# ‘무선LAN’의 안전한 사용을 위한 보안대책

**NCSC-TR050019**

국가사이버안전센터
National Cyber Security Center

# '무선LAN'의 안전한 사용을 위한 보안대책

## ❶ 무선LAN 보안 기술 동향

## ❷ 무선LAN 보안 취약성

## ❸ 무선LAN 보안 대책

국가보안기술연구소 ▌최명 사, mgchoi@etri.re.kr

### 1. 서 론

1990년대 초 미국의 연방통신위원회(Federal Communications Commission: FCC)가 산업·과학·의료용(ISM : Industrial, Scientific and Medical)으로 2.4GHz의 비허가 주파수대역(Unlicensed Band)을 할당하여 특수한 장소나 이동성이 요구되는 작업환경에서 무선랜을 사용할 수 있도록 하였다. 이에 1.6Mbps의 전송속도(FHSS 변조방식 채택)를 지원하는 무선랜 제품이 출시되면서 무선랜 기술의 상용화가 이루어졌다.

우리 나라도 이미 무선랜이 본격적으로 사용되고 있으며 공항이나 호텔 로비, 도시 중심가의 식당에서 이미 무선랜 서비스가 제공되어 인터넷과 같이 생활 속의 필수 요소로 자리잡아 가고 있다. 국가·공공기관은 무선랜의 장점을 이용한 업무 혁신을 위해 무선랜 도입을 서두르고 있지만, 무선랜의 보안 취약점은 조직의 보안을 약화시키는 요인이 되고 있다.



미국에서도 무선랜을 도입하여 업무에 활용하고 있지만 보안 문제가 심각한 것으로 보고 되고 있다. 최근 미국 회계청(GAO)이 발간한 보고서에 따르면 24개의 미 연방기관 중 무선 네트워크 보안정책을 수립하지 않은 기관은 9개, 무선랜 구성설정 요구사항이 없는 기관은 13개, 보안 교육 프로그램이 없는 기관은 18개 등으로 조사되었다. 조사자는 워싱턴에 있는 6개 연방 건물에서 무선랜 신호 노출, 안전하지 않은 무선랜 구성 설정, 인가되지 않은 무선랜 장치 사용 등을 발견했고, 워싱턴 D.C.내에서 수천 개의 정부기관 네트워크를 감지하였다고 보고하고 있다.

본 글에서는 국가・공공기관의 안전한 무선랜 활용을 위해서 무선랜 보안 기술 및 보안대책 등을 3회에 걸쳐 연재한다

## 2. 무선랜 특징

무선랜 기술이 최근 들어 각광을 받고 있는 이유는 주로 설치 비용이 적고 사용의 편리성 때문이다. 무선랜 기술의 주요 장점을 살펴보면 다음과 같다.

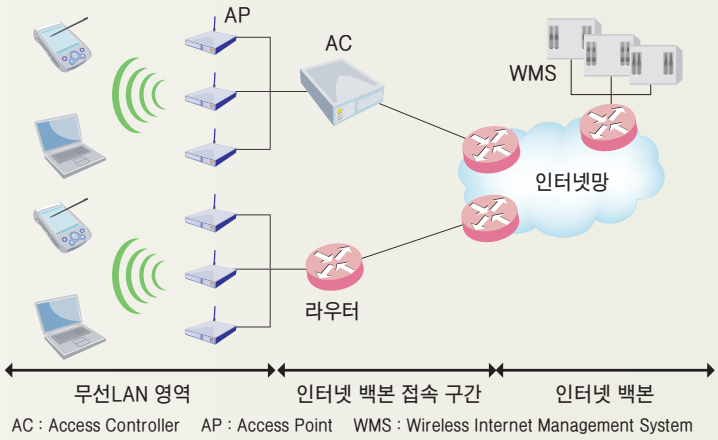
1) 이동성 : 유선 네트워크에 접속이 가능하지 않은 물리적인 상태에서 인터넷을 비롯한 네트워크 접근이 가능하며, 유선 네트워크와 비슷한 통신 품질을 보장한다.
2) 설치 용이성 : 네트워크 라인을 설치할 필요가 없이 쉽게 무선 네트워크를 설치할 수 있다.
3) 유연성 : 네트워크 사용이 불가능한 장소에서도 액세스 포인트(Access Point: AP)만 설치하면 네트워크를 사용할 수 있다.
4) 확장성 : 여러 개의 AP 설치를 통해 네트워크 사용 범위를 쉽게 확장할 수 있다.

