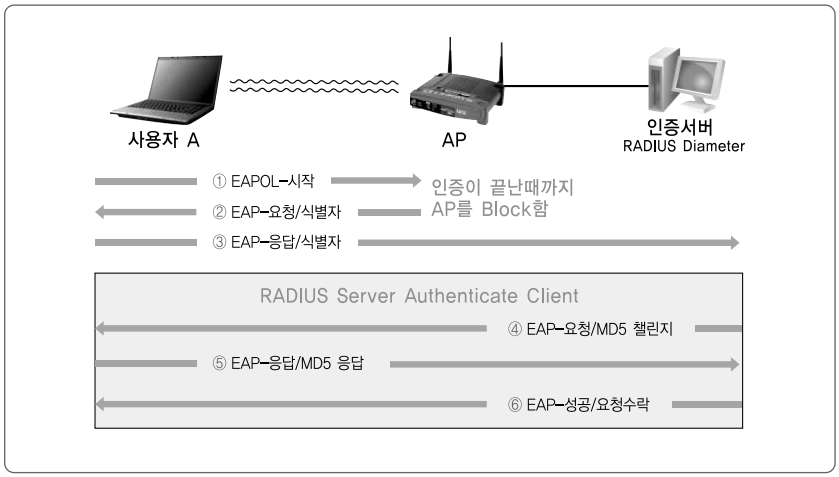
나. EAP-MD5 인증

EAP-MD5 인증은 단방향 인증 방법으로 무선랜 사용자의 패스워드를 기반으로 하는 네트워크 인증 방식이다. 이것은 802.1x 유선 이더넷 스위치에 구현되는 방식으로, 무선랜에서 보안 방식으로도 사용되고 있다. 아래 〈그림 33〉은 EAP-MD5 인증절차를 나타내고 있다. 기본적인 인증 절차는 앞에서 설명한 EAP 인증 절차를 따른다. 즉, 무선랜 클라이언트가 AP에 네트워크 접속을 요구하고, AP는 인증이 수행되어 연결이 설정될 때까지 AP를 차단하는 것까지는 앞에서 설명한 방식대로 수행된다.

① 사용자 A는 AP에 EAP로 연결 설정을 하기 위한 EAPOL-시작 메시지를 보낸다.

② AP가 사용자 A의 EAPOL-시작 메시지를 받고, EAP-요청 메시지와 AP

[그림 33]
MD5 인증절차



식별자를 사용자 A에게 보낸다. 이때 연결 설정을 위한 사용자 정보를 요구한다.

③ 사용자 A는 무선랜 인증을 위한 자신의 식별자를 AP를 이용하여 인증서버에 전송한다.

④ 인증서버는 사용자 A에게 챌린지 메시지를 보내어 사용자 A가 정상적으로 무선랜 서비스에 접속 가능한 사용자인지를 묻는다.

⑤ 사용자 A는 인증서버에서 보내온 챌린지에 맞는 응답 메시지를 인증서버에 전송한다.

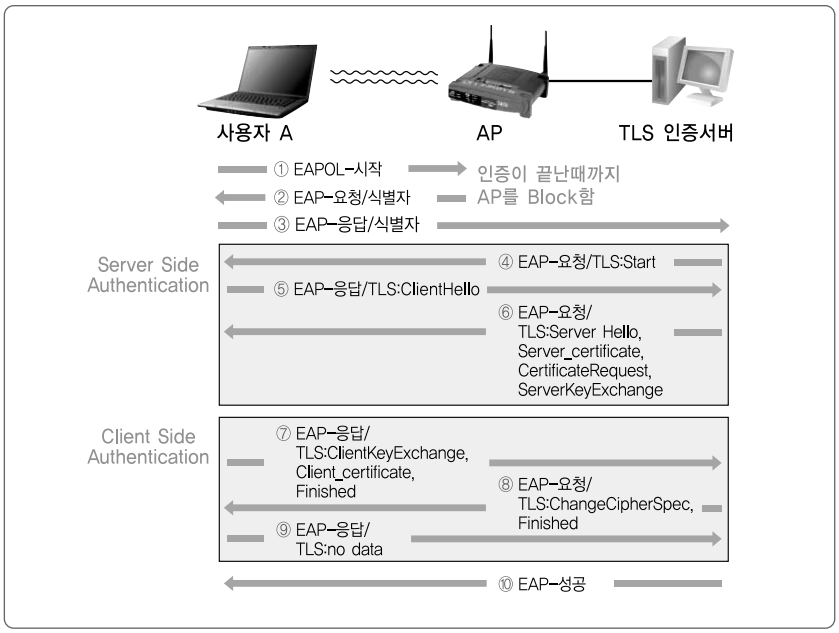
⑥ 인증서버는 자신이 전송한 챌린지에 합당하는 응답이 왔는지 확인한다. 응답 메시지가 정당하다면, 접속을 허용하는 메시지를 사용자 A에게 보낸다.

위의 인증 절차에서도 알 수 있듯이, EAP-MD5 인증은 인증 절차가 간편하여, 사용자 단말기에서 무리 없이 인증절차를 수행할 수 있다. 이로 인해 인증시 소요되는 시간이 매우 짧게 된다. 하지만, EAP-MD5 인증은 인증서버에서만 접속을 요구하는 사용자를 인증하는 단방향인증이다. 이러한 단방향 인증은 WEP 인증의 취약성에서도 설명한 바 있는 복제 AP에 의한 공격 등에 매우 취약하다. 뿐만 아니라 EAP-MD5 인증은 동적 WEP을 지원하지 않아, 사용자 식별자와

패스워드 기반의 간편한 인증 메커니즘을 제공하기는 하지만, 무선 데이터를 위한 암호화를 지원하지 않아 앞으로 설명할 다른 EAP 인증 방식보다 보안에 취약하다.

다. EAP-TLS 인증

EAP-TLS는 가장 일반적인 인증서 기반의 인증 방식이다. 이 방식은 무선랜 AP가 EAP-TLS를 지원해야 한다. 이 방식은 2001년 말에 마이크로소프트의 윈도우 XP가 소개되면서 본격적으로 사용되고 있다. 아래 〈그림 34〉은 EAP-TLS 인증 절차를 나타내고 있다.



[그림 34] EAP-TLS 인증절차

① ~ ③ EAP-MD5의 인증 절차와 동일하다.

④ 인증서버는 사용자 A에게 TLS 시작 메시지를 보내어 사용자 A가 EAP-TLS 인증을 시작할 것을 알린다.

⑤ 사용자 A는 인증서버에게 Client Hello 메시지를 보내어 서버의 인증서를 보내 줄 것을 요구한다.

⑥ 인증서버는 사용자 A가 보내온 Hello 메시지를 받고, 인증 서버가 갖고 있는 인증서 정보를 보낸다. 이때, Server Hello 메시지를 사용자에게 보내어 사용자 A의 인증정보를 인증서버에게 보낼 것을 요구한다.

⑦ 사용자A는 서버가 보내온 인증 정보를 분석하여, 자신이 접속하고자 하는 네트워크가 정확한지 여부를 결정한다. 서버에 대한 인증이 끝나면, 서버가 보내온 Hello 메시지에 대한 응답으로 사용자 A는 자신의 인증 정보를 전송한다.

⑧ 인증서버는 사용자 A가 보내온 인증정보를 이용하여 접속을 허용해도 되는 사용자인지 여부를 결정한다. 사용자 A가 접속을 허용해도 되는 사용자일 경우에는 암호에 관한 정보를 전송한다.

⑨ 사용자는 이제 EAP-TLS 인증 절차가 성공적으로 이루어졌고, 인증서버에서 보내온 암호 정보를 잘 받았다는 응답 메시지를 보낸다.

⑩ 인증서버는 이제 EAP-TLS 인증 절차가 성공적으로 끝났음을 사용자 A에게 알리고, 접속을 허용함을 알린다.

앞에서 언급한 바와 같이 EAP-TLS 프로토콜은 인증서를 기반으로 하는 무선랜 사용자와 인증 서버간의 세션 키를 생성하는 상호 인증(양방향 인증)을 지원한다. 이것은 먼저 무선랜 사용자에게 키 분배를 요구한 다음, 인증서버에서 안전한 유선 연결을 통한 서버 인증서를 요구한다. 즉, 인증서버는 EAP-TLS를 이용한 인증을 지원함은 물론이고, 인증서도 관리해야 한다.

EAP-TLS 인증 적용의 장점은 최종 사용자의 신원을 확인하는 방법으로 디지털 인증서를 사용한다는 것이다. 여기서 인증서를 관리하고 운영하는 것이 부담스럽다고 생각할 수도 있을 것이나, 인증서를 사용하는 것이 패스워드를 사용하는 방식보다 보안상으로 더욱 안전하므로 패스워드 방식보다 많이 사용되고 있다.

디지털 인증서는 엔트루스(Entrus)와 베리사인(Verisign)같은 상용 CA (Certificate Authority) 서비스 업체를 이용하거나, 무선랜 운영 기관 자체에 CA서버를 구축하여 적용할 수 있다. 상용 CA 서비스 업체란 데이터의 무결성을 증명하

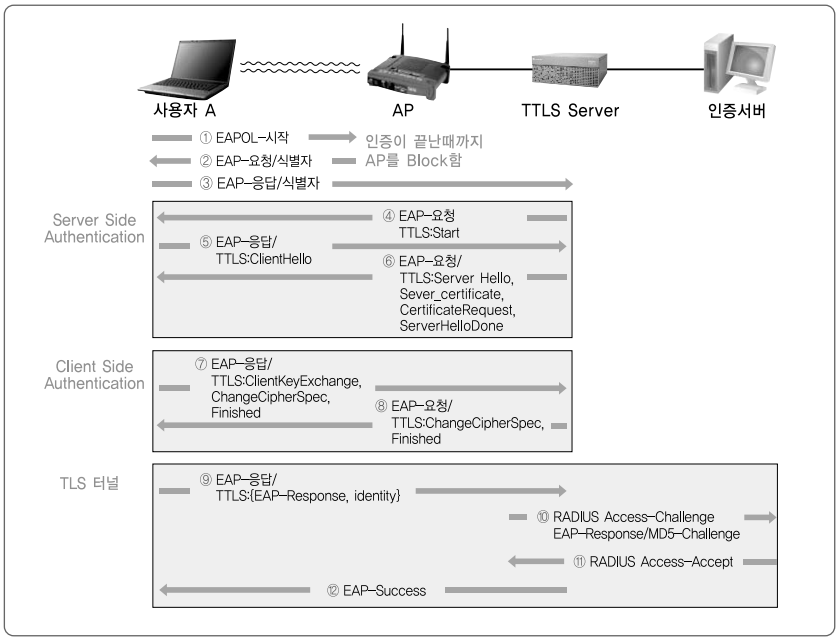
는 디지털 인증서 서비스를 하는 곳을 말한다.

EAP-TLS는 상호 인증(무선 클라이언트는 네트워크를, 네트워크는 무선 클라이언트를 인증)하는 사설 또는 공공키를 사용한다. 여기에서 사용되는 디지털 인증서는 버전, 인증서 시리얼 번호, 시그너처 알고리즘 식별자(signature algorithm identifier), 이름, 사용 기간, 공공키, 사인 값(signature value) 등의 정보를 갖는다.

라. EAP-TTLS 인증

EAP-TTLS는 EAP-TLS와 CHAP(Challenge Handshake Authentication Protocol) 또는 OTP(One Time Password) 등의 전통적인 암호 기반으로 하는 터널 방식의 인증 메커니즘이다.

아래 〈그림 35〉은 EAP-TTLS의 인증 절차를 나타내고 있다. 아래 그림에서도 알 수 있듯이, TLS 터널을 형성하기 위해서 인증서버 앞단에 TTLS 서버가 이용되고 있다. 하지만 실제로는 TTLS 서버를 별도로 운영하지 않고, 인증서버에서 TTLS 서버의 기능도 함께 수행하는 것이 일반적이다.



[그림 35] EAP-TTLS 인증절차

① ~ ③ EAP-MD5의 인증 절차와 동일하다.

④ TTLS 서버가 사용자 A에게 TTLS 시작 메시지를 보내어 사용자 A가 EAP-TTLS 인증을 시작할 것을 알린다.

⑤ 사용자 A는 인증서버에게 Client Hello 메시지를 보내어 TTLS 서버의 인증서를 보내 줄 것을 요구한다.

⑥ TTLS 서버는 사용자 A가 보내온 Hello 메시지를 받고, 사용자가 요구한 TTLS 서버의 인증서를 보낸다. 이때, Server Hello 메시지를 사용자에게 보내어 사용자의 인증 정보를 TTLS 서버에 보낼 것을 요구한다.

⑦ 사용자 A는 TTLS 서버가 보내온 인증 정보를 분석하여, 자신이 접속하고자하는 네트워크가 정확한지 여부를 결정한다. TTLS 서버에 대한 인증이 끝나면, TTLS 서버가 보내온 Hello 메시지에 대한 응답으로 자신의 인증 정보를 전송한다.

⑧ TTLS 서버는 사용자 A가 보내온 인증정보를 이용하여 접속을 허용해도 되는 사용자인지 여부를 결정한다. 접속을 허용하는 사용자일 경우에는 암호에 관한 정보를 전송하고, 사용자 A와 인증서버 사이에 TLS 터널을 형성한다.

⑨ 사용자 A는 이제 형성된 TLS 터널을 이용하여 다시 한 번 인증을 수행한다. 즉, 자신의 식별자를 전송하면서, 인증서버에 챌린지 메시지를 보내어 인증을 수행할 것을 요구한다.

⑩ 인증서버는 사용자 A가 보내온 요구 챌린지 메시지를 확인하여 접속을 허용할 것이지 여부를 결정하고 응답 메시지를 보낸다.

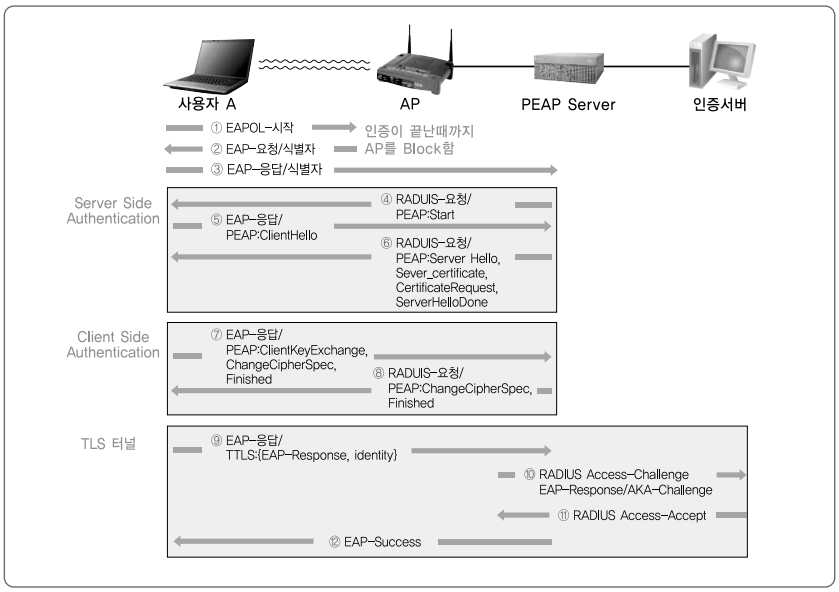
⑪ 이제 인증서버로부터 접속 허용 메시지를 받은 TTLS 서버는 사용자 A에게 접속 성공 메지시를 보내어 인증이 성공적으로 이루어졌음을 알린다.

EAP-TTLS 인증은 무선랜 사용자가 인증서를 사용하기 보다는 패스워드 데이터베이스를 재사용하여 패스워드를 요구하는 방식을 적용한다. 이러한 방식은, 오직 TTLS 서버에서만 인증서를 요구하기 때문에 인증서의 개수를 줄일 수 있는 동시에, 관리도 간소화할 수 있는 장점이 있다.

TLS 터널은 처음에 무선랜 사용자와 인증서버 사이에 만들어지고, 무선랜 사용자는 TTLS 서버로부터 부여되는 인증서를 인증함으로서 연결되는 네트워크를 인증한다. 이러한 방식은 안전한 웹서버 연결에서 사용되는 기술과 매우 유사한 방식이다. 즉, 인증된 터널을 만들고, 이후 사용자에 대한 인증이 이루어지는 것이다. EAP-TTLS 인증은 무선 네트워크에서의 최종 사용자에 대한 동일성을 보장하는 장점이 있고, EAP-TTLS의 최종 사용자의 익명성을 보장하고, 기존 어떤 RADIUS 서버나 이와 관계된 데이터베이스를 재사용할 수 있는 장점이 있다.

마. PEAP 인증

PEAP은 터널링 방식의 인증 알고리즘으로, 사용자 패스워드를 기반으로 하는 인증 방식이다. 아래 〈그림 36〉는 PEAP의 인증절차는 나타내고 있다. PEAP 서버를 이용하여 TLS 터널을 생성하고 이를 통한 인증서버와 사용자간의 인증이 이루어지는 것이 EAP-TTLS와 유사한다.



[그림 36] PEAP 인증 절차

인증 절차에 관한 설명은 EAP-TTLS와 유사하여 생략하기로 한다.

TLS 터널 생성과정에서 인증서 기반의 인증을 수행하기도 하고, TLS 터널 내

부에서는 EAP을 이용한 사용자 인증을 적용하고 있어, TLS Session Resume을 통한 빠른 재인증을 제공하고 있다. PEAP의 적용은 사용자 인증의 보안성이 높고, 관리하기가 편한 반면, 구현이 어렵고 계산 양이 많아 인증 속도가 느려져 사용자의 접속시간을 지연시키는 경우가 발생한다.

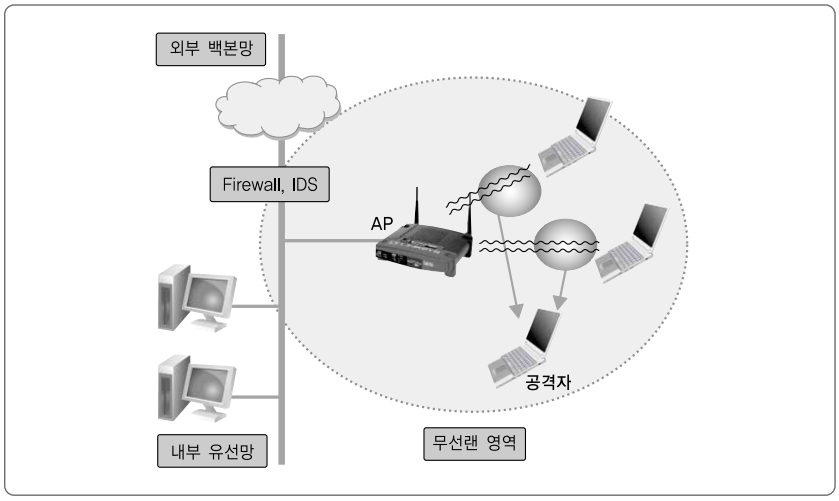
제3절 무선 데이터전송 취약성과 대응기술

이 절에서는 무선랜 환경에서 무선 전파를 이용하여 사용자 데이터를 전송하는 과정에서 발생하는 취약성과 이를 방지하기 위해 적용하고 있는 암호화 프로토콜, 무결성 보장기술 등을 알아본다.

1. 무선패킷 전송관련 일반적인 취약성

무선랜 환경에서 전파를 이용하여 사용자 데이터를 전송할 경우에 무선랜 단말기나 무선랜 패킷 분석도구에 의해서 도청이나 감청이 되는 경우가 발생한다. 아래 〈그림 37〉은 무선랜 서비스 영역에 있는 공격자에 의해서 사용자 데이터가 도

[그림 37] 무선랜 환경에서 전송 패킷 도청



청되는 것을 나타내고 있다.

무선랜 서비스 영역 안에서 공격자가 정상 사용자와 AP 사이의 무선 패킷을 분석하는 것은 아주 쉽게 행하여 질 수 있어, 발생 빈도도 높게 나타나고 있다. 이러한 경우에는 사용자 데이터를 분석하여 주요한 정보를 수집하거나, 향후 침해 공격에 악용할 목적으로 필요한 정보를 수집하는 경우 등으로 나타난다. 이러한 도청과 감청으로부터 사용자 데이터를 보호하기 위해 사용자 데이터를 암호화하고 있다.

2. WEP 적용과 보안 취약성

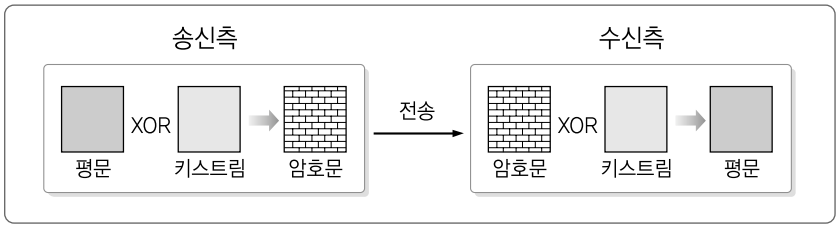
앞에서 언급한 바와 같이 WEP은 유선과 동등한 프라이버시를 제공한다는 목적에서 개발되었다. 개발초기에는 무선랜 보안을 위해 상당히 중요한 기술로 여겨졌으나, 현재는 WEP 설계상의 오류로 인해서 많은 문제점이 제기되고 있다.

WEP은 같은 공유키를 갖고 있는 사용자끼리만 데이터를 알아볼 수 있도록, 데이터를 암호화하여 통신하는 방식을 제공한다. 즉, AP와 무선랜 단말기 사이에 공유키를 이용한 데이터 암호화를 적용하는 것이다. WEP은 데이터 암호화뿐만 아니라, 공유키를 이용한 사용자 인증 기능도 제공한다. WEP에서 제공하는 사용자 인증은 아주 간단하다. WEP은 서로 같은 공유키를 갖는 사람을 정상 사용자로 인증하는 방식을 채택하고 있다.

가. WEP의 암호화 개요

WEP에 사용하고 있는 암호화의 기본원리는 아래 〈그림 38〉에서 표현하고 있는 것처럼 송신측에서 보내고자하는 평문의 메시지를 같은 길이의 키스트림과 비트연산인 XOR 연산을 하여 암호문으로 만든다. 생성된 암호문을 이용하여 송신측에서 수신측으로 전송하면, 수신측에서는 암호문을 전송받아 송신측과 같은 키스트림을 이용하여 비트 XOR 연산을 수행하여 송신자가 보낸 평문의 메시지를 얻는다.

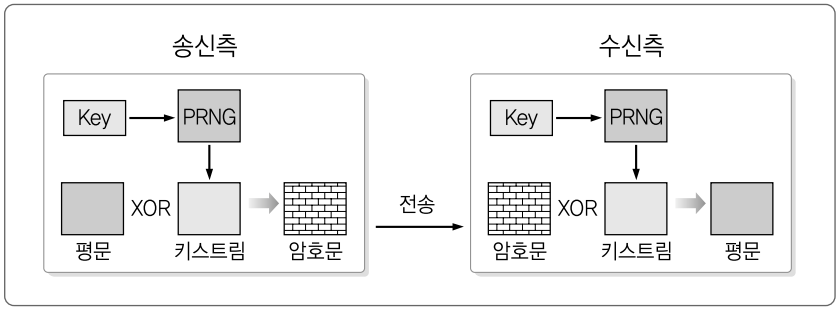
[그림 38] 데이터 암호화의 기본원리



이러한 방식의 적용은 송신측과 수신측에서 항상 같은 키스트림을 이용하여 XOR 연산을 통한 암호문을 생성하기 때문에 쉽게 깨어질 수 있다.

하나의 키스트림을 사용하여 전송 데이터를 암호화 하는 것은 아주 쉽게 데이터가 노출될 수 있으므로, 전송되는 패킷마다 서로 다른 값의 키스트림을 이용하여 암호화 하는 방식을 사용한다. 아래 〈그림 39〉은 공유키와 난수 발생기인 PNRG(Pseudo Random Number Generator)를 이용하여 키 값에 따라 발생하는 난수를 키스트림으로 이용하여 암호문을 생성하는 방식을 나타내고 있다.

[그림 39] 공유키를 이용한 암호화 프로토콜



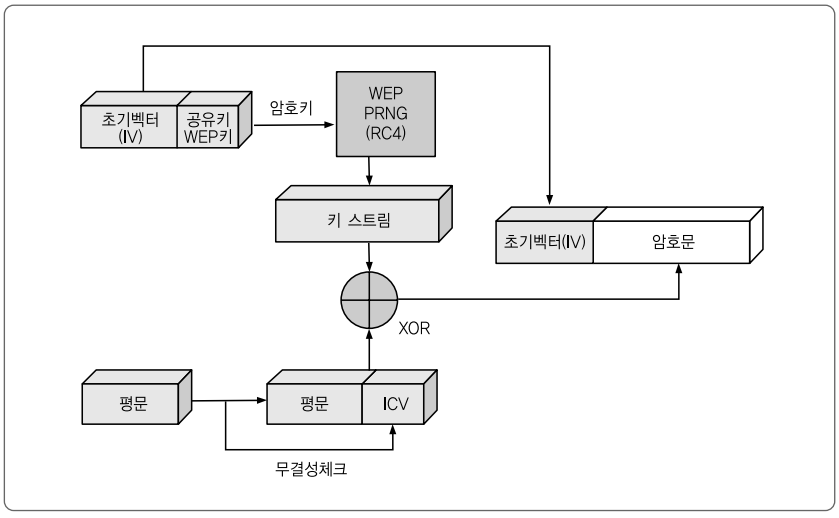
위의 방식은 공유키가 변경되면, 난수 발생기인 PNRG에서 발생하는 난수도 변경되는 특성을 이용하고 있다. 즉, 전송되는 매 패킷마다 서로 다른 키 값을 사용하여 전송하면, 암호학적으로 더욱 안정되게 데이터를 전송할 수 있게 되는 것이다.

송신측과 수신측의 난수 발생기인 PRNG에 같은 키를 이용하여 발생하는 난수가 항상 같아야 한다. 또한, 패킷마다 서로 다른 키스트림을 적용하기 위해서는 패킷마다 서로 다른 키값을 사용하여야 하고, 송신측에서 사용하는 키 값과 같은 값을 수신측에서 사용할 수 있도록 제공하여야 한다. 이러한 공유키와 난수 발생

기를 이용하는 암호화 방식을 좀 더 발전시켜 WEP 프로토콜에서 데이터 암호화 메커니즘을 제공하고 있다.

나. WEP의 데이터 암호화 절차

이제까지 WEP에서 사용하는 암호화의 기본원리에 대해서 알아보았다. 지금부터는 WEP 패킷 생성 절차에 대해서 알아본다. 앞에서 설명한 바대로 WEP은 공유키와 난수 발생기를 이용하여 키스트림을 생성하고, 생성된 키스트림과 전송하고자 하는 평문과의 XOR 연산을 통하여 암호문을 생성한다. 이러한 방식으로 데이터 암호화를 지원할 뿐만 아니라, WEP은 전송되는 데이터의 무결성을 보장하기 위해서 CRC32 알고리즘으로 구성되는 ICV (Integrity Check Value)를 사용한다. ICV는 전송 도중에 발생하는 사용자 데이터 부분을 보호하여 무결성을 제공한다. 아래 〈그림 40〉는 WEP의 패킷 생성 절차를 나타내고 있다.



[그림 40] WEP 패킷 생성 절차

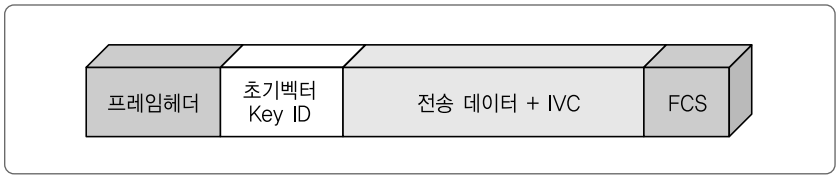
우선, 난수발생기인 PRNG의 입력 값으로 사용하는 암호키를 초기벡터 값과 WEP 키 값을 이용하여 구성한다. 이 값을 이용하여, 난수 발생기에서 키스트림을 생성한다. 이때, 난수발생기는 RC4 암호 알고리즘을 사용하여 난수를 생성한다. 이와 병행하여 전송하려는 평문의 데이터에 무결성을 보장하기 위한 ICV를

CRC32를 이용하여 생성한다. 무결성 체크 값을 생성하는 이유는 전송 도중에 발생할지도 모르는 데이터 변경을 막기 위함이다. 이제, 암호문을 만들기 위해서 난수발생기에서 생성된 키스트림과 전송하려는 평문의 데이터와 ICV 값이 합해진 데이터를 XOR하여 암호문을 만든다.

이렇게 생성된 암호화문에 초기벡터 값을 추가하고, 802.11 표준에서 사용하는 헤더 값을 추가하여 최종적으로 전송하고자 하는 패킷으로 구성한다.

아래 〈그림 41〉는 WEP이 적용된 데이터를 802.11 패킷으로 구성하는 모습을 나타내고 있다. 우선 데이터에 ICV를 추가하고, 난수 발생기에서 생성된 키스트림과 XOR하여 암호문을 만든다. 생성된 암호문에 802.11 프레임 헤더와 FCS(Frame Check Sequence), 초기벡터 값 등을 추가하여 802.11 프레임으로 구성한다. 구성된 패킷 프레임은 무선랜을 통하여 전송된다.

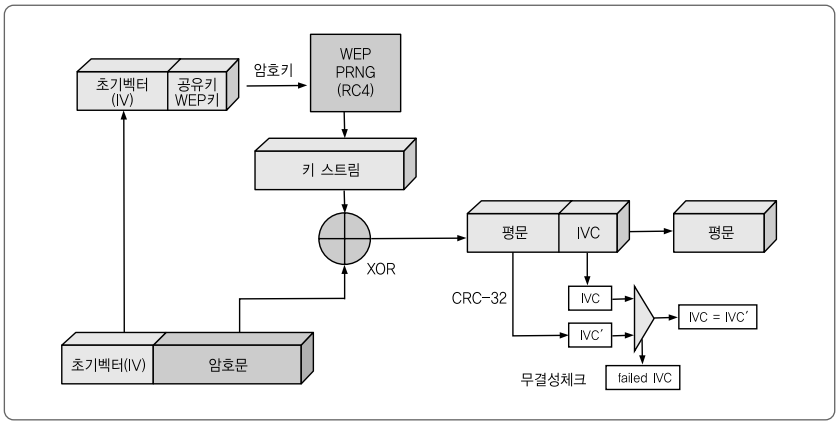
[그림 41] 802.11 패킷 프레임 구성



다. WEP의 복호화 방식

이제 WEP 프로토콜로 암호화된 패킷을 전송 받은 수신측에서 암호문을 풀어주는 방식에 대해 알아보자. 아래 〈그림 42〉은 WEP으로 암호화된 802.11 패킷에서 송신자가 보낸 데이터를 추출해 내는 과정을 나타내고 있다. 송신자가 보낸 패킷에서 초기벡터값을 추출해 내고, 추출해낸 초기벡터값과 자신이 갖고 있는 WEP키를 암호키로 난수발생기에서 난수를 생성하여 키스트림을 구성한다. 구성된 키스트림과 암호문을 XOR 연산을 통하여 복호화 시킨다. 복호화된 평문의 데이터와 IVC를 이용하여 무결정을 체크한다. 무결성 체크 방법은 평문을 무결성 체크를 위하여 CRC32를 이용하여 ICV′을 구한 후 ICV′과 송신자로부터 전송받은 ICV를 비교하여 전송 도중에 혹시라도 패킷 데이터가 변경되었는지 여부를 체크한다. 이렇게 무결성 체크가 성공적으로 이루어지면, 평문의 데이터를 최종

적으로 수신한다.



[그림 42] WEP의 복호화 절차

라. WEP 암호의 취약성

(1) 암호 메커니즘의 취약성

WEP이 갖는 암호학적 취약성 분석을 위해 우선 생일 패러독스 이론을 알아본다.

■■■ 생일 패러독스

생일 패러독스는 같은 생일의 존재에 관한 문제다. 어떤 방안에 사람들이 모여 있다고 하고, 그 사람들 가운데 서로 생일이 같을 두 사람이 있을 확률은 얼마인가를 생각해보는 문제이다. 우선, 방에 모여 있는 사람들이 366명 이상이면 생일이 같은 날인 사람들의 쌍이 발생할 확률은 1이다.

이제 문제를 바꾸어 생각해 본다. 생일이 같은 날인 사람의 쌍이 발생할 확률이 1/2이상이 되려면 방안에 몇 명이상의 사람이 있어야 되는가를 생각해본다. 확률 1/2로 생일이 같은 사람의 쌍이 발생할 수 있는 집단은 실제로 23명 이상이면 된다. 집단의 크기가 23명은 365일과 비교하면 보통 사람들이 생각하는 기대치보다 훨씬 작아서 패러독스라는 말을 사용한다.

이 생일 패러독스를 이용하여 WEP이 갖는 암호학적 취약성을 분석해 보자. 802.11b 표준을 따르는 무선랜의 경우, 여러 곳에서 측정해 본 결과 초당 패킷 전송수가 19개인 것으로 측정되었다. 또한, WEP에서 사용하는 초기벡터에 대해서

생각해 보면, 초기벡터는 24bit 길이로 표현됨으로 전체 224 = 16,777,216개 중의 하나의 특정 값을 사용하게 된다. 이러한 값들을 이용하여 생일 패러독스와 연결하여 생각해 보면 다음과 같다.

- 특정인 = 전송 패킷
- 특정인의 생일 = 특정 패킷의 초기벡터 값
- 365일(총 날짜) = 16,777,216 (총 초기벡터 값)
- 같은 생일날 = 같은 IV값 사용

위의 생일 문제를 "얼마나 많은 무선랜 패킷이 전송되면, IV 값이 중복되어 사용될 확률이 1/2이상 되겠는가?"로 바꾸어 볼 수 있다. 이때 위의 값을 사용하여 확률을 계산하여 보면 4,823개의 패킷이 전송되어질 경우에 같은 값의 IV를 사용하는 패킷이 발생할 확률이 50%이상이 된다. 앞의 계산을 확장하면 12,430개의 패킷이 전송될 경우에는 IV 값의 중복될 확률이 99%이상이 됨을 알 수 있다.

위에서 설명한 측정값에서 802.11b 표준을 적용한 무선랜 환경에서 초당 19개의 패킷을 전송하고 있음으로 이를 고려하여 보면 같은 IV 값을 사용하는 패킷이 발생할 수 있는 12,430개의 패킷이 전송되기까지의 시간은 10분도 안 걸리는 것을 알 수 있다. 즉, 24bit의 초기 벡터를 사용하는 WEP 알고리즘은 10분까지는 안전한 것으로 볼 수 있지만, 10분이 지나면 보안상 매우 취약하다고 볼 수 있다.

(2) WEP 키 관리 취약성

앞의 3장 2절에서도 설명한 바와 같이 WEP은 고정 키 값을 사용하고 있어, 외부 유출의 위험성이 상당하다. 뿐만 아니라, WEP은 일정시간 동안 패킷을 수집 분석하는 공격자에 의해 키 값이 크랙 될 수 있음으로 키 관리에 항상 유의해야 한다. 고정키 값을 사용하는 WEP의 키 관리에 관한 취약성을 줄이기 위해서 동적 WEP을 적용하여 사용할 수 있다. 하지만, 동적 WEP을 적용하여 사용한다 하

더라도, WEP 프로토콜 자체가 갖는 암호학적 취약성을 완벽하게 보완한다고는 할 수 없다. 즉, 동적 WEP의 적용은, WEP 키를 짧은 주기로 변경하여 공격자의 암호키 크랙을 위한 공격에 어느정도 방어 방법을 제공하기는 하지만 키 크랙 공격을 완벽하게 방어 할 수는 없다는 것이다.

3. TKIP 적용과 보안 취약성

가. TKIP의 개요

TKIP은 WEP 알고리즘의 취약성을 보완하기 위해서 연구되었다. TKIP은 WEP을 적용할 수 있도록 구성된 무선랜 장비 펌웨어 업그레이드나 소프트웨어 업그레이드를 통해, 사용자 레벨의 보안을 강화하기 위한 방법을 제공하고 있다. TKIP은 WEP의 암호학적 취약성을 보완하기 위해, 소프트웨어 업그레이드의 적용이나 새로운 패치를 적용하는 등의 방법을 이용하고 있어, 새로운 장비의 추가 구입이나 기존 장비의 교체가 필요 없게 된다.

즉, TKIP의 적용은 WEP이 갖는 취약성을 보완하여 무선랜 보안 기능을 강화하면서 소프트웨어 업그레이드를 통해 보안 기술을 적용할 수 있어, 하드웨어 장비의 추가설치로 인해 발생할 수 있는 비용을 감소 할 수 있게 된다. 또한, TKIP은 전송되는 데이터 패킷마다 증가되는 초기벡터인 IV 시퀀스 값을 WEP키와 함께 해쉬하고, 새로운 WEP키를 생성하여 각 패킷마다 키 지정이 가능하도록 제공한다. 이러한 것은 새로운 키 생성 함수를 이용함으로써 가능해지는 것이다. 즉, 새로운 키 생성 함수에 키 재설정 방식을 적용하여 고정된 WEP 키를 사용할 때 발생하는 키의 외부 유출 가능성을 줄여준다.

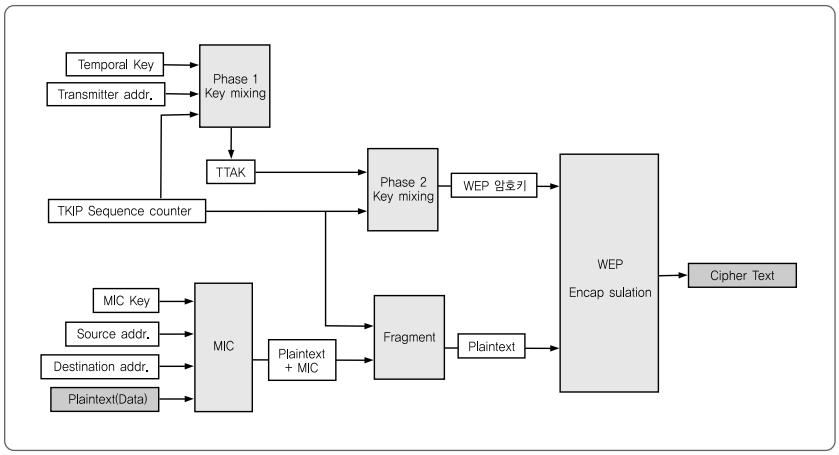
TKIP은 RC4 암호 알고리즘을 기반으로 하고, 다음의 4가지 보안기술을 이용하여 WEP의 취약성을 보완하고 있다.