무선랜과 인터넷의 연동 구조는 [그림 1]과 같으며 일반적으로 무선 랜카드, AP, 옥외용 랜브릿지로 구성된다.

1) 무선랜 카드 : 컴퓨터와 안테나 사이에서 인터페이스 기능을 수행하여 네트워크와 투명한 연결을 제공한다.
2) 엑세스포인트(Access Point) : 무선환경의 허브로 표준 이더넷 케이블을 통하여 유선망의 백본과 연결되어 안테나를 통하여 무선 단말기와 통신한다. AP의 반경은 20~500m이며, 1개의 AP는 기술방식과 구성 방법에 따라 수십 개의 무선단말기를 지원한다. AP는 자신의 영역에서 사용자의 움직임을 추적하며 특정 사용자의 통신을 허가 또는 거절할 수 있다. 최근에는 라우터 기능을 겸비하거나

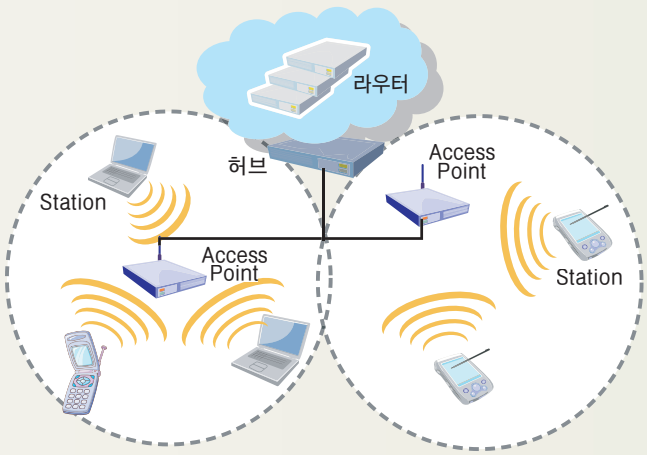
ADSL, 케이블 모뎀(Cable Modem) 등의 초고속통신망과의 연결을 지원하는 AP도 출시되고 있다.

3) 옥외용 랜브릿지(LAN Bridge) : 서로 다른 빌딩간의 랜 접속에 이용한다. 빌딩간 접속을 위해 광케이블을 도입하는 경우 비용 문제나 도로, 하천 등 물리적인 장애물이 존재할 경우 무선 랜브릿지는 경제적인 대안으로 채택될 수 있다. 무선 랜브릿지는 지향성 안테나를 이용하여 비교적 고속의 데이터 전송을 할 수 있으며, 수 Km 반경에서 사용할 수 있다. 국내의 경우 전용회선 비용을 절감하기 위한 방법으로 인접 PC방 사이에 많이 도입되고 있다.




[그림 1] 무선랜과 인터넷 연동

표준화된 무선랜인 IEEE802.11b의 구조는 인프라스트럭쳐 네트워크 (Infrastructure Network)과 애드혹(Ad-hoc) 네트워크로 나눌 수 있다. 인프라스트럭쳐 네트워크는 [그림 2]와 같이 구성된다. 인프라스트럭쳐 네트워크는 유선랜을 무선통신 영역으로 확장한 것이다. 노트북과 같은 무선 단말기를 이용해 셀(Cell)을 이동하면서 유선랜을 사용한다. 셀은 하나의 AP가 서비스를 제공할 수 있는 범위로 BSS(Basic Service Set)이라 불린다. 인프라스트럭쳐 네트