- 48 bit의 확장된 길이의 초기벡터(IV)를 사용한다.
- 초기벡터 값인 IV의 순차적 증가 규칙을 보완하고 있다.
- 패킷마다 사용되는 암호키에 새로운 혼합 함수를 적용하고, 미분과 분포를 이용하여 키 재설정 기술을 지원하고 있다.
- 메시지 무결성 체크를 위해 WEP에서 무결성 보장을 위해서 적용되었던 CRC-32 알고리즘보다 안전한 MIC(Message Integrity Check)를 사용할 수 있도록 제공하고 있다.

나. TKIP의 암호화 방식

아래 〈그림 43〉은 TKIP을 이용하여 사용자의 데이터를 암호화하는 절차를 나타내고 있다.

[그림 43] TKIP 암호화 절차



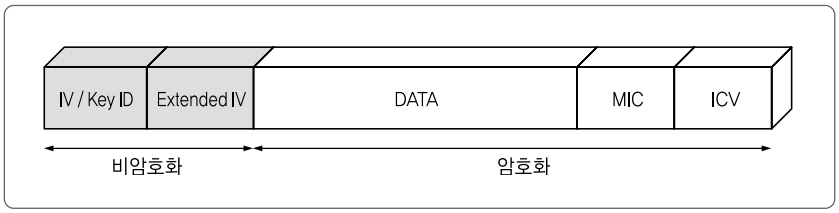
앞에서도 언급했듯이, WEP의 데이터 암호화 단점을 보완하기 위해서, WEP에서 사용하던 24bit의 초기벡터를 확장한 48bit의 초기벡터 값을 이용하고 있다. 위 〈그림 43〉에서도 알 수 있듯이 확장된 초기벡터 값을 만들기 위해서, 임시키(Temporal Key), 전송 주소 값(Transmitter Address), TKIP 시퀀스 카운터(TSC : TKIP Sequence Counter)를 입력으로, 첫 번째 키 생성함수(Key mixing)를 이용하여 TTAK 값을 계산한다. 이 TTAK 값과 TKIP 시퀀스 카운터 값을 입력으로 하는 두 번째 키 생성함수를 이용하여 암호키 값을 계산하게 된다.

여기에서 계산된 암호키 값을 이용하여 WEP 암호화 알고리즘을 적용한다.

TKIP은 암호화뿐만 아니라, MIC를 적용하여 전송하려는 데이터의 무결성도 강화하고 있다. 전송하려는 사용자 데이터에 MIC 키, 근원지 주소, 목적지 주소 등을 키 값으로 하여 MIC 값을 생성한다. 생성된 MIC 값을 전송하려는 사용자 데이터에 추가한다. 이렇게 만들어진 값과 TKIP 시퀀스 카운터 값을 조각화하여(Fragment)하여 전송하기 위한 평문으로 만들고, 앞에서 생성한 암호키 값을 이용하여 WEP 암호화 알고리즘을 적용하여 암호문을 생성한다.

이렇게 생성된 TKIP의 암호문은 단순히 WEP 암호화 알고리즘만을 적용하였을 때 보다, 초기 벡터 값을 확장하고 키 혼합 함수를 이용하여 암호키의 생성을 보완하였고, 전송하려는 사용자 데이터의 무결성을 강화하는 등 보안성을 강화하였다.

TKIP의 암호화 방법을 적용하여 생성된 패킷은 아래 〈그림 44〉과 같은 구조를 갖는다. 〈그림 44〉에서도 알 수 있듯이, TKIP은 48 bit의 확장된 초기벡터를 사용하고 있고, 무결성 강화를 위해서 패킷 뒷부분에 MIC 필드를 추가하고 있다.



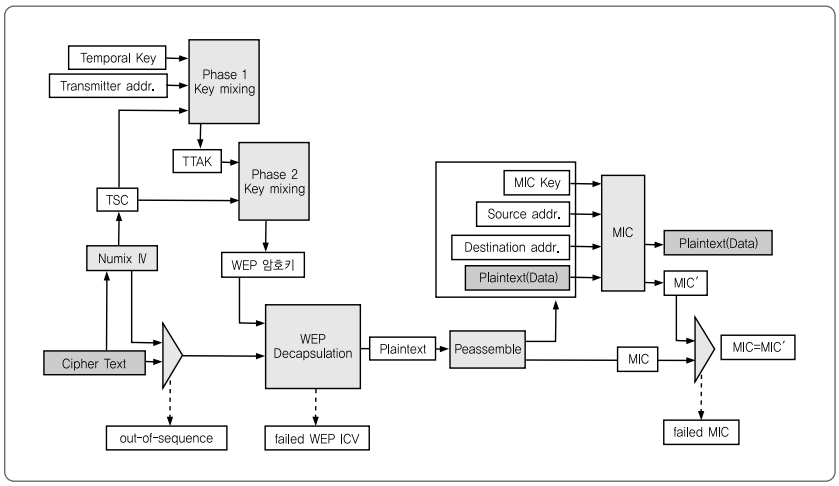
[그림 44] TKIP packet 구조

다. TKIP의 복호화 방식

아래 〈그림 45〉는 TKIP의 복호화 절차를 나타내고 있다. TKIP 복호화는 전송받은 패킷에서 초기벡터인 IV에서 TSC와 Key id를 분리해내는 작업부터 시작된다. 이렇게 분리된 정보인 TSC가 시퀀스 규칙에 부합되지 않을 경우엔 TKIP 패킷을 폐기하고, 그렇지 않을 경우에는 TSC, Key id 등의 정보를 이용하여 암호키 값을 생성한다. 생성된 WEP 암호키 값인 WEP IV 값과 RC4키 값을 이용하여 암호화가 적용된 패킷을 복호화 한다. 복호화된 패킷은 ICV 체크를 한다.

WEP ICV에 문제가 있는 패킷은 폐기하고, 아무런 문제가 없는 패킷은 MIC 알고리즘을 적용하여 데이터 무결성 체크를 한다. 만일 MIC 값에 문제가 있을 경우에는 ICV 체크와 마찬가지로 패킷을 폐기하고 문제가 없을 경우에는 헤더 값을 제거하여 전송전의 데이터를 추출해낸다. 이러한 방법으로 암호화된 TKIP 패킷에서 평문의 데이터를 추출해 낸다.

[그림 45]
TKIP 복호화



라. TKIP의 암호의 취약성

이제까지 WPA 보안기능인 TKIP에 대해서 알아보았다. WPA에서 제공하는 TKIP은 802.11i 보안 기술이 적용되기 전에, 소프트웨어 업그레이드를 이용하여 WEP이 갖는 보안상의 취약성을 보완하고자 연구되어 사용되고 있다. 하지만, TKIP이 새로운 암호 알고리즘을 사용하는 것은 아니라 WEP을 기반으로 하면서 여전히 RC4 암호 알고리즘을 사용하고 있다. 즉, TKIP은 WEP이 갖는 암호학적 문제점을 완전히 보완하였다고는 볼 수 없다. 다만, WEP이 갖는 보안 취약성을 보완하고 있다고 볼 수 있다.

즉, 앞에서 설명한 TKIP 암호화 절차에도 알 수 있듯이, TKIP 프로토콜이 제공하는 암호는 WEP 프로토콜에서 제공하는 암호화 방식을 확장하여, WEP이 갖던 취약성을 보완하고 있다. 초기벡터 값을 24bit에서 48bit로 확장하여 키 값의

난수 발생 영역을 확장하였고, 데이터 무결성을 보장하기 위해서 CRC-32를 이용하는 것 등은 암호 키를 공격자의 크랙 공격의 위험과 무선 패킷의 위조공격으로 인한 전송 데이터의 무결성이 깨지는 위험을 보완하고 있다. 하지만, 암호 알고리즘을 여전히 WEP에서 사용하고 있는 RC4 암호알고리즘을 사용하고 있고, 키 관리 방법을 제공하고 있지 않고, 무선 패킷 수집 분석을 통한 키 크랙공격의 가능성이 내재되어 있는 등, WEP이 갖고 있던 기본적인 취약성을 그대로 갖는 단점이 있다. 뿐만 아니라, TKIP의 적용은 소프트웨어 업그레이드를 이용하고 있기 때문에, 인증과 암호를 모두 소프트웨어적인 계산으로 처리함으로 연결 시 인증속도 저하와 패킷 전송 시 암호화와 복호화로 인한 시간지연 등의 문제가 여전히 남아 있다. 하지만, WEP의 취약성을 기술적으로 보완하고 있는 것은 사실이다. 또한, 인증시 소요시간은 단말기의 성능 향상과 더불어 점점 짧아질 것으로 기대되고 있어, WPA 표준에서 제공하는 사용자 인증과 데이터 암호화 메커니즘을 적용하는 기관이 증가될 것으로 예상되고 있다.

4. CCMP의 개요 및 특성

가. CCMP의 개요

CCMP는 AES 블록 암호를 사용한 데이터의 비밀성과 무결성을 보장하기 위한 규칙들을 정의하고 있다. 앞에서 설명된 TKIP가 RC4를 사용한 암호를 사용하는 반면, CCMP는 이미 전문가들의 많은 검토를 통해 안전성이 입증된 AES를 기반으로 한다. CCMP는 802.11i를 사용한 보안에서의 기본 모드에 해당하며, 더 높은 보안성을 갖는다. TKIP가 기존의 하드웨어를 수용하기 위한 과도기적 기법인 반면 CCMP는 기존 하드웨어를 고려하지 않고 초기부터 보안성을 고려하여 새롭게 설계되었다.

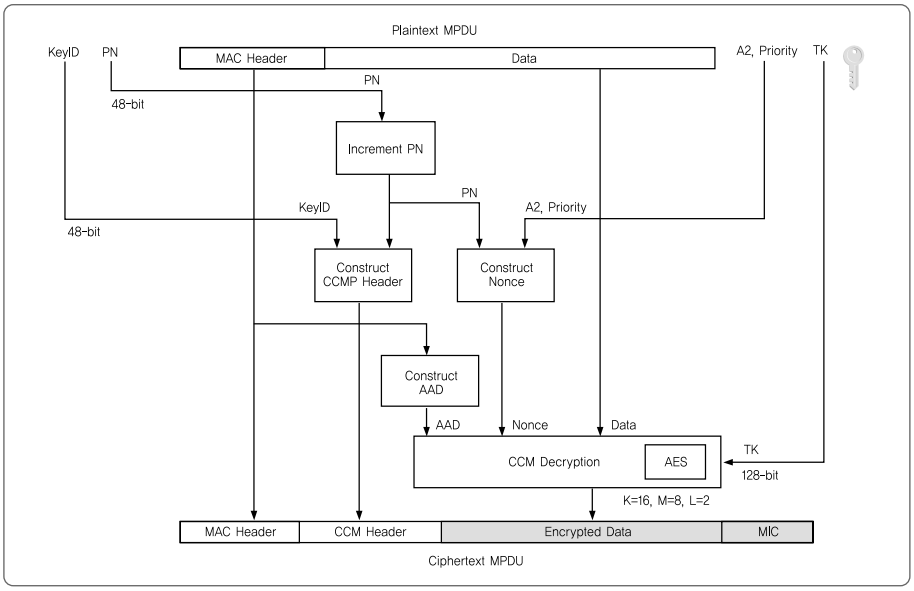
CCMP와 TKIP는 기본적으로 키관리 등에 있어 유사점을 갖는다. 이 두 방법의 가장 큰 차이점은 알고리즘에 있다. CCMP는 128bit의 대칭키를 사용하고, 48bit의 초기벡터를 사용한다. AES가 제공하는 여러 모드 중 CCMP는 Counter 모드

기반으로 CBC MAC (Cipher Block Chaining Message Authentication Code)을 결합한 CCM을 기반으로 한다. CCMP는 패킷의 데이터 영역과 IEEE 802.11 헤더의 무결성을 보장한다. CCMP가 사용하는 PN(Packet Number)는 패킷의 재연(replay)를 방지 할 수 있다. CCM기반의 CCMP의 특성은 아래와 같이 요약될 수 있다.

- 비밀성과 무결성을 위한 단일 암호키는 복잡도를 낮추며, 성능을 높여줌.
- 패킷의 데이터에 대한 비밀성 뿐 아니라, 패킷의 헤더와 데이터에 대한 무결성 보호를 제공함.
- 특정 암호화를 위한 파라미터의 계산을 패킷을 수신하기 전에 수행하여, 패킷이 도착했을 때의 부하를 줄여서, 지연시간을 감소시킴.
- 하드웨어 및 소프트웨어의 구현 범위가 작아 비용이 적게 듬.
- 보안과 관련된 패킷의 부하 적음 (암호화 및 무결성을 지원하기 위한 최소 데이터의 사용)
- 특허 관련 문제로 인한 장애가 없음.

나. CCMP의 암호화 방식

[그림 46] CCMP 암호화 절차



〈그림 46〉[1]은 CCMP 암호화 절차를 보여주고 있다. 이에 대한 간략한 설명은 아래와 같다.

세션을 위한 패킷번호(PN: Packet Number)를 유지 한다. 패킷번호와 주소 필드의 다른 영역 값들을 조합하여 nonce를 생성한다. CCMP 헤더는 임시키(Temporal Key)의 ID 또는 KeyID와 패킷번호를 사용하여 만들어진다. 프레임 헤더(MAC Header)는 AAD(Additional Authentication Data)를 만드는데 사용된다. 22바이트 또는 28바이트의 파라미터로 구성된 AAD 내에는 주소값, 서비스 품질관리 필드 등의 CCM 인증 절차에 추가적으로 사용되는 입력이 포함되어 있다. AAD, nonce와 평문 데이터는 임시키와 함께 CCM의 입력으로 제공되어 데이터의 암호화가 이루어진다. 패킷의 헤더, CCM 헤더와 암호화된 데이터가 연결되어 암호화된 패킷이 완성된다.

CCM에서는 인증 및 암호 입력으로 사용되는 아래 4가지 입력이 존재한다.

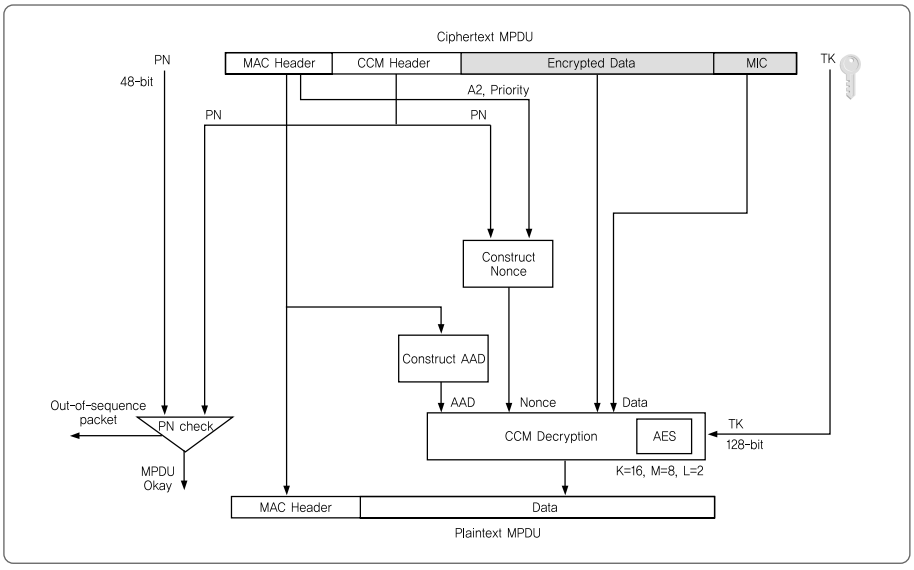
1) 128-bit 암호화 키, TK
2) 48-bit nonce (48-bit의 패킷번호로부터 얻어진)
3) Additional Authentication Data (AAD)
4) 가변적 크기를 갖는 MAC 헤더를 포함한 프레임 자체

CCM은 새로운 임시키를 매 세션마다 사용한다. TKIP와는 다르게, AES를 사용하기 때문에 패킷 별로 키를 가질 필요성을 제거하였다. 결과적으로, TKIP의 2단계 키 혼합 과정이 CCMP에서는 등장하지 않는다. 〈그림 46〉의 가장 윗부분은 전송직전의 평문을 보여주고, 가장 아랫부분은 전송되게될 평문 헤더와 암호화된 결과를 보여준다. 802.11 무선랜을 위해 MIC의 길이는 8바이트로 지정되어 그림에서도 M=8로 명시되어 있다. K=6, L=2로 표시되어 있는 것은 AES 키의 길이가 16바이트이고, 2바이트의 최대 패킷길이 필드가 할당되었음을 의미한다. CCMP는 48비트의 패킷번호를 초기벡터 값으로 사용하며, 패킷번호의 증가함수는 매 프레

1) NIST Special Publication SP 800-97, "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i", Feb 2007

임이 암호화 될 때마다 새로운 값이 사용되는 것을 보여준다. 이 패킷번호의 역할은 패킷의 재연(replay)를 방지 하는 것이지만, 추가적으로 임시키의 유효기간이 세션의 유지시간보다 길도록 보장해 주는 기능을 제공한다.

[그림 47] CCMP 복호화 절차



다. CCMP의 복호화 방식

〈그림 47〉[2]는 CCMP의 복호화 절차를 나타내고 있다. 이 복호화 절차의 핵심 단계를 아래와 같이 요약할 수 있다.

1) 암호화된 프레임은 파싱되어 AAD와 nonce를 재 생성한다. AAD는 프레임 헤더로부터 만들어진다.
2) Nonce는 MAC 헤더의 전송주소(A2), 우선순위와 PN을 사용하여 생성한다.
3) CCM은 임시키, AAD, nonce, MIC와 암호화된 데이터를 사용하여 평문을 생성하고, MIC를 사용하여 무결성 검증을 한다. 만일 무결성 검증이 제대로 되지 않으면 평문을 얻어내지 못한다.

2) NIST Special Publication SP 800-97, "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i", Feb 2007

4) 수신 프레임의 헤더와 평문 데이터는 평문 프레임으로 조합된다.

5) 재연공격 방지를 위해 패킷번호는 세션을 유지하면서 관리되는 패킷번호와 비교를 통해 검증이 되고, 새로 받은 패킷번호가 세션의 패킷번호보다 크지 않으면 해당 프레임은 버려진다.

무 선 랜 보 안 가 이 드

제4장 무선랜 보안 가이드

Korea Information Security Agency

제4장 무선랜 보안 가이드

무선랜의 보안문제는 무선랜이 보급된 이래로 지속적으로 반복되고 있는 문제이다. 무선랜에 대한 보안은 여러 가지 관점으로 나눠 생각해 볼 수 있는데, 무선랜을 구성하고 있는 구성요소, 무선랜의 사용 주체, 또는 무선랜의 사용용도에 따라 다양하게 생각해 볼 수 있다.

본 장에서는 무선랜의 최초 구성시에 고려해야 하는 사항에 대해 알아보고, 무선랜을 구성하는 구성요소 별로 적용해야 하는 보안설정, 그리고 무선랜의 사용하는 주체, 즉 개인 또는 사업자가 적용해야 하는 보안설정으로 나누어서 알아보도록 한다.

제1절 무선랜 보안정책

무선랜의 안전한 운영을 위한 보안정책의 재정에 앞서서 고려되어야 할것이 "과연 무선랜이 꼭 필요한가?"라는 부분이다. 무선랜의 운영으로 인해 발생하는 추가적 위협 사항으로 인해, 무선랜 서비스 도입이 단순히 사용상의 편리함을 위해서라고 한다면 무선랜 도입에 대해 재고가 필요하다고 할 수 있다. 이 밖의 무선랜 도입 시 고려해야할 사항들은 아래와 같다.

■■■ 유선랜과 무선랜의 분리 운영

일반적으로 무선랜을 기존 유선랜의 확장한 개념으로 사용하는 경우가 많다. 이 경우 무선랜을 통해 기존의 내부 네트워크에 접속이 가능하게 되어 무선랜의 보안설정이 취약할

경우, 외부의 사용자가 아무런 제한 없이 기업 내의 주요 시스템에 접근할 수 있음을 뜻한다. 기본적으로 무선랜과 내부 업무용 네트워크는 분리하여 운영하는 것이 필요하며, 분리 운영이 어려운 경우에는 무선랜의 보안강화를 통해 무선랜을 통한 내부 망으로의 접근을 차단하도록 한다.

■■■ 전송데이터 보안유지 여부

전송데이터 보안은 일반적으로 무선 클라이언트와 무선 AP와의 구간에서의 보안성 유지를 위해 전송 데이터 암호화를 사용하는 것을 말한다. 무선 통신은 특성 상 데이터가 실린 전파신호를 도청하거나 전파방해가 가능하므로, 기본적으로 보안에 민감한 정보는 무선랜을 통해 전송하지 않는 것이 필요하다. 무선랜의 보안에서 데이터 암호화 방식이 중요한 부분을 차지하며, 암호화 방식의 적용은 무선랜 구축 시 사용되는 관련 장비(무선 단말기 OS, 무선 랜카드, 무선 AP)에서 지원되는 방식을 필히 확인한 후 적용한다.

또한, 암호화 방식에 따른 무선 장비의 성능도 고려되어야 한다. 무선 장비의 성능은 무선 데이터의 암호화가 적용된 경우, 무선 장비의 추가적인 인증작업과 동작을 필요로 하므로 암호화를 적용하지 않은 경우에 비해 데이터 전송 효율이 떨어지게 된다. 따라서 무선 클라이언트의 수와 전송 데이터의 크기를 고려하여 충분한 수의 무선 AP를 운영하여야 한다.

■■■ 무선랜 접근제한 설정

무선 전송 데이터의 암호화와 더불어 중요한 사항으로, 무선랜에 허가된 무선 클라이언트만이 접속 가능하도록 운영하는 것이 필요하다. 일반적으로 무선 AP의 네트워크 이름(SSID)와 네트워크 키값을 이용해 인증과정이 진행되게 되며, 이를 통해 기본적인 접근제한이 적용될 수 있다.

하지만, 취약한 인증방식이 사용되는 경우, 임의의 무선 클라이언트의 접속이 가능하게 되어 보안사고의 발생 가능성이 높아지게 된다. 따라서 최초 무선랜의 구축 시에 안전한 인증방식을 선택하고, 해당 방식이 지원되는 무선 관련 장비를 구매하도록 한다.

■■■ 전파간섭 등으로 인한 서비스 거리 제한

유선랜 UTP 케이블의 거리제한와 같이 무선랜도 거리제한을 고려해야 한다. 무선에서는 대기 중의 잡음, 사무실 환경 등에 따라 거리의 제한이 발생하므로 최초 구축 시 무선랜이 사용될 범위 및 사용자 수에 따라 속도저하가 발생한다. 이를 고려하여 무선 AP의 수를 조정해야한다. 사용자 수의 증가로 인해 속도저하가 발생할 경우, 무선 AP의 확장이 필요하므로, 초기 구축 시 확장성을 염두에 두어야 한다.

802.11b 또는 802.11g에서 사용되는 2.4GHz 대역은 몇몇 전자기기에서도 사용되는 대역으로, 아래와 같은 기기와는 일정거리 이상을 거리를 두거나 무선 AP의 설정변경을 필요로 한다.

전자기기별 AP 운영 주의사항

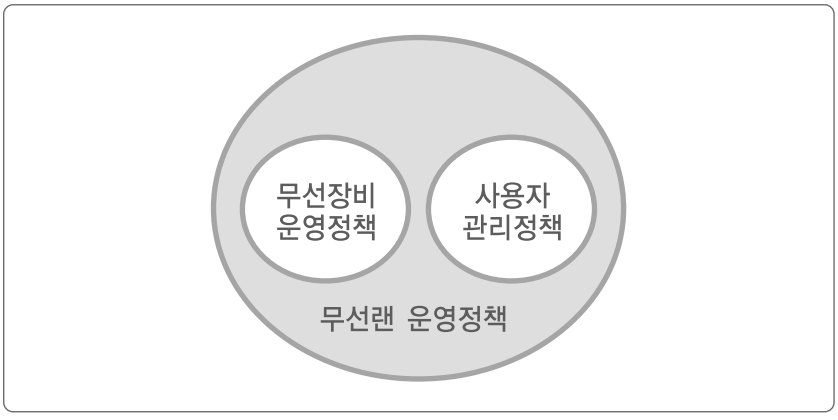
전자기기	주의사항
전자레인지	5미터 이상 이격, 무선 AP의 채널을 1, 2, 12, 13번으로 조정
플라즈마 전구	무선 AP의 채널을 11~13번으로 조정
블루투스	5미터 이상 이격 필요
DSRC	802.11a 설정 무선 AP의 경우, 161번 채널 사용금지

무선랜의 체계적인 운영 및 관리를 위해서는 무선랜의 보안정책 수립이 필요하다. 정책적으로 기본적인 무선랜의 운영 방안과 보안 기준을 설정함으로서 세부적인 시스템의 구성과 운영방향이 명확해지고, 보안 수준의 유지와 더불어 보안의 향상도 이뤄질 수 있기 때문이다.

이러한 보안정책은 무선랜을 최초 도입하는 시점에 앞서 수립함으로서 적절한 무선 장비의 도입이 가능해지는 것은 물론 향후 목적하는 수준의 보안유지가 가능하다.

무선랜의 보안정책에 대해 본 가이드에서는 무선 AP, 무선 단말기와 같은 무선장비의 운영정책, 무선랜에 대한 운영적인 보안정책, 그리고 관리자 및 사용자 관리정책 등 크게 3가지 분야로 나눠 정의하였다. 또한 각 업체의 상황과 요구하는 보안 수준의 차이가 있을 수 있으므로, 직접적인 정책을 제시하지 않고, 각 부분에서 다뤄져야하는 항목을 제시하였다.

[그림 48] 무선랜 보안 정책의 구성요소



추가로, 무선장비 운영정책에 있어서는 각 업체가 상황에 맞춰 활용할 수 있도록 기본적으로 갖추어야 하는 기본정책과 추가로 권장하는 확장정책으로 나누어 제시하였다.

1. 무선랜 운영정책

무선랜의 이용 목적을 정의하고 그에 맞는 운영방향을 결정하는 것을 말한다. 무선랜 운영정책은 최초 무선랜을 도입하는 시점에 앞서 준비되어야 하며, 전반적인 보안 운영정책을 먼저 정하고, 세부적인 장비의 설정이나 사용자 관리정책 등은 추가적인 정책 수립을 통해 관리하는 것이 효율적이다. 무선랜 운영정책은 각 업체의 운영상황과 필요에 따라 수립을 하며, 가능한 다음 항목이 포함되도록 한다.

가. 기본 무선랜 운영정책

(1) 무선랜의 서비스 범위 및 용도의 정의

여기서 말하는 서비스 범위는 2가지 관점에서의 범위를 뜻한다. 첫 번째는 무선랜이 사용되고 있는 업무의 종류와 범위를 뜻한다. 회사 내에서 진행되는 여러 가지 업무 중 무선랜이 이용되는 업무의 종류와 다른 업무와의 연관성을 포함한다. 이는 무선랜의 장애가 발생하였을 경우에 영향을 받는 업무와 관련 업무의 범위를 신속히 파악하므로서 2차적인 피해의 진행을 사전에 파악하기 위함이다.

두 번째로는 실제 무선랜이 서비스되는 시간 및 공간적 범위를 뜻한다. 무선랜이 설치되어 제공되어야 하는 범위를 사전에 정의함으로서 무선 서비스 제공지역 이외에서 불법적인 무선랜의 운영상황을 신속히 파악할 수 있게 된다. 또한 서비스 장애 발생 시 장애 범위의 파악과 장애로 인해 서비스가 중지되는 지역의 파악에 많은 도움이 되게 된다.

(2) 무선랜 네트워크 구성도(기존 유선랜을 포함한 구성도)

네트워크 구성도는 유선랜과 마찬가지로 초기 무선랜 구축 시에 필수적으로 작성하게 되는 것으로 필요에 따라 여러 형태의 구성도를 보유하고 있는 것이 관리적 차원에서 유리할 것으로 보인다.

○ 무선랜 네트워크 구성도
- 단순히 무선랜 네트워크만을 포함하는 구성도

○ 유선랜/무선랜 네트워크 구성도
- 기존의 유선랜과 무선랜의 구성을 함께 포함하는 네트워크 구성도

구성도에는 무선장비 운영정책에서 정리된 보유 무선장비 및 무선 단말기의 정보를 충실하게 반영하는 것이 장애 처리 시 보다 효율적이다.

이러한 구성도를 통해서 고려할 수 있는 추가적 운영정책으로, 무선랜에서 생성된 데이터의 통제를 위한 흐름도의 작성이 있다. 무선랜 생성 데이터 흐름도는 무선랜 장애 및 사고 발생 시 그 원인을 찾는 데에 유용하게 활용될 수 있다.

(3) 무선랜을 통한 접근가능 네트워크 범위 정의

무선랜 네트워크를 통해 내부 또는 외부 네트워크로의 접근이 가능하도록 정책을 세울 것인지 정의하는 것을 말한다. 이 부분은 보안운영정책에서 아주 중요한 부분으로서, 무선랜 또는 유선랜의 취약점을 통해 침해사고가 발생한 경우, 피해규모와 피해의 확산을 제한된 범위로 한정하겠다는 것을 말한다.

무선랜의 보안취약점으로 인해 미인가 무선 단말기의 접속이 가능한 경우, 만일 무선랜을 통해 내부 네트워크로의 접속에 제한이 되어 있지 않다면, 무선랜 취약점으로 인해 보다 큰 2차 피해가 발생하게 된다. 이러한 사고의 한 사례로서 2005년 미국의 대형 의류 할인점에서는 고객 정보가 전달되는 결재 단말기에서 사용되는 무선랜 구간의 취약점을 이용해 내부 네트워크로 침입하여 수 천만건의 고객정보를 내부 중앙컴퓨터로부터 탈취한 사고가 발생하였다.

이러한 피해의 확산을 막고 피해규모의 예측을 위해 반드시 무선랜은 기존의 유선랜과는 분리하여 운영하는 것을 원칙으로 하고, 분리가 어려운 경우에는 별도의 보안장비를 이용해 내부 유선랜으로의 접근을 제한한다.

(4) 무선랜을 통한 인터넷 접속여부 및 기준 정의

무선랜에 연결된 무선단말기로부터 외부의 인터넷으로의 접속여부를 결정하는 부분으로, 일반적인 관점에서는 무선 단말기의 인터넷 접속은 제한하는 경우가 많다. 하지만, 무선 단말기의 경우, Windows Mobile, Symbian 등의 Mobile OS가 설치되게 되는데 이러한 Mobile OS의 신속한 보안패치와 설치 S/W의 관리측면에서는 인터넷 접속이 필요할 수 있다. 하지만 반대로 인터넷으로의 접속을 통해 악성코드 감염 등의 위험성에 노출되는 부분도 존재하게 된다.

따라서, 이 부분은 각 회사의 무선랜 유지보수 정책에 맞춰 정책을 수립하도록 하며, 그 정책에 맞춰 충실히 적용하도록 한다.

(5) 주기적인 무선장비 관련 암호의 변경

무선장비의 보안을 강화하기 위한 기본적인 방안으로서 무선 AP와 같은 무선장비의 관리자 암호화와 무선 AP의 인증암호 등을 강화하는 정책을 수립하도록 한다. 대부분의 네트워크 장비와 마찬가지로 무선 AP의 경우에도 H/W 제작사마다 공장출고 시에 장비의 관리자 암호로서 기본 설정 암호(Default Password) 값을 가지고 있다. 이 기본 설정 암호는 장비의 초기화 시 기본적으로 가지게 되는 값으로서, 장비의 초기 설치 시 반드시 변경하여 관리하도록 한다.

또한, 이러한 암호의 주기적인 변경에 대한 정책을 통해 일정 수준의 보안이 유지되도록 하며, 별도의 사용 암호에 대한 규칙도 함께 수립하는 것이 바람직하다.

(6) 무선랜 관리팀 및 담당자 지정

무선랜 시스템의 유지와 보안수준의 지속적인 관리를 위해서는 관리업무를 전담하는 인력이 필요하다.

무선랜의 구축 이전에 앞서 운영 중이던 기존 시스템의 관리업무를 담당하는 팀 또는 담당자가 무선랜에 대한 관리업무를 수행하는 것이 일반적일 것으로 예상된다. 관리할 시스템의 규모가 일정 규모 이상인 경우, 관리팀과 보안 팀이 분리되어 운영되는 경우가 있는데, 이번 정책항목은 시스템의 일반적인 관리를 뜻하므로 기존의 관리팀에서 업무를 담당하는 것이 적절하다.

무선랜의 관리팀과 담당자는 무선랜의 평상 운영을 담당하고, 주기적인 점검은 물론 장애 발생 시의 신속한 복구업무를 담당한다. 또한 무선랜 보안 점검리스트의 작성, 갱신과 함께 무선랜의 전반적인 운영정책의 관리도 담당해야 한다.

(7) 무선랜 보안점검 주기 정의

무선랜 보안점검 주기란 무선랜에 대한 정기적인 보안점검의 실시에 대한 항목으로, 무선랜의 운영상태 및 보안수준에 대해 주기적으로 점검하는 정책을 수립하는 것을 말한다. 무선랜에 대한 보안점검은 2가지 측면에서 진행될 수 있는데, 무선랜을 구성하고 있는 주요 장비 및 운영 상태에 대한 점검과 함께 무선랜의 불법적인 이용에 대해 수시 모니터링 및 보안점검을 진행하는 부분으로 나눠 생각해 볼 수 있다.

무선랜 장비 및 운영 상태에 대한 점검은 기존 유선랜과 내부 서버의 정기점검 일정에 맞춰 무선랜의 보안점검을 실시하는 것이 효율적이지만, 무선랜의 불법 이용에 대한 보안점검은 실시간으로 점검이 이뤄져야만 효과를 볼 수 있다. 실시간 점검방법에는 Net Stumbler와 같은 프로그램을 이용한 모니터링과 별도의 솔루션을 구축하여 진행하는 방법이 있다.

(8) 무선랜 보안 점검리스트

정기적 또는 비정기적으로 운영 중인 보안랜의 점검을 실시하기 위해서는 보안점검리스트의 준비가 필수적이다. 보안 점검리스트에 포함되어야 하는 항목들은 여러 내용이 포함될 수 있겠지만, 기본적으로 무선장비 및 무선 단말기에 대한 점검항목과 사용자 점검항목에 대해서는 가능한 철저히 준비하도록 하며, 지속적으로 점검 리스트를 추가해 나가도록 한다.

2. 무선장비 운영정책

무선장비 운영정책에서는 무선랜을 구성하고 있는 주요 장비의 관리 및 보안설정 내용을 포함한다. 무선랜 관련 장비들의 기본 운영에 필요한 설정과 함께 보안설정을 가능한 모두 포함시키도록 한다. 특히 무선 AP와 무선 단말기에 대한 보안설정과 더불어 장비의 관리적인 측면의 정책도 반드시 포함하도록 한다.

가. 기본 무선장비 운영정책 항목

(1) 무선 장비 (무선 AP/무선 단말기)의 설정 정의

무선 장비에서 설정해야 하는 설정값에 대해 정의하는 항목이다. 여기서 말하는 무선 장비는 무선랜을 운영하는데 필요한 무선 AP, 무선 단말기, 인증시스템 등을 말하며 기본적인 무선랜의 운영에 필요한 무선 AP의 설정값은 물론 보안관련 설정값도 필히 포함되어 기본 설정값을 정의하도록 한다.

[표 5] 무선 장비의 주요 관리항목

무선장비	주요항목
무선 AP	SSID, 무선 인증방식 설정 (WEP, WPA), 암호화 방식 (TKIP, AES), SSID 브로드캐스트 설정, MAC 인증 사용설정, MAC 등록
무선 단말기	무선 인증방식 설정, 인증 암호값, 암호화 방식

각각의 항목에 대해 설정되어야 하는 설정값을 전체적으로 정리하여 〈표 5〉와 같이 관리하도록 하며, 각 항목의 내용은 무선랜 보안점검리스트에 포함시켜 정기점검 또는 평시 모니터링 시 활용하도록 한다.

(2) 접속 허용 무선 단말기 리스트

무선랜의 특성 상 여러 가지 보안 설정을 적용하더라도 새로운 보안 취약점의 발견이나 비밀키의 노출 등으로 인해 임의의 사용자에 대한 접근을 완벽하게 차단하지 못할 수 있다. 이에 좀 더 안전한 무선랜의 보안유지를 위해 사용되는 무선 단말기 리스트를 관리할 필요가 있다.

접속을 허용할 무선 단말기의 리스트 작성을 통해 현재 보유 중인 무선 단말기의 일반적인 관리를 진행하고, 추가적으로 무선 단말기의 고유값을 근거로 하여 무선랜의 참여를 제한하도록 한다.

그 한 예로서 무선 단말기의 MAC 주소를 얘기할 수 있는데, MAC 주소의 변조를 통한 우회 접속이 가능한 것이 사실이나 무선 단말기의 MAC 주소를 이용해 접속제한을 설정하는 것이 무선랜의 보안 수준을 한 단계 높이는 방법으로, 가능한 무선 AP에 보유 단말기의 MAC 주소를 등록하여 운영하도록 한다.

만일 무선 단말기가 사용되는 서비스 지역의 지정이 가능하다면 사용지역의 무선 AP에만 MAC 주소를 등록하여, 사용지역을 벗어난 무선 단말기는 통신이 되지 않도록 조치하는 것도 보안을 한 단계 높일 수 있는 방법이다.

(3) 무선 단말기에 설치되는 S/W 리스트

무선 네트워크의 보안을 향상시키기 위해서는 무선 네트워크에 접속하는 무선 단말기의 보안이 중요한 부분을 차지한다. 특히 일반 사용자가 사용하게 되는 무선 단말기의 경우, 보안에 취약한 요소를 다수 가지게 되므로 철저한 무선 단말기의 관리는 무엇보다 중요하다고 할 수 있다.