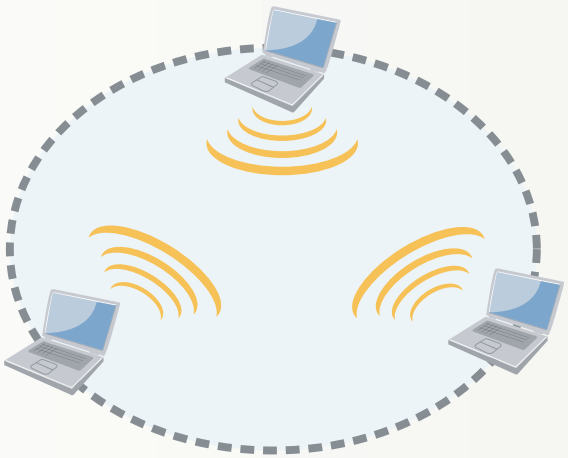

[그림 2] IEEE802.11b 인프라스트럭쳐 네트워크





워크는 이와 같은 셀들의 집합을 ESS (Extended Service Set)라고 한다. 인프라스트럭쳐 네트워크는 건물이나 대학 캠퍼스 등지에서 무선랜 서비스를 제공하는데 적합하며, 여러 개의 AP를 이용해 무선랜 서비스 범위를 확장할 수 있다.

애드혹 네트워크 구조는 [그림 3]과 같은 구조이며, 좁은 공간에서 유선랜 없이 클라이언트 간 통신에 사용된다. 애드혹 구조에서 서로 연결된 단말기들은 IBSS (Independent Basic Service Set)라고 한다.



[그림 3] 무선랜 애드혹(Ad-hoc) 구조

## 3. 무선랜 표준화 현황

1997년 6월 IEEE (Institute of Electrical and Electronic Engineers)는 표준 없이 독자적인 기술로 사용되던 FHSS (Frequency Hopping Spread Spectrum), DSSS (Direct Sequence Spread Spectrum), IR (Infrared Ray) 등의 무선 LAN 기술을 통합하고 IEEE802.11로 표준화하여 무선 LAN 기술 발전을 위한 일대 전기를 마련하였다. IEEE는 1999년에 IEEE802.11을 802.11a와 802.11b로 분리하였다. IEEE 802.11b는 고속 무선 이더넷(Higher Rate Wireless Ethernet: 일명 WiFi) 표준으로 네트워크 시장의 주류로 등장하였다. 또한, 5GHz UNII (Unlicensed National Information Infrastructure) 주파수 대역에서 OFDM (Orthogonal Frequency Division Multiplexing) 전송방식을 사용하여 최대 54 Mbps의 전송속도를 갖는 IEEE 802.11a(일명 WiFi 5) 표준 제품이 2001년 하반기부터 본격적으로 출시되었다. 802.11 표준의 특징은 [표 1]과 같다.

현재 가장 널리 사용되고 있는 무선랜 기술인 802.11b는 가장 최근에 표준화가 완료되었다. 802.11b는

| 표준안 | 개 념 |
|---|---|
| 802.11a | • 1999년 채택되었으며, 5GHz 밴드<br>• 54Mbps의 속도를 제공하며 시장에 제품이 출시된 상태 |
| 802.11b | • 1999년에 채택되었으며, 2.4GHz 밴드 이용함<br>• 11Mbps의 속도를 제공하며 기업 및 가정용 시장 대상 |
| 802.11d | • 새롭게 논의중인 표준으로 미국 이외의 규제영역에서 관련 장비 채택허용 |
| 802.11e | • 보안기능 강화, QoS 강화를 위해 MAC 지원기능 채택<br>• IP전화와 비디오와 같은 초고속 서비스에 QoS를 제공함 |
| 802.11f | • AP간의 로밍 기능을 향상시킨 표준 |
| 802.11g | • 기존의 802.11b와 비슷하나 속도 20(54)Mbps로 향상<br>• 2001년 11월에 승인 |
| 802.11i | • 무선랜의 보안기능을 대폭 향상함<br>• 채택은 보류 중 |
| 802.11h | • 기존 802.11e에 전파간섭을 방지하는 기능을 지원함 |

[표 1] IEEE802.11 무선랜의 특징

별도의 인가 없이 사용할 수 있는 좁은 대역폭을 가지고 있어 좀 더 넓은 대역폭을 가진 802.11a보다 널리 사용되고 있는 실정이다.