무선 단말기의 경우, 기본적인 OS의 설치이외에도 업무에 필요한 다수의 S/W가 설치되는데 무선 단말기의 보안을 위해서는 무선 단말기에 설치되는 S/W를 관리할 필요가 있다.

일반적으로 무선 단말기의 경우, 특정한 용도로 사용되기 때문에 용도이외의 S/W를 설치하는 경우는 적지만, 만일 무선 네트워크가 인터넷에 연결되어 있는 경우에는 사용자가 예상하지 못한 순간에 임의의 프로그램이 설치될 가능성이 존재하게 된다.

따라서, 별도로 무선 단말기에 설치되어야 하는 S/W 리스트를 작성하여 사용자에게 전달하고, 주기적인 점검을 통해 불필요한 S/W나 악의적인 S/W의 설치 여부를 점검하도록 한다.

(4) 무선 AP 물리적 보안 정의

무선 AP는 무선 서비스의 특성 상 외부에 노출된 형태로 설치되는 것이 일반적이다. 이 경우, 외부의 비인가자의 접근이 가능하게 되어 전원 케이블이나 내부 네트워크 케이블의 노출로 인한 문제가 발생할 가능성이 존재하게 된다.

따라서, 무선 AP 등의 무선장비를 설치하기 위한 환경조건을 무선장비 운영정책에 반드시 명기하여 기본적인 무선 장비의 물리적인 보안 수준을 유지하도록 한다.

나. 확장 무선장비 운영정책

확장 무선장비 운영정책은 기본적인 운영정책에 보안정책의 추가를 통해 무선랜의 보안수준을 한 단계 더 높이고자 할 때 적용하는 운영정책을 말한다. 반드시 추가하여야 하는 정책은 아니지만, 무선랜을 통해 침해사고가 발생했을 경우의 대응을 위해서는 가능한 정책추가를 통해 운영할 필요가 있다.

(1) 주기적인 무선장비 로그의 점검

주기적인 무선장비의 로그 점검은 무선 AP나 인증서버 등의 무선 장비에서 생성되는 로그를 일정기간 보관하고, 주기적으로 점검하여 불법행위가 있었는지 확인하고자 할 때 필요한 정책이다.

일반적으로 라우터, 스위치 등의 네트워크 장비의 로그는 별도로 관리되지 않고 있는 것이 현실이나, 실제 침해사고나 불법행위의 자세한 분석을 위해서는 네트워크 장비의 로그를 통해 많은 정보를 확인할 수 있으므로 침해사고 분석에 많은 도움을 주게 된다. 무선 장비의 로그는 장비에 직접 저장되어 관리하는 형태가 아닌 별도의 로그서버 구축을 통해 관리가 가능하다.

(2) 불법 AP의 주기적인 검색

불법 AP의 주기적인 검색이란 운영 중인 무선랜의 서비스 지역 내에 불법적으로 설치한 무선 AP가 존재하는지 확인하는 것을 말한다. 불법 AP를 통해 시도되

는 공격유형은 무선랜을 통해 전송되는 정보의 획득이 주를 이루며, 이러한 공격을 차단하기 위해서는 주기적인 불법 AP의 검색이 필요하다.

실시간 모니터링을 위한 무선랜 모니터링 S/W가 활용될 수 있으며, 일부 무선랜 솔루션에서는 불법 AP의 탐지 및 알람 기능이 제공되기도 한다.

(3) 무선랜 접속 인증서버의 관리

802.11i에서 802.1x/EAP를 이용해 무선랜 인증을 구축한 경우에는 별도의 인증 서버가 구성되게 된다. 이 경우 인증서버는 일반적으로 기존 사내의 유선 네트워크에 위치하여 무선 AP를 통해 전달받은 내용을 근거로 무선랜의 인증여부를 판단하게 된다.

3. 사용자 관리정책

기업 내 보안정책은 기본적으로 운영 및 시스템 관리 정책과 더불어 사용자에 대한 보안정책이 기본적으로 구성되어야 한다. 그 중 사용자 관리정책은 시스템과 보안에 대한 인식이 부족한 사용자에 대한 관리방안을 명시하는 정책으로서 다른 정책에 비해 고려해야할 점이 많다.

가. 기본 사용자 관리정책

(1) 무선랜 사용자 리스트 작성

무선랜을 사용하는 사용자의 리스트 작성을 통해 임의의 사용자가 무선랜에 접속하는 것을 차단하는 목적에 활용한다. 단순한 사용자 리스트만으로 실제 접속 제한을 구현할 수는 없으므로, 사용자별 접속 아이디와 패스워드 리스트, 그리고 앞서 언급된 무선장비 운영정책의 접속 허용 무선 단말기 리스트를 하나의 리스트로서 관리하여 접근제한을 구현하는 것이 효과적이다.

다음은 무선랜 사용자 리스트의 작성 예로서 앞서 언급한 주요 요소를 〈표 6〉과 같이 작성 할 수 있다.

[표 6] 무선랜 사용자 리스트의 작성 예

연번	사용자이름	아이디	패스워드	보유무선단말기	MAC address	비고
1	A	ID1	PW1	결재단말기	00-00-00-00-00	
2	B	ID2	PW2	무선 POS	00-00-00-00-00	
•	•	•	•	•	•	•

본 리스트에는 중요 정보가 포함되어 있으므로, 비밀등급의 부여를 통해 관리자를 포함한 필수 인력만이 취급할 수 있도록 관리하여야 한다.

(2) 무선랜 사용자의 주기적인 보안교육 실시

무선랜의 보안은 시스템의 보안유지와 관리자만의 노력으로는 유지 될 수 없다. 무선랜 사용자의 작은 실수하나가 전체 무선랜의 보안에 치명적인 영향을 줄 수 있으므로, 사용자 대상의 보안교육을 주기적으로 실시하여 사용자 인식의 제고가 필요하다.

주요 무선랜 보안교육 내용에는 무선랜에 대한 이해와 보안의 필요성, 올바른 무선랜의 이용방법 등을 포함해야 하며, 새로운 인력 입사시 반드시 보안교육을 실시하여 무선랜 사용자의 보안수준을 일정 수준이상으로 유지할 수 있도록 노력해야 한다.

제2절 무선랜 적용영역 별 보안대책 및 AP 보안

무선랜 표준에서 가장 이슈가 되고 있는 부분은 무선랜의 보안으로, 점차 무선랜의 속도가 향상되고 사용자가 증가함에 따라 그 중요성도 더욱 높아지고 있다. 본 장에서는 무선랜을 적용하는 대상별로 어떻게 보안 기술을 적용 운영해야 하는지에 대해 알아보도록 한다.

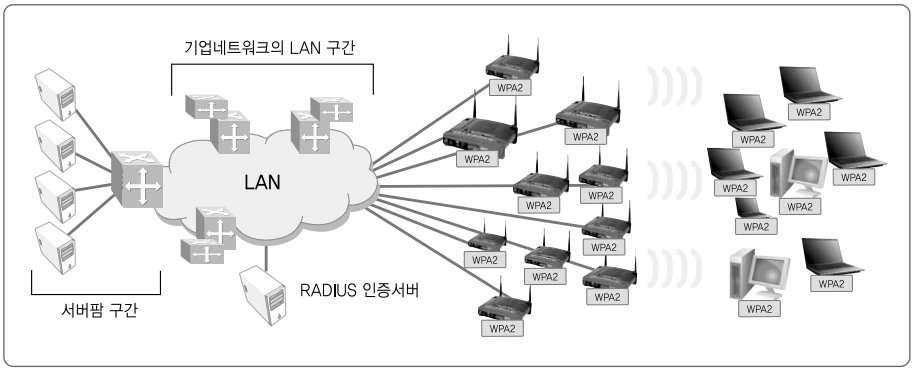
WPA와 WPA2는 〈표 7〉과 같이 인증과 암호화 관점에서 차이점이 있다. 무선랜 환경의 안전한 운영을 위해서는 WPA2를 사용하는 것이 권장되고 있다. 하지

만, WPA2를 지원하는 하드웨어 장비가 구비되어야만 하기 때문에 무선랜 환경을 완전히 WPA2 기반으로 바꾸기는 어려운 실정이다.

[표 7] WPA, WPA2의 모드별 비교

	WPA		WPA2	
	Authentication	Encryption	Authentication	Encryption
엔터프라이즈 모드	IEEE 802.1X/EAP	TKIP/MIC	IEEE 802.1X/EAP	AES-CCMP
개인 모드	PSK	TKIP/MIC	PSK	AES-CCMP

[그림 49] WPA2와 인증 서버를 이용한 무선랜 보안 구성



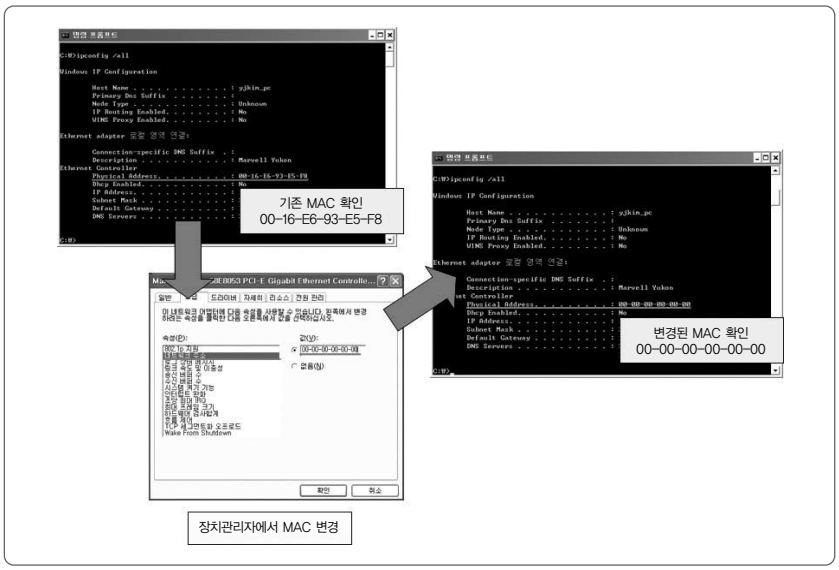
무선랜 적용을 2가지의 영역으로 나누면, 일정규모 이상의 네트워크를 소유하고 이의 일부로 무선랜을 사용하는 기업 사용자와 네트워크 구성의 편리성을 위해 개인이나 SOHO 수준의 네트워크로 구분할 수 있다.

일정규모 이상의 기업 사용자 관점에서는, 본 장의 1절에서 명시한 무선랜 보안정책들이 정의되어야 하며, 보안정책을 기반으로 기술의 적용이 이루어져야 한다. 〈그림 49〉와 WPA2를 기반으로 데이터의 암호화와 RADIUS 인증서버를 사용한 무선 단말의 인증을 통해 무선랜의 안전한 사용을 위한 보안구성을 보여주고 있다. 본 절에서는 〈그림 49〉와 같은 보안 설정을 위한 요소기술 및 이들의 설정 방법을 제시하고자 한다. 또한, 개인 또는 SOHO 수준의 네트워크에서는 안전한 무선랜 환경을 만들기 위한 최선의 방법을 제시하고자 한다. 또한, 기업 및 개인 모두에게 적용될 수 있는 무선 AP의 관리적 물리적 방안을 제시하고자 한다.

1. 기업 네트워크에서의 무선랜 보안

가. 무선 단말 인증

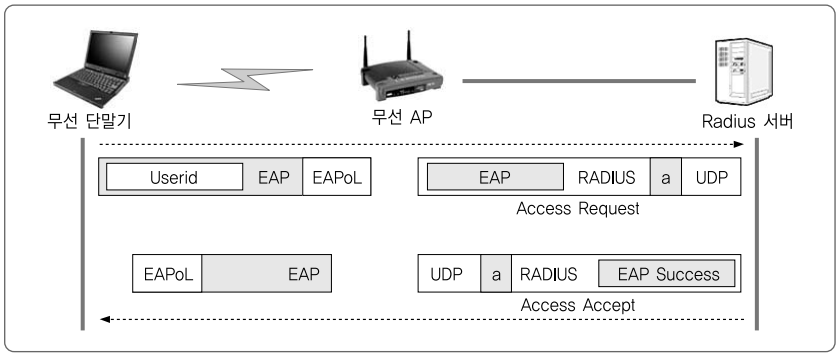
기업 네트워크에서의 무선단말 인증은 RADIUS(Remote Authentication Dial-In User Service) 서버를 활용하여 EAP 기반의 인증을 하도록 권고한다. 무선 단말의 인증을 위해 사용할 수 있는 MAC 주소 인증의 경우 운영체제에서 손쉽게 스푸핑을 할 수 있기 때문에 권장하기 어려우며, 데이터의 암호화를 위해 사용하는 WEP 키 기반의 단말 인증은 그 취약점에 대해서 3장에서 명시하였다. 따라서, 무선 단말 인증을 위한 전용 서버의 사용은 기업 내 무선랜의 비중이 높아지는 시점에서 매우 필수적이라고 할 수 있다. 다음 〈그림 50〉은 윈도우 환경에서 MAC 주소를 변경하는 방법을 보여주고 있다.



[그림 50] Windows XP에서의 MAC 어드레스 변경 방법

별도의 RADIUS 서버 운영은 무선 AP에 참여할 수 있는 사용자에 대한 정보를 별도로 관리하여 허가받은 사용자에게만 무선랜의 사용을 허용함으로서 본장의 1절에서 명시하였던 무선랜 보안정책의 효과적 적용을 위한 기술적 지원 받을 수 있다. RADIUS 인증절차는 〈그림 51〉와 같다.

[그림 51] RADIUS 인증 동작



① 무선 클라이언트는 사용자 계정을 포함한 EAP 메시지를 무선 AP로 송신 (무선구간)

② 무선 AP는 수신된 EAP 패킷을 RADIUS 패킷으로 싸서 RADIUS 서버로 전달 (유선구간)

③ RADIUS 서버는 사용자 계정DB와 비교하여 유효한 사용자인지를 판단한 후, 결과를 정상 사용자의 경우, EAP Success 메시지가 내포된 (Encapsulation) 된 RADIUS Access-Accept 메시지를 무선 AP로 전달

④ 무선 AP는 해당 사용자의 무선 인터넷 접속을 허용, EAP Success 메시지를 EAPoL 패킷에 내포하여 사용자에게 전달

무선망에서의 RADIUS 인증은 EAP(Extensible Authentication Protocol) 메시지를 이용해 사용자 인증을 수행한다.

EAP는 초기에는 PPP(Point to Point Protocol)에서의 사용을 위해서 개발되었으나, 무선랜 802.1x에서 사용자 인증 방법으로 사용되어지고 있다. 다음은 다양한 인증 방법에 사용될 수 있도록 설계된 EAP의 기본구조이다. EAP는 링크계층에서 다양한 인증방법의 전송을 지원한다. EAP는 다양한 인증방법을 제공하기 위해 코드 필드에서 사용하는 인증방법을 구분하고, 데이터 영역은 가변 길이로 정의를 하고 있다.

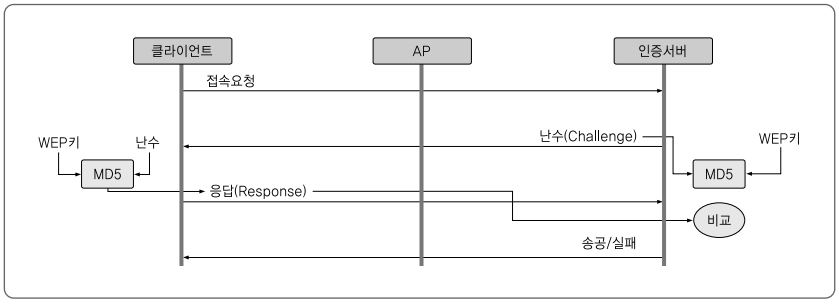
코드필드의 값에 따라 지원되는 EAP 인증 프로토콜이 결정되며, EAP를 이용

하는 사용자 인증방법으로는 WAP-MD5, EAP-TLS, EAP-TTLS, PEAP 등이 있다.

RADIUS 서버를 무선랜에 적용하는 경우, 추가적으로 RADIUS 서버에 대한 보안도 같이 고려되어야 한다. 무선랜을 통한 RADIUS 서버로의 접근 제한을 통해, 일반 무선 클라이언트 등이 접속할 수 없도록 제한하고, 무선랜의 중요도에 따라 RADIUS 서버의 이중화 등도 고려하도록 한다. 다음은 EAP를 이용한 단말의 인증에 있어서 많이 사용되는 EAP-MD5, EAP-TLS에 대한 구성 및 설정을 보여주고 있다.

(1) EAP-MD5의 구성

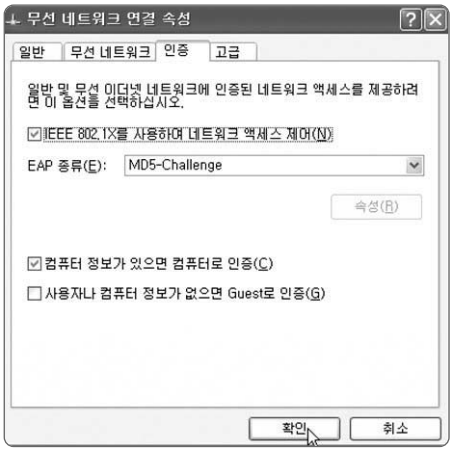
EAP-MD5의 구성은 〈그림 52〉와 같다. 이는 많은 인터넷 뱅킹에서 사용하고 있는 보안카드를 떠올리면 이해가 쉽다. 즉, 인증서버가 전송한 난수를 무선랜카드는 WEP 키를 이용해서 해쉬값을 구해서 전송하게 되고, 인증서버는 자신이 구한 값과 클라이언트가 전송한 값을 비교하여 동일하면 인증에 성공한 것으로 간주한다. 따라서 EAP-MD5를 사용하기 위해서는 반드시 WEP 키가 설정되어 있어야 한다.



[그림 52]
EAP-MD5

클라이언트에서 EAP-MD5를 설정하는 방법은 〈그림 53〉과 같다.

[그림 53] 윈도우 XP에서 EAP-MD5 사용

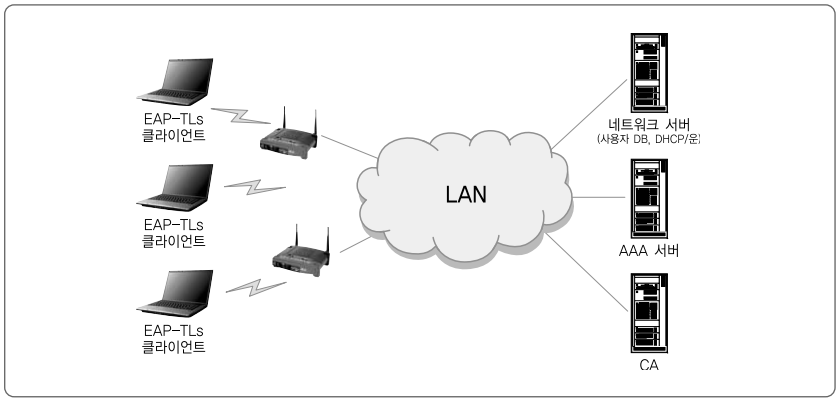


(2) EAP-TLS의 구성

EAP-MD5의 경우는 설정이 비교적 간단한 편이지만 EAL-TLS의 경우는 좀 더 복잡하다. 우선 EAP-TLS를 이용하기 위해서는 다음과 같은 구성요소가 모두 갖춰져야 한다.

- AP : EAP-TLS를 지원하는 AP
- 인증서버 : EAP-TLS를 지원하는 AAA (Authentication, Authorization, Accounting) / RADIUS 서버
- 클라이언트 : 윈도우 XP 및 EAP-TLS를 지원하는 무선랜카드
- CA 시스템 : 인증서 발급을 위한 CA 시스템

[그림 54] EAP-TLS 구성 요소

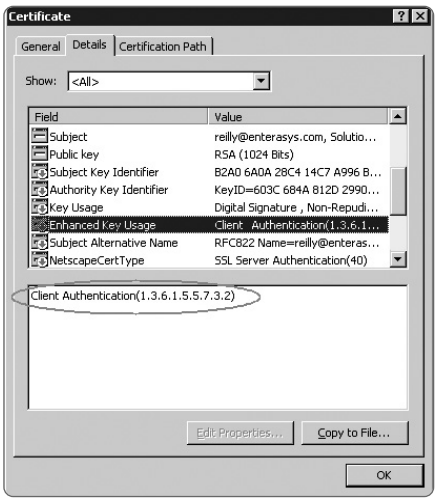


이와 같은 EAP-TLS 관련 시스템들은 〈그림 54〉와 같이 구성된다. 〈그림 54〉에서는 일반적인 환경을 고려하여 네트워크 관련 서버도 추가하였다.

(3) EAP-TLS 인증서

EAP-TLS는 인증서 기반의 상호인증을 제공하기 때문에 인증서버와 클라이언트는 모두 인증서를 소지하고 있어야 한다. 우선, 무선랜에서 사용되기 위해서 클라이언트 인증서는 다음과 같은 요구사항을 만족시켜야 한다.

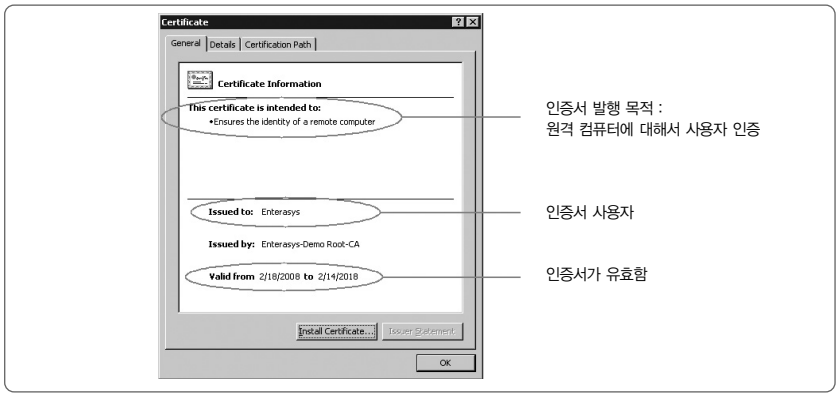
- 인증서는 X.509 v3 규격을 따라야 한다(이는 일반적으로 인터넷 뱅킹 등에서 사용되는 인증서와 동일하다).
- 〈그림 55〉와 같이 Enhanced Key Usage 필드가 반드시 사용되어야 하며, 이 필드의 값은 Client Authentication 이어야 한다.
- 발급대상(Subject name) 필드는 user ID와 동일해야 한다.



[그림 55] 무선랜 사용자 인증을 위한 사용자 인증서

클라이언트 인증서가 정상적이라면 〈그림 56〉과 같이 유효한 것으로 검증되게 된다. 이 때 클라이언트 인증서의 발행 목적이 원격 컴퓨터에서 자신의 신원을 인증하는 것임을 눈여겨 볼 필요가 있다.

[그림 56] 클라이언트 인증서 유효성 검사

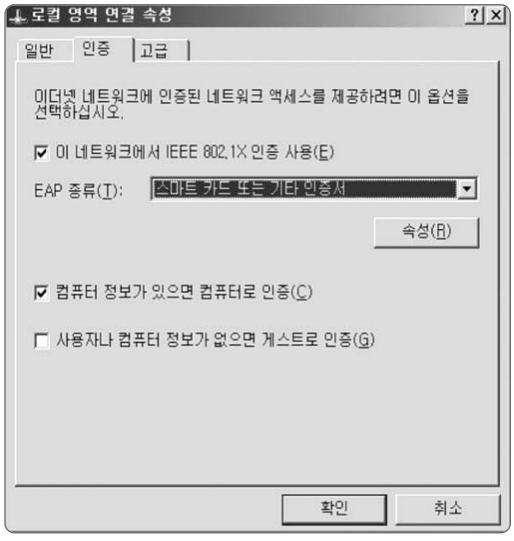


EAP-TLS 환경에서는 인증서버에서 사용자를 인증하기도 하지만 사용자 역시 인증서버를 인증해야 한다. 따라서 인증서버 역시 적절한 인증서를 소지하고 있어야 한다. 서버 인증서 역시 다음과 같은 사항을 만족시켜야 한다.

- 인증서는 X.509 v3 규격을 따라야 한다.
- Enhanced Key Usage 필드가 반드시 사용되어야 하며, 이 필드의 값은 Server Authentication 이어야 한다.

사용자 및 서버 인증서의 설치에 대한 자세한 설명은 생략하기로 하고,

[그림 57] EAP-TLS 설정



Windows XP에서 EAP-TLS를 사용하기 위해 필요한 설정에 대해서 살펴보면 다음과 같다.

EAP-MD5의 경우와 마찬가지로 네트워크 설정 → 무선 네트워크 → 인증 창을 띄운다(〈그림 57〉 참조).

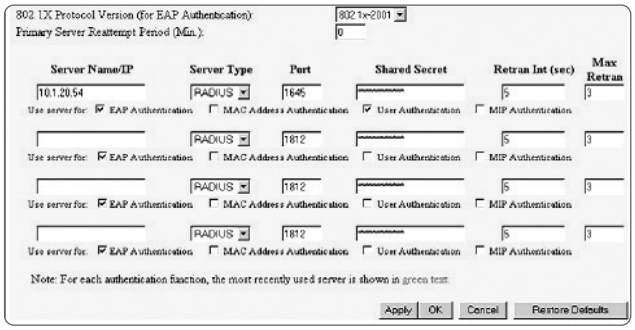
〈그림 57〉에서 보는 바와 같이 EAP-TLS 사용을 위해서 IEEE 802.1x를 사용하도록 체크한다. 그리고 EAP Type는 "스마트카드 또는 기타 인증서"를 선택한다. 그 후 속성 버튼을 클릭하면 〈그림 57〉과 같이 인증서와 관련된 설정을 할 수 있는 창으로 이동한다.

이때, "내 스마트 카드사용"은 클라이언트의 인증서가 스마트카드에 저장되어 있을 경우에 사용한다. "이 컴퓨터의 인증서 사용"은 인증서가 컴퓨터의 하드디스크에 저장되어 있을 경우에 사용한다. 〈그림 58〉을 통해서 서버 인증서를 검증함을 알 수 있다. 즉, 클라이언트 인증뿐만 아니라 서버 인증도 수행한다. 그리고 최상위 CA를 설정하도록 되어 있음을 알 수 있다.

[그림 58] AP에서 EAP 설정

〈그림 59〉는 AP에서 EAP를 설정하는 관리 페이지이다. 〈그림 59〉와 같이 AP에서는 인증에 사용될 RADIUS 서버의 IP 주소 및 포트를 설정할 수 있다. 이때, 여러 개의 RADIUS 서버를 설정하는 것도 가능하다.

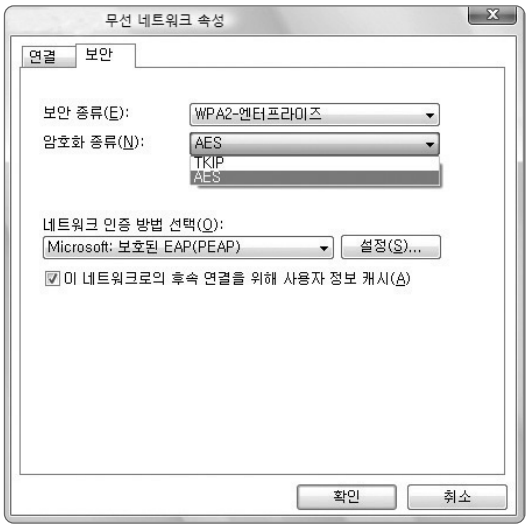
[그림 59] EAP-Type 속성



나. 전송데이터의 암호화

일정 수준이상의 기업 환경에서 사용 권장되는 무선 전송데이터의 암호화 방식은 WPA-엔터프라이즈이며, 여기서는 TKIP 또는 AES 기반의 CCMP를 사용하여 암호화 및 복호화를 수행한다. WPA2-엔터프라이즈 환경에서의 암호화 설정은 〈그림 60〉와 같다.

[그림 60] WPA2-엔터프라이즈 암호화 설정



TKIP의 경우, WEP의 취약점을 보안하는 암호방식으로, WEP과는 달리 고정된 암호화 key를 사용하는 대신 EAP에에 의한 사용자 인증결과로부터, 무선 채널 보호용 공유 비밀키를 동적으로 생성하여 패킷의 암호화를 진행한다. TKIP의 암호문은 WEP 암호화 알고리즘을 적용하였을 때 보다 초기벡터 값을 확장하고

키 mixing 함수 사용을 통해 암호키의 생성과정을 보완하였으며, 사용자 전송 데이터의 무결성을 강화하였다. TKIP에 대한 자세한 설명은 3장에 기술되어 있다.

TKIP는 기존 하드웨어를 사용하면서 전송데이터를 암호화하기 위한 방법이었다면, CCMP는 이미 검증된 암호화 기법인 AES를 기반으로 무선랜 환경의 데이터에 대한 비밀성과 무결성을 보장하기 위한 방법이다. CCMP는 IEEE 802.11i의 표준을 따르는 전송데이터의 암호화 기법으로서, TKIP보다 안전하다고 여겨지며, 권장되는 설정이다. 하지만, 현재 구입한 하드웨어가 이를 지원해 주지 않는 다면 이를 활용하는 것이 불가능하다. CCMP에 대해서는 3장에 기술되어 있다.

2. 개인 및 SOHO 사업자의 무선랜 보안

가. 사설망을 통한 인증 및 암호화

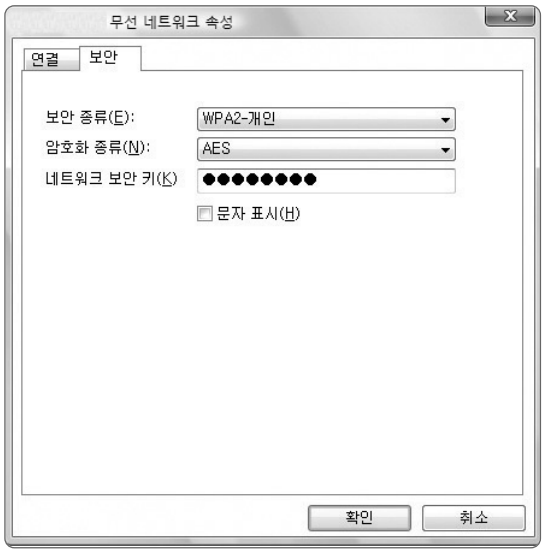
WPA의 한 형태인 WPA-개인은 개인사용자를 위한 WPA 기술의 적용이고, 앞서 설명한 WPA-엔터프라이즈는 일정 수준 이상의 기업 환경에서 사용할 수 있는 기술이다. 이 두 접근의 가장 큰 차이점은 인증서버의 사용여부로서, 기업의 유선랜 환경과 연동되어 중요한 정보들을 교환하는 상황이 발생하는 경우 WPA-엔터프라이즈가 권장되지만, 인증서버를 두기 어려운 상황에서는 WPA-개인을 사용하게 된다. WPA-개인의 PSK는 무선 단말과 AP가 나누어 갖는 키로서, 이를 통해 단말인증을 수행하게 된다. 무선 AP와 무선 단말은 공통으로 설정한 비밀키(PSK)를 가지고 4 웨이 핸드쉐이킹 절차를 통해 무선랜에 접속할 수 있다.

무선 데이터 암호화에는 안전성이 검증된 CCMP가 권장되며, CCMP의 경우에는 128비트 블록키를 사용하는 CCM(Counter Mode Encryption with CBC-MAC)모드의 AES 블록 암호 방식을 사용한다. WPA2-개인 환경에서의 암호화 설정은 〈그림 61〉와 같다.

이러한 WPA2 방식을 사용하기 위해서는 무선 AP와 무선 단말기 모두에서 WPA2를 지원하여야만 해당 기능을 사용할 수 있다. 현재 WPA2-PSK의 경우

앞서 언급한 바와 같이 초기 무선랜 인증 시 진행되는 4 웨이 핸드쉐이킹 단계의 무선 패킷수집을 통해 비밀키 유추가 가능한 문제가 있다. 이를 보완하기 위해서는 비밀키는 특수문자를 포함한 임의의 문자를 사용하여 최대한의 자리수를 사용하도록 한다.

[그림 61] WPA2-개인 암호화 설정



나. 무선랜 사업자의 서비스 이용

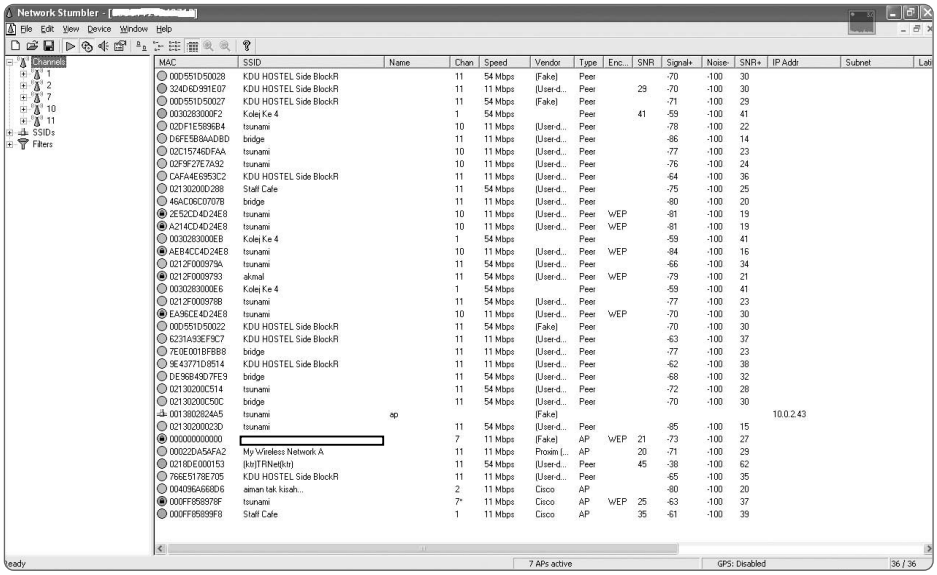
국내 무선 인터넷 서비스 제공업체가 제공하는 인증서버를 통한 단말 인증기능을 사용하는 것도 안전한 무선랜 운영을 위한 방법이라고 할 수 있다.

3. 무선 AP의 물리적/관리적 보안

가. SSID Broadcast 금지

SSID(Service Set Identifier)는 무선 AP를 이용해 구성되는 무선 네트워크를 구별하는 식별자로서 다수의 무선 네트워크가 존재하는 경우, 무선 클라이언트가 접속할 네트워크를 구분하는 역할을 하게 된다. 대부분의 무선 AP는 무선 클라이언트가 무선 네트워크의 존재를 인식할 수 있도록 SSID를 broadcast 하도록 설

정되어 있는 것이 일반적이다.



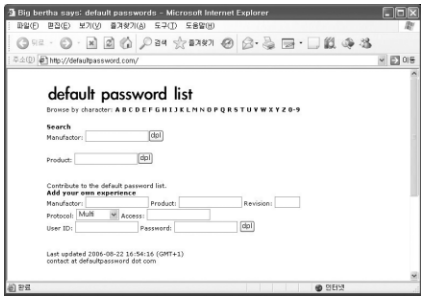
[그림 62]
SSID Br●adcas
기능의 비활성화를
적용한 무선랜

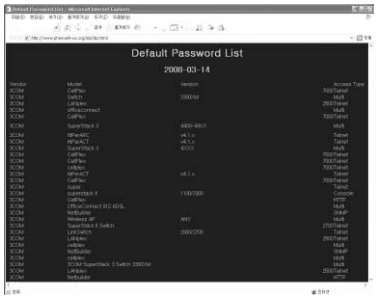
하지만, SSID 값의 broadcast로 인해 공격자는 공격대상이 되는 무선 네트워크의 존재를 쉽게 인식할 수 있게 된다. 물론 무선 데이터 패킷의 캡처를 통해서도 무선 네트워크의 존재를 알 수 있으나, SSID broadcast를 사용하지 않으므로 보안수준을 향상시킬 수 있다.

나. 무선 AP의 Default Passw●rd 변경

Default Password의 사용은 무선 AP에 국한되는 문제는 아닐 수 있다.기본적으로 대부분의 네트워크 제품은 공장 출하 시 설정되는 Default Password를 가지고 있고, 특히 관리상의 편의를 위해 기본 설정되어 있는 Password를 사용하는 경우가 종종 확인되고 있다. 하지만 이는 암호를 설정하지 않은 보안수준으로서, 반드시 일반적으로 통용되고 있는 수준의 암호 설정을 통해 무선 AP를 관리 · 운영하도록 한다.

[그림 63] 검색엔진을 통해 확인되는 디폴트 패스워드 리스트





■■■ 안전한 무선 AP 관리암호의 사용 예

1) 8자이상의 암호 사용
2) 숫자 및 영문자, 특수문자 혼용하여 사용
3) 일반 단어가 아닌 한글-영타 암호(예:암호-dkagh)의 사용
4) 주기적인 암호의 변경

다. 무선 AP의 물리적 접근제한

일반 네트워크 장비의 경우, 외부에 노출되지 않는 경우가 많아 네트워크 장비에 대한 물리적 보안은 초기 구축 시 고려하지 않는 경우가 많다. 하지만, 무선 AP의 경우, 서비스를 위해 외부에 노출될 수밖에 없어 물리적인 접근제한이 필요하게 된다.

또한, 무선 AP의 경우, 장비의 설정을 초기화로 돌리는 "Reset 스위치"를 가지고 있는 경우가 많아, 장비의 물리적인 보안이 더욱 중요하며, 장비가 Reset이 되는 경우, 기존 운영되던 무선 서비스의 중지는 물론 장비 설정의 초기화로 인해 보안상의 문제도 같이 발생하게 된다.

[그림 64] 무선 AP의 Reset 버튼

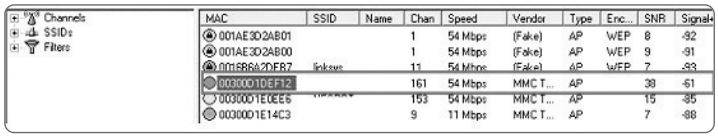
따라서, 무선 AP는 외부에 노출된 형태로 설치되더라도 별도의 수납공간 형태의 분리공간에 설치하고, 추가로 잠금장치를 설치하여 외부의 비인가자의 접근을 차단하도록 한다.