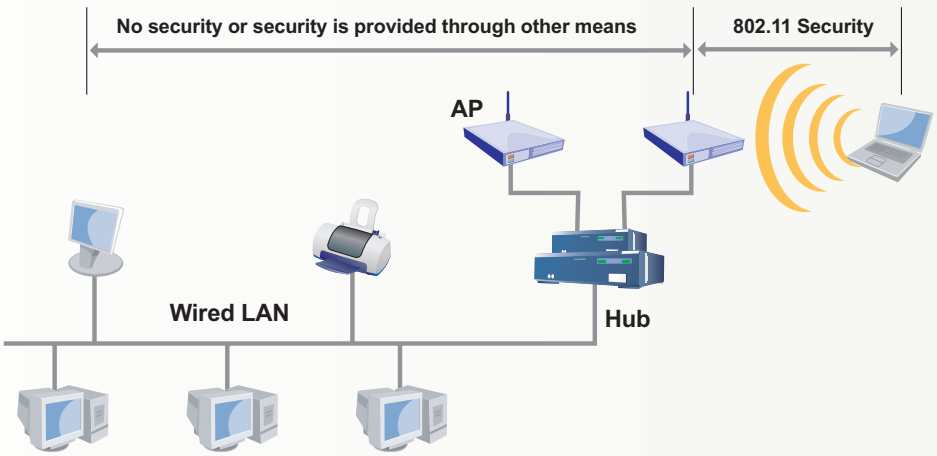
## 4. 무선랜 보안 메커니즘

현재 가장 많이 사용중인 무선랜 기술인 IEEE802.11b의 보안 메커니즘을 살펴보면 802.11b는 WEP(Wired Equivalency Privacy)을 이용하여 사용자 인증, 기밀성, 메시지 무결성 등의 보안 서비스를 제공한다. 802.11b의 사용자 인증 메커니즘의 문제점을 해결할 수 있는 방법으로 고려되고 있는 EAP(Extended Authentication Protocol) 구조를 채택한 IEEE 802.1x를 설명한다.

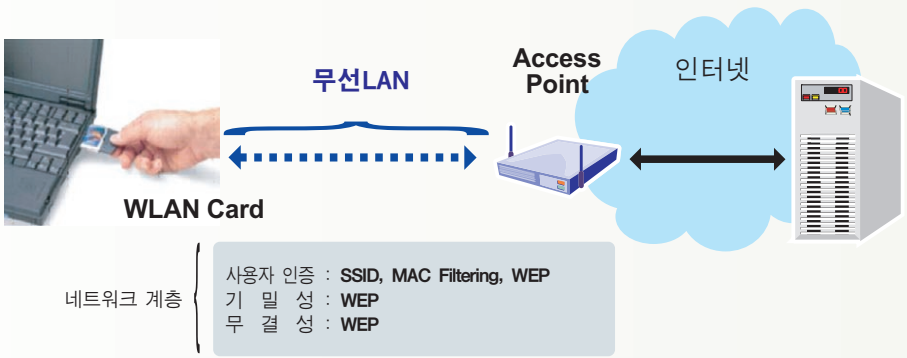
WEP은 무선 단말기와 AP사이에서 무선으로 전송되는 링크 계층의 데이터를 보호하기 위한 보안 프로토콜이다. 또한 [그림 4]와 같이 유선랜 상에 있는 서버와 무선 단말기 사이의 단대단(End-to-End) 보안은 제공하지 못하며, 다만 무선 단말기와 AP 사이에서만 보안 서비스를 제공한다.