제3절 무선 인터넷 서비스 사용자 보안 권고

1. 유료 무선 인터넷 서비스

국내 ISP에서 제공 중인 유료 무선 인터넷 서비스는 가정은 물론 사람이 많이 모이는 공공장소와 커피숍 등에서 널리 제공되고 있다.

현재 국내에서 제공되고 있는 유료 무선 인터넷 서비스는 사용자 암호와 무선 전송데이터에 대한 암호화는 적용되고 있으나, 사용자 계정에 대해서는 암호화를 하지 않은 채 전송하고 있으며, 구형장비가 사용 중인 일부 지역에서는 데이터에 대한 암호화도 적용되지 않고 있어 개인정보가 외부로 노출될 가능성이 존재하고 있다.



[그림 65] 암호화 적용이 되지 않은 유료 인터넷 서비스용 무선 AP

〈그림 65〉에 표시된 영역의 경우, 무선 네트워크를 통해 전송되는 데이터는 모두 평문(Plain text) 형태로 전송되게 되어, 사용자가 입력하는 모든 정보는 무선 전파를 수신할 수 있는 모든 사용자에게 노출되게 된다.

〈그림 66〉은 평문으로 전송되는 무선랜 환경에서 E-Mail을 전송했을 경우에 무선 패킷을 캡처하여 본 내용이다. 위의 그림에서 보이는 메일의 본문 내용이 실제 캡처한 무선 패킷에서 그대로 노출되는 것을 볼 수 있다. 무선 인터넷 서비스에서 별도의 무선 전송 데이터에 대한 암호화를 적용하지 않았기 때문에 발생하

[그림 66] 유료 무선 인터넷 서비스를 이용한 메일 전송 데이터 캡처 화면

는 문제로서, 대부분의 웹 사이트에서도 일반적으로 웹 컨텐츠 전송 시 암호화를 하지 않는 경우가 대부분이므로 메일 내용은 물론 로그인시의 개인정보의 노출도 마찬가지로 발생하게 된다.

이러한 문제점의 해결책은 현재와 같이 무선 인터넷 서비스 업체에서 무선 데이터의 암호화를 제공하지 않는 경우에는 사용자 개인이 해결할 수 있는 방법은 없으며, 무선 인터넷 서비스 이용 시에는 계정정보 등의 민감한 정보는 가능한 입력하지 않는 것이 필요하다.

2. 공공장소 무료 무선 인터넷 서비스

무료 무선 인터넷 서비스를 제공하는 은행 및 커피숍 등이 점차 늘어가고 있지만, 대부분 간단한 인증만을 통해 무선 인터넷에 접속할 수 있어, 별도의 유료 인터넷 서비스에 가입을 하지 않은 사용자도 무선 단말기를 통해 쉽게 인터넷에 접속할 수 있다.

이 경우의 문제점은 이러한 무료 인터넷 서비스는 대부분 별도의 인증절차 없이도 무선 네트워크로의 참여가 가능하여, 불법 AP 등을 이용한 무선랜 사용자가 입력하는 개인정보의 유출이나 단순한 무선 전송데이터의 캡쳐만으로도 정보유출이 가능하다는데 있다. 이는 유료 무선 인터넷 서비스에서와 마찬가지인 문제점으로 근본적인 무선랜의 보안이 이루어지지 않은 경우에는 동일하게 발생하는 문제점이다.

또, WEP 암호화 방식을 적용한 무선랜 환경 하의 무료 인터넷 서비스의 경우,

일반적으로 다량의 무선 전송 데이터를 수집한 후 크랙이 가능한 것으로 알려져 있으나 실제 인터넷 상에서는 공격자가 악성 패킷을 사용자 무선 단말기로 전송하여 발생되는 응답 패킷의 수집을 통해서도 공격이 가능하며, 이러한 방법을 이용하는 공격 툴이 공개되어 있는 상태이다.

이와 같은 환경 하에서 인터넷에 접속하여 사용자 아이디, 암호 등의 정보를 입력할 경우, 해당 정보가 외부의 다른 사용자에게 노출될 수 있으므로, 가능한 간단한 웹 서핑 등의 용도로만 사용을 하도록 한다.

또한, 무료 인터넷 서비스를 제공하는 해당 업체에서는 가능한 WPA 이상의 무선 인증방식을 사용하여, 고객이 보다 안전한 환경에서 인터넷을 사용할 수 있도록 무선랜의 설정을 유지하여야 한다.

무 선 랜 보 안 가 이 드

제5장 결 론

Korea Information Security Agency

제5장 결 론

무선랜은 이미 현대사회의 여러 분야에서 사용되고 있고, 이는 향상된 전송속도를 제공하는 새로운 무선 표준의 상용화와 더불어 더욱 다양한 분야에서 활용되어 유선랜의 상당부분을 대체할 것으로 예상되고 있다.

이에 따라 무선랜의 보안은 더욱 중요한 부분을 차지하게 될 것으로 예상되지만, 무선랜의 사용자나 관리자의 인식은 여전히 부족한 상태로, 여러 조사 자료나 반복되는 사고의 발생에서도 그러한 사실을 확인할 수 있다.

안전한 무선랜의 사용을 위해서는 무선랜의 구축에서부터 보안이 고려되어야 하며, 항상 새로운 취약점이 나오는 현실에 맞춰 꾸준히 보완되고 관리되어야 한다. 또한 사용자나 관리자의 인식변화를 위한 주기적인 교육과 관련 시스템의 보안 수준 유지를 위해 정기적인 점검이 수반되어야 한다.

무선랜은 서비스의 특성 상, 무선 장비들에 대한 물리적인 보안이 필히 강구되어야 한다. 무방비로 노출된 무선 AP는 외부로부터의 여러 형태의 공격에 취약하며, 사용자의 무선 단말기는 분실이나 도용 등으로 인해 중요 정보의 유출 가능성이 높다. 또한 사용되는 무선 장비들이 어떠한 무선랜 표준을 지원하는지 파악하고, 향후 사용 환경의 변화와 수요를 예측하여 적절한 장비를 도입하는 것이 필요하다.

또한, 무선랜의 사용 환경에 맞는 적절한 인증과 암호화 설정을 통한 보안강화가 중요하다. 무선랜 공격의 목적은 대부분 불법적인 무선랜의 이용과 무선 전송 데이터의 유출이므로 불특정 다수에게 무선신호가 전달되는 무선랜 서비스의 특성 상 사용자 인증과 무선 전송 데이터의 암호화 설정은 무선랜 보안에 있어 가장 중요한 부분이라 할 수 있다.

이러한 무선랜 운영 시 필요한 고려사항과 유의사항들은 모두 하나의 운영정책

을 통해 일괄적인 기준을 가지고 관리되어야 한다. 본 가이드에서는 무선랜에 대한 기본적인 지식부터 무선랜의 보안정책, 취약점과 대응방안에 대해 다뤄, 사용자와 관리자의 무선랜에 대한 이해를 돕고자 하였다.

안전한 무선랜의 운영을 위해 사용자와 관리자 모두 무선랜의 취약점과 사용방법에 대해 고민하고, 무선랜 기술이 기반이 될 것으로 예상되는 유비쿼터스 환경에서는 현재보다 편리하고 안전한 무선랜의 구축과 활용이 가능하기를 바란다.

무 선 랜 보 안 가 이 드

부 록

Korea Information Security Agency

부록 1 TTA 무선랜 정보보호 체크리스트

■ 기업 무선랜 관리자용 정보보호 체크리스트

무선랜 관리자용 정보보호 체크리스트	중요도	적용 용이성	확인
○ 무선랜 사용자 현황을 파악 하였는가? – 사내 무선랜 사용자 명단, 사용자별 단말, 무선랜 카드종류, MAC주소, IP주소 등을 파악한다.	중요	예	
○ 장비 운영 현황을 파악 하였는가? – 장비명, 제조회사, 구매일자, 운영 프로그램 버전, 설치장소 등 파악한다.	중요	예	
○ 무선랜 운영 소프트웨어 현황을 파악 하였는가? – 무선랜 장비에 설치되어 운영되고 있는 소프트웨어명, 종류, 버전 등을 파악하고 매뉴얼을 확보한다.	선택	아니오	
○ 무선랜 장비를 보호하고 있는가? – AP 도난 및 공격자의 접근으로부터 보호할 수 있는 물리적 보안대책 확보한다. – AP 접근방지를 위한 보호케이스 설치, 데이터 라인, 파워 라인 등의 보호케이스 설치한다. – 인증서버 운영시, 공격자의 물리적 접근을 방지하기 위한 물리적 접근 방지 방법 적용한다.	선택	예	
○ AP 관리자 모드 접속 암호변경 하였는가? – AP의 설정값을 변경할 수 있는 관리자 모드의 접속 암호를 주기적으로 변경하여 사용한다.	중요	예	
○ 사내 무선랜의 무분별한 사용을 방지하기 위해서 무선랜 사용에 관한 보안 정책을 정의하고 있는가? – 사용자, 사용 가능 시간 및 프로토콜 등을 정의하고 사내 무선랜 사용자에게 준수하도록 한다. – 사내 장비의 분실 및 정보 유출을 방지하기 위해서, 사내 장비의 반출절차를 마련하여 준수한다. – 사내에 비인가 장비의 운영을 막기 위해, 외부 장비의 사내 반입시 보안상 적절한 절차를 마련해야 한다. – 장비의 도난 및 훼손시에는 관리자에게 보고하도록 하는 처리 절차를 마련하여야 한다.	선택	아니오	
○ 무선랜 장비를 반출/폐기 또는 도난 단말의 발견시 적절한 조치를 취하였는가? – 사내 무선랜 장비를 폐기할 때 장비에 설정된 값들을 모두 제거하여 주요정보 유출을 방지한다. – 사내 무선랜 장비의 반출/도난 시에 암호키를 변경하였는가?	중요	예	
○ SSID를 새로운 값으로 변경하였는가? – SSID를 AP 초기설정 값을 사용하는 것은, 공격자의 공격대상이 될 수 있고, AP별 초기 설정값은 이미 알려져 있어 매우 위험하다.	중요	예	

무선랜 관리자용 정보보호 체크리스트	중요도	적용 용이성	확인
○ SSID를 숨김 모드로 설정하였는가? – SSID가 공개되어 공격자가 접속시도를 줄이기 위해 SSID를 숨김 모드로 운영한다.	선택	예	
○ AP 채널이 인접 AP와 중복되지 않도록 설정하여 운영하고 있는가? – 회사에서 운영하는 AP나 인근 AP가 전파 간섭으로 인해 데이터 전송율이 저하되지 않도록 채널을 설정하여 운영한다.	선택	예	
○ 사내 무선랜 서비스 이용가능 영역에서만 회사의 AP전파를 수신할 수 있도록, AP 전파 출력을 조절하였는가? – 사내에서 운영하는 AP의 전파가 인가된 영역(회사내부 등)을 이월하여 비인가 영역에서도 전파 송수신이 가능하게 되면, 이월되는 전파를 이용하여 공격자가 접속시도, 데이터 도청 등의 공격을 수행할 수 있다.	중요	예	
○ 무선랜을 위한 IP대역을 따로 마련하고 있는가? – 무선랜에서 사용하는 IP 대역을 구분하여 사용하여 무선랜을 통한 침해사고 발생 시 사고 경로 분석이 용이하도록 한다.	선택	예	
○ 무선랜 사용자들이 고정 IP를 사용하도록 하고 있는가? – 무선랜 접속 시 AP에서 IP를 자동으로 부여하는 경우(DHCP를 사용하는 경우)가 있다. 이 경우에는 공격자의 접속 요청시에도 사내 IP를 부여할 수 있어 보안상 위험하다.	선택	예	
○ 사내 무선랜 데이터의 도청 및 감청을 방지하기 위해서 AP에서 제공하는 데이터 암호화 기능을 적용하고 있는가? – 무선 전파를 통하여 전송되는 데이터를 보호하기 위해서 데이터 암호화를 적용하여야 한다.	중요	예	
○ 사내 AP에 제공하는 사용자 인증을 적용하고 있는가? – 무선랜 공격자의 접속을 방지하기 위해서 사용자 인증방식을 적용한다.	중요	예	
○ 사용자 인증방식의 안정도는 높은가? – 사용자의 정보를 보호하고, 안전한 인증을 수행하기 위해서 양방향 인증방식인 EAP-TLS이거나 인증채널을 보호하는 방식인 EAP-TTLS 등을 적용한다.	선택	아니오	
○ 암호키를 긴 값으로 설정하여 사용하고, 설정된 암호키 값을 주기적으로 변경하고 있는가? – 공격자가 무선 네트워크 구간에서 패킷을 수집하여 암호키를 크랙하지 못하도록 긴 킷값을 사용하고, 공격자에게 암호키가 노출되지 않도록 키 값을 주기적으로 변경한다.	중요	예	
○ 안전한 무선랜 운영을 위해 Firewall, VPN 장비 및 바이러스 월 등의 보안 솔루션을 사용하고 있는가? – 무선랜을 통한 공격자의 해킹 및 바이러스 유포등을 방지하기 위해서 보안 솔루션을 설치 운영하여야 한다.	선택	아니오	
○ 무선랜 네트워크를 모니터링할 수 있는 장비들을 활용하여 무선랜 운용 상황을 주기적으로 확인하고 있는가? – 무선랜 운용 상황이 실시간으로 모니터링 되고, 침입탐지 및 대응 시스템과 연계된다면 더욱더 안전하게 무선랜을 운용할 수 있다.	선택	아니오	

무선랜 관리자용 정보보호 체크리스트	중요도	적용의 용이성	확인
○ 사내 무선랜 환경에 대해 주기적인 보안점검을 수행하는가? (다음 사항을 중점적으로 주기적 점검) • 무선랜 장비가 정상적으로 동작하고 있는가? • AP 보안설정의 불법적인 변경은 없었는가? • 사내 무선랜에 적용하고 있는 암호화 메커니즘은 정상적으로 동작하고 있는가? • 사용자 인증은 정상적으로 동작하고 있는가? • 보안솔루션들은 정상적으로 동작하고 있는가? • 무선랜 채널의 중복은 없는가? • 사내 AP의 전파 강도가 적절한가? • 사내 비인가 AP의 운영은 없는가? • 회사 일부 영역이 외부 AP의 서비스 영역으로 포함 곳이 발생하였다면, 무선랜 사용자들은 그 사실을 인지하고 있는가? • 소프트웨어 업그레이드 및 보안패치가 안된 것은 없는가?	중요	아니오	
○ 사내 주요정보가 외부인에게 유출되는 것을 방지하고 있는가? – 용역업체 직원, 퇴사자, 방문자 등에 암호키, 인증정보 등의 주요 정보가 노출되지 않도록 한다.	중요	예	
○ 사내 무선랜 사용자를 대상으로 무선랜 보안교육을 실시하고 있는가? – 사내 무선랜 사용자에게 무선랜 보안 취약성, 공격유형, 보안설정 방법 등을 설명한다. – 사내 무선랜 운영환경을 설명하고, 사내에 적용된 무선랜 보안기능 사용법을 설명한다.	중요	예	
○ 무선랜 단말이 네트워크 공유 폴더를 사용하고 있는가? – 노트북 형태의 무선랜 단말에 공유 폴더 사용을 제한하되, 불가피한 경우는 쓰기 금지 모드와 패스워드를 사ㅛㅇ하고 사용하지 않을 경우는 반드시 공유폴더를 해제하여야 한다.	중요	예	
○ 무선랜 장비 및 단말의 운영체제 및 응용 프로그램을 주기적으로 패치하고 있는가? – 장비 소프트웨어의 취약점으로 인한 공격자의 공격을 방지하기 위해서 최신 프로그램으로 업그레이드하거나 패치를 해야 한다.	중요	예	
○ 사용자 인증, 데이터 암호화 메커니즘을 가장 최신 버전을 사용하고 있는가? 또한 관련 소프트웨어를 업그레이드하거나 패치 하였는가? – 사용자 인증, 데이터 암호화 메커니즘 소프트웨어장비 운영 프로그램의 취약점으로 인한 공격자의 공격을 방지하기 위해서 최신 프로그램으로 업그레이드하거나 패치를 해야 한다.	선택	아니오	

■ 무선랜 사용자용 정보보호 체크리스트

무선랜 사용자용 정보보호 체크리스트	중요도	적용의 용이성	확인
○ 무선랜 단말의 분실 및 도난을 방지하기 위해 보관을 잘하고 있는가? – 휴대성이 뛰어난 만큼 분실 위험성도 큰 단말의 분실 및 도난 등을 방지하기 위해서 보관 및 관리가 철저해야 된다.	중요	예	
○ 무선랜 단말에 로그온 암호를 적용하고 있는가? – 분실된 무선랜 단말을 공격자가 악용하여 주요 정보를 습득하거나 회사 무선랜 서비스에 접속하지 못하도록 시스템 로그온 암호를 사용한다.	중요	예	
○ 사내 무선랜 관리자가 지정한 무선랜 보안정책을 준수하고 있는가? – 회사 무선랜 보안 관리자가 정한 보안정책을 준수하여 안전한 무선랜 운영환경을 유지할 수 있도록 한다. • 무선랜 운영조건 준수 • 무선랜 장비 반출 · 입 절차 준수 • 사용자 인증 방식 적용 • 데이터 암호화 방식 적용 및 암호키 값의 주기적인 변경 • 사내 주요정보의 외부 유출 금지 • 단말 운영 프로그램 등의 업그레이드 실시 등	중요	예	
○ 무선랜 단말에 바이러스 백신 등의 보안 솔루션을 사용하고 있는가? – 무선랜 단말을 통해 바이러스 및 악성코드 유포 등을 방지하기 위해 보안 솔루션을 설치하여 운영한다.	중요	예	

■ 개인 및 SOHO 용 무선랜 정보보호 체크리스트

소호 및 가정용 무선랜 정보보호 체크리스트	중요도	적용의 용이성	확인
○ AP 특성을 파악하고 있는가? – 모델명, 제조회사, 구매일자, 운영 프로그램 버전, 등 파악한다.	중요	예	
○ AP 운영 소프트웨어 현황을 파악하고 있는가? – AP 운영 소프트웨어의 이름, 종류, 버전 등을 파악하고 매뉴얼을 확보한다.	선택	예	
○ AP의 물리적 보호하고 있는가? – AP 파워라인, 데이터 전송라인 등의 손상을 방하는 보호케이스 설치한다. – AP 리셋 버튼이 눌리지 않도록 조치한다.	선택	아니오	
○ AP 관리자 모드 접속 암호변경 하였는가? – AP 관리자 모드의 접속 암호를 변경하여 공격자가 AP 관리자 모드로 접속하는 것을 방지한다.	중요	예	
○ SSID를 새로운 값으로 변경하였는가? – SSID를 AP 초기설정 값을 사용하면, 공격자의 공격대상이 될 수 있음으로 새로운 값으로 변경한다.	중요	예	
○ SSID를 숨김 모드로 설정하였는가? – 공격자의 접속시도를 줄이기 위해 SSID를 숨김 모드로 운영한다.	선택	예	
○ AP 채널이 중복되지 않도록 설정하여 운영하고 있는가? – 집 근처에서 운영하는 AP로 인해 채널중첩이 일어나지 않도록 채널을 설정한다.	선택	예	
○ 집 밖에까지 무선랜 서비스 영역에 포함되지 않도록 AP 전파출력을 조절하였는가? – AP 전파가 집 밖으로 이월하면, 집 밖에 있는 공격자가 접속을 시도하거나 데이터를 도청 등의 공격을 수행할 수 있다.	중요	예	
○ 사용자 인증과 데이터 암호화를 위해 AP에서 제공하는 암호 기능을 사용하고 있는가? – 공격자의 접속을 방지하고, 무선 구간에서의 데이터 기밀성을 유지하기 위해 AP에서 제공하는 암호기능(WEP, TKIP 등)을 사용한다. – 암호 키 값의 크랙을 방지하기 위해서 키 값을 주기적으로 변경하도록 한다.	중요	예	
○ 무선랜 보안관련 정보를 인지하고 있는가? – 무선랜 보안 취약성, 공격유형, 보안설정 방법 등의 정보를 수집한다. – 현재 운영하고 있는 무선랜 무선랜 운영환경 및 보안 기능을 파악하고, 필요시 패치나 업그레이드를 수행한다.	중요	아니오	

부록2 WPA-PSK 무선 보안설정 가이드

■ 개 요

최근 무선랜의 사용이 급속히 증가하면서 무선 네트워크 보안에 대한 중요성 또한 크게 부각되고 있다. 무선은 물리적으로 위치되어야 하는 유선 네트워크와 달리 전파가 도달할 수 있는 반경 내에 존재하는 모든 장비들에서 공격이 가능하므로 유선에 비해 보안의 위험 요소가 더 크다고 할 수 있다.

백화점 등과 같은 무선랜을 사용하는 환경에서 보다 안전하게 사용할 수 있는 무선 네트워크 보안 방법으로는 다음과 같은 3가지 방법이 존재한다.

- ○ MAC Address Filtering
- ○ WEP (Wired Equivalent Privacy)
- ○ WPA(Wi-Fi Protected Access)-PSK (WPA2)

MAC Address 필터링은 무선 네트워크를 사용하는 장비들의 고유 MAC address를 승인하는 방법이며 누군가에 의해 MAC 번호를 변조하여 사용이 가능하다. WEP는 일정한 KEY 값으로 승인하는 방법으로 KEY값이 고정되어 있어 쉽게 노출될 수 있는 보안상 취약한 부분이 있다.

반면 WPA-PSK는 KEY 값이 고정된 WEP와 달리 KEY값을 자동으로 변경시켜 줌으로써 보안 신뢰도를 높였다. 따라서 무선 네트워크를 사용하는 환경에서는 WPA-PSK를 사용하기를 권고한다.

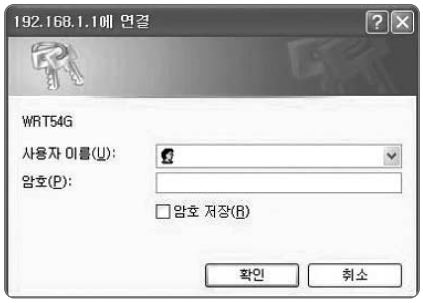
■ 무선 AP 설정 방법

1) 무선 AP admin 페이지 접속

자신의 AP 사용 설명서를 참조하여 AP를 설정할 수 있는 화면으로 접속한다. 대부분 웹을 통해 http://192.168.1.1 또는 http://192.168.11.1로 접속하도록 지원하고 있다.

2) 로그인

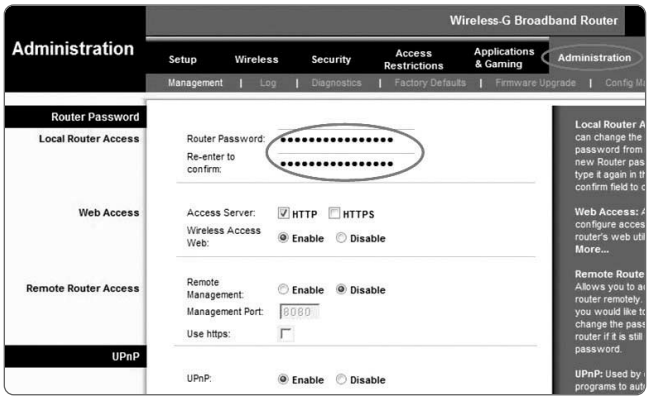
사용자 이름과 암호를 입력하여 AP 설정 화면으로 들어간다.



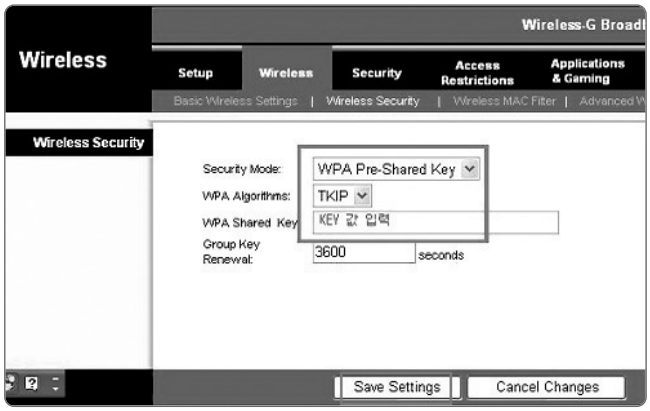
3) 초기 비밀번호 변경

먼저 초기 비밀번호를 반드시 새로운 비밀번호로 변경해야한다. 'Administration'에서 비밀번호를 입력하여 저장한다.

※ 초기 비밀번호를 그대로 사용하는 경우 비밀번호가 타인에게 노출되어 악용될 수 있으므로 반드시 변경해야 한다



4) Wireless를 선택하여 WPA-PSK 설정부터 Key 값까지 보안 설정한 후 저장 버튼을 클릭하여 설정을 완료

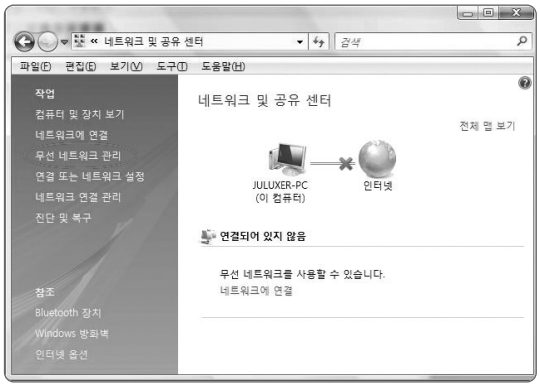


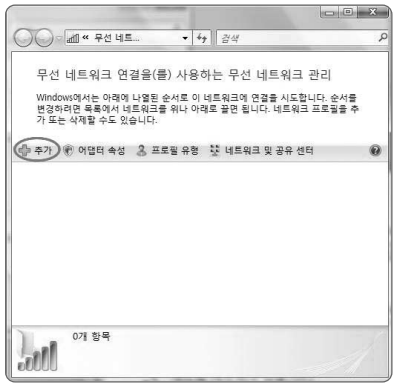
■ 무선 장비 설정 방법

○ 비스타 운영체제

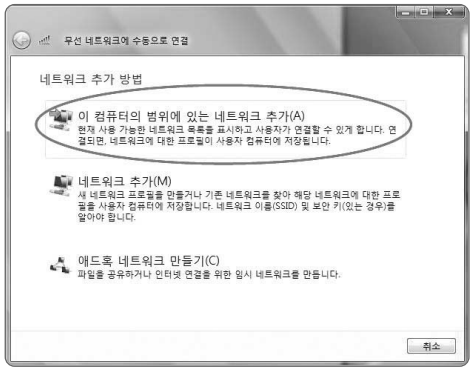
1) 시작프로그램에서 '제어판'을 클릭한 후 '네트워크 및 공유센터' 더블클릭

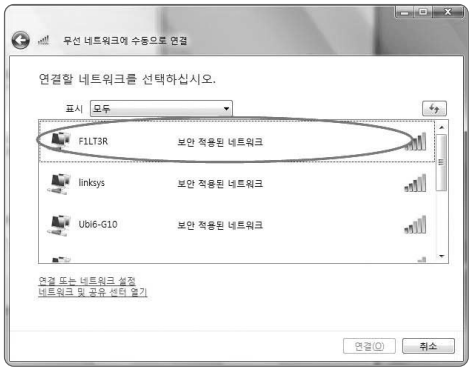
2) '무선 네트워크 관리' 클릭 한 후 '추가' 선택



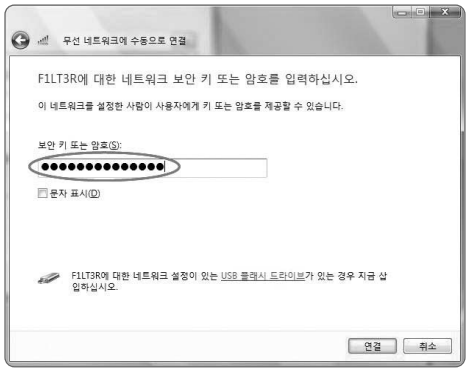


3) '이 컴퓨터의 범위에 있는 네트워크 추가'를 선택한 후 WPA로 설정된 보안적용된 네트워크(F1LT3R)를 선택



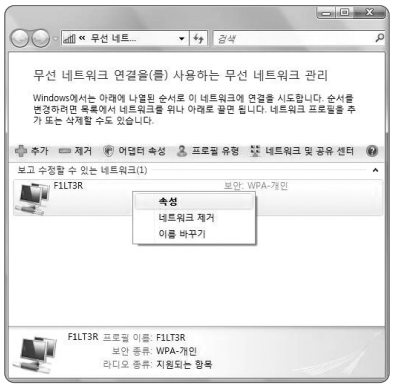


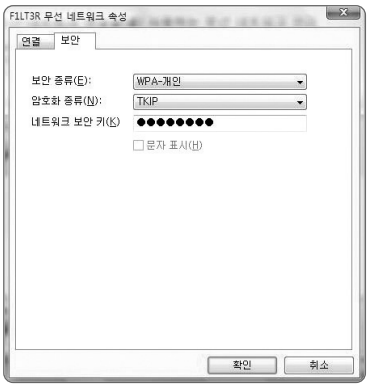
4) AP에서 설정한 KEY 입력



5) 설정 확인

무선네트워크 관리에서 해당 SSID를 선택하여 오른쪽 마우스를 클릭한 후 속성을 선택하면 WPA 설정이 되어 있음을 확인할 수 있다.

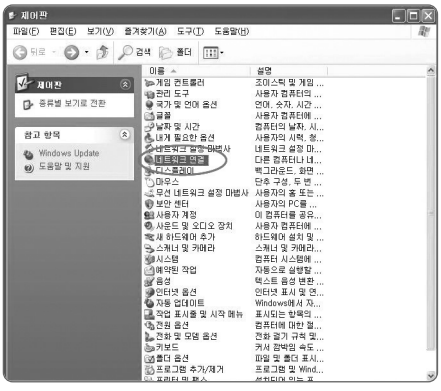




※ 비스타 운영체제에서 네트워크를 추가하는 방법은 기타 다른 환경에서도 대동소이하므로 이후부터는 보안 설정 하는 부분만 언급함

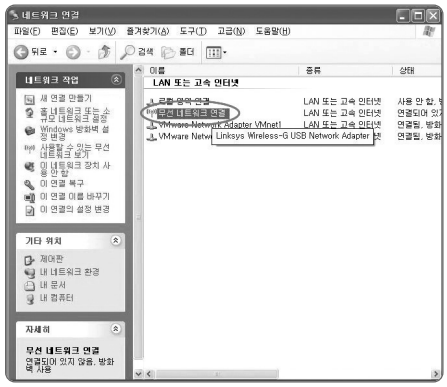
○ XP 운영체제

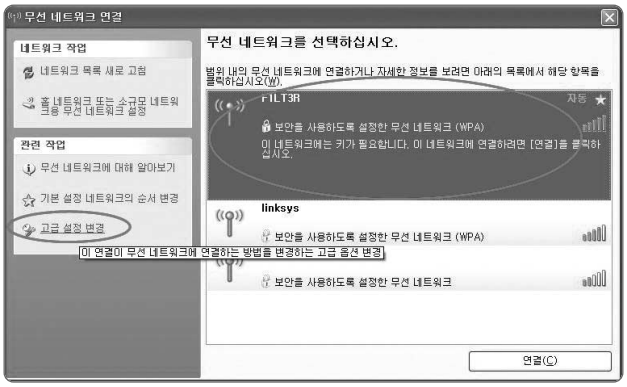
1) '시작' 프로그램에서 '제어판'을 클릭 한 후 '네트워크 연결' 더블 클릭



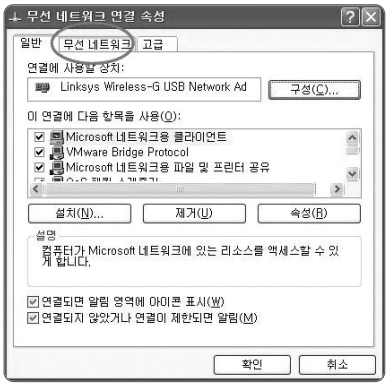
2) '무선 네터워크 연결'을 선택한 후 해당 SSID(F1LT3R)를 선택하여 '고급 설정 변경' 클릭

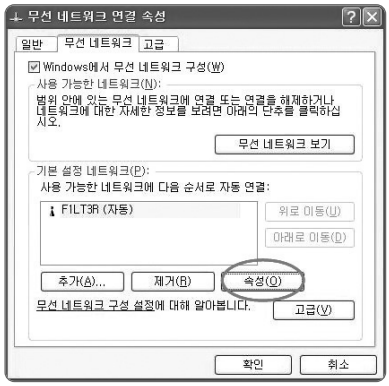
부록



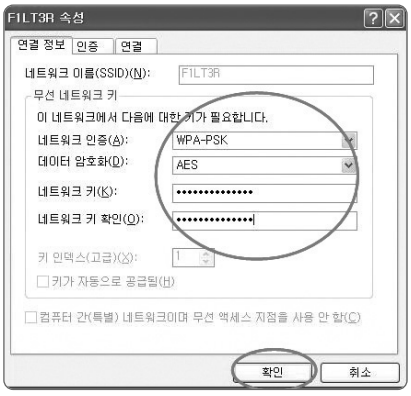


3) '무선 네트워크' 탭을 선택 한 후 해당 SSID(F1LT3R)의 '속성' 버튼을 클릭





4) WPA 설정 및 Key를 입력한 후 '확인' 버튼을 클릭하여 완료

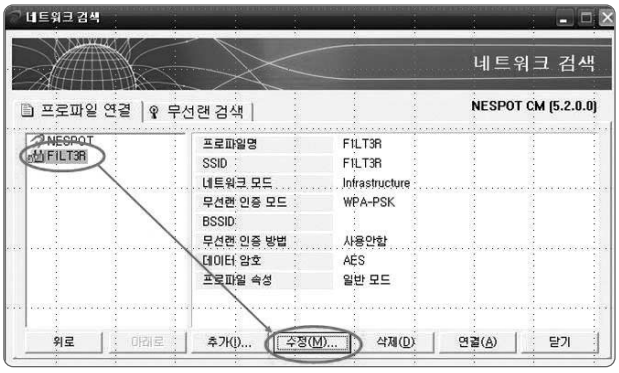


※ 보안 설정은 AP에서 설정한 값과 동일하게 설정해야 하나 이 경우 데이터 암호화 방법을 보여주기 위해 임시적으로 '데이터 암호화' 부분에서 AP 설정값인 'TKIP' 아닌 'AES'로 설정함

○ 네스팟

1) 네스팟 화면에서 네트워크 검색 클릭

2) 해당 SSID(F1LT3R)을 선택한 후 수정 버튼 클릭



3) 무선랜 인증 모드에서 WPA-PSK, TKIP 선택

4) 설정된 Key 값 입력 후 확인

○ Windows mobile 5.1 (스마트폰)

1) 설정에서 '인터넷 공유' 선택 후 '메뉴'에서 '연결 설정' 선택

2) '무선관리자' 선택 후 '메뉴'에서 'Wi-Fi 설정' 선택

3) 해당 SSID(F1LT3R)를 선택 후 WPA-PSK를 선택하고 네트워크 키까지 입력 후 완료

○ Windows mobile 5.1 (PDA)

1) '시작' 메뉴에서 '설정' 클릭 후 '연결' 탭 선택

2) 'iPAQ Wireless' 선택 후 WiFi의 '설정' 버튼 클릭

3) 해당 SSID(F1LT3R) 선택 후 '네트워크 키' 탭 클릭

4) WPA-PSK 를 선택 후 네트워크 키 값까지 입력하여 설정을 완료

■ 맺음말

네트워크 환경의 특성으로 무선네트워크 보안을 설정 할 수 없는 경우 등에는 보안성을 더욱 강화하기 위해 어플리케이션 레벨에서 소프트웨어를 사용하여 네트워크 전송 시 데이터를 암호화할 수 있다.

참 고 문 헌

[1] IEEE "Wireless Medium Access Control (MAC) and phtsical layer (PHY) specifications", IEEE Std 802.11, 1999
[2] IEEE, "Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed physical layer in the 5GHz band", IEEE Std 802.11z, 1999
[3] IEEE, "Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band", IEEE Std 802.11b, 1999
[4] IEEE, "Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Port-Based Network Access Control", IEEE Std 802.1x, 2001
[5] IEEE, "Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security", IEEE Std 802.11i, 2004
[6] "Wireless Network Security for IEEE 802.11a/b/g and Bluetooth (Draft)", NIST, 2007
[7] "The Caffe Latte Attack : How it works and How to block it", Lisa Phifer, 2007
[8] "Cafe Latte with a Free Topping of Cracked WEP - Retrieving WEP Keys From Road-Warriors", Md Sohail Ahmad, Vivek Ramachandran, 2007
[9] "A Comprehensive Review 0f 802.11 Wireless LAN Security and the Cisco wireless security suite", Cisco, 2002
[10] "Csco Wireless Mobility Findings:, Cisco, 2007
[11] "와이브로 정보보호 가이드", 한국정보보호진흥원, 2006
[12] "무선랜 안전 운영가이드", 한국정보보호진흥원, 2004
[13] "무선 LAN 보안 프로토콜", 윤종호, 교학사 2005
[14] "무선랜 보안", 김상철, 한국정보보호진흥원, 2002
[15] "무선 인터넷 이용실태조사", 한국인터넷진흥원, 2007
[16] "ISP 무선인터넷 보안점검", 한국정보보호진흥원, 2008
[17] "무선랜 보안 실태 조사 및 분석을 통한 보안 강화 방안 연구", 정현철, 2006
[18] http://www.gison.com, 지아이에스
[19] 정보보호21C, (주)인포더
[20] 무선랜 보안, 블루버드소프트
[21] NIST 기술문서, SP 800-48 Rev.1, Guide to Securing Legacy IEEE 802.11 Wireless Networks, Jul 2008
[22] NIST 기술문서, SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, Feb 2007

무선랜 보안 가이드

2008년 11월 인쇄
2008년 11월 발행

발행인 황중연
발행처 한국정보보호진흥원
서울시 송파구 중대로 135 IT벤처타워(서관)
TEL. (02)4055-114, http://www.kisa.or.kr
인쇄처 호정씨앤피(Tel. 02-2277-4718)

〈비매품〉