본 글은 802.11b를 중심으로 하는 WEP 보안 메커니즘을 살펴볼 것이다. WEP은 [그림 5]와 같이 네트워크 계층에서 사용자 인증, 기밀성, 무결성 등의 보안 서비스를 제공한다. 이외에 부인 봉쇄 서비스가 있지만 부인 봉쇄 서비스는 전송되는 모든 메시지에 대해 전자 서명을 하기 때문에 네트워크에 많은 부담을 줄 수 있어 어플리케이션에서 제공하는 것이 일반적이다.

# '무선LAN'의 안전한 사용을 위한 보안대책




[그림 4] 802.11b 보안 구조

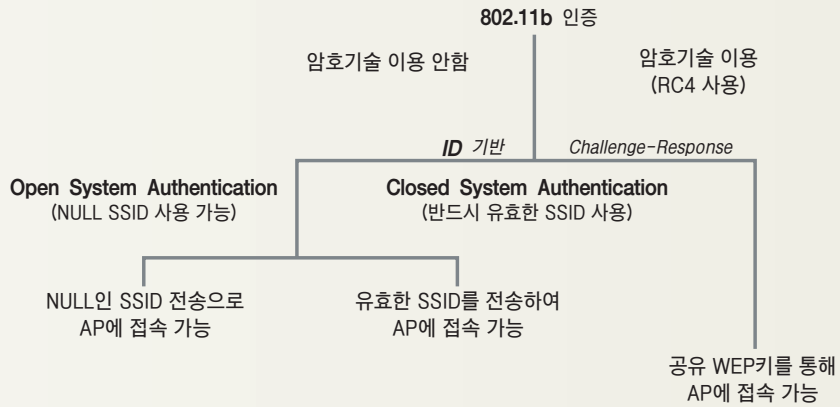



[그림 5] 802.11b 보안 서비스

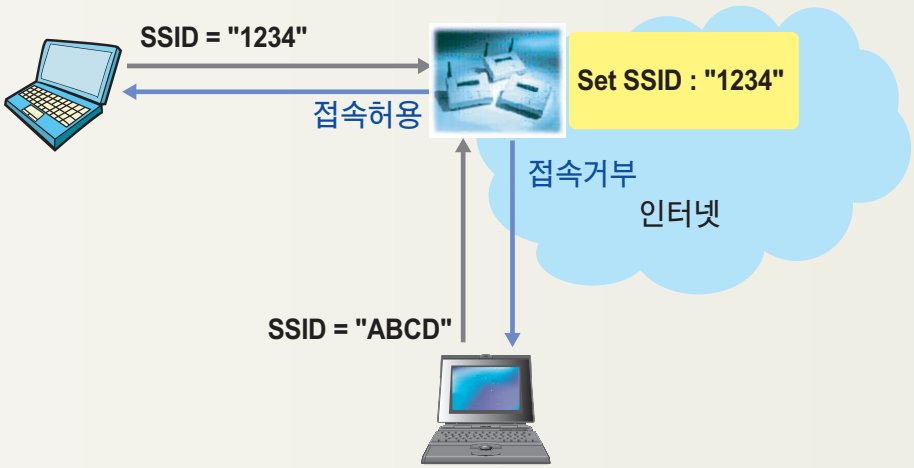
### 가. 사용자 인증

802.11b에서 네트워크에 접속하려는 무선 사용자를 인증할 수 있는 방법은 [그림 6]과 같이 암호기술을 이용한 방법과 [그림 7]과 같이 SSID(Service Set Identifier)를 이용한 방법으로 구분된다.

첫째, SSID를 이용한 방법이다. 이 방법은 [그림 7]과 같이 무선랜 카드에서 AP에 접속시 사전에 알고 있는 SSID를 이용한다. 인증시 반드시 유효한 SSID를 사용해야만 인증이 이루어진다. 널(Null) 값을 갖는 SSID를 이용해서 접속이 가능한 방식을 개방형인증(Open System Authentication)이라 한다.




[그림 6] 사용자 인증 서비스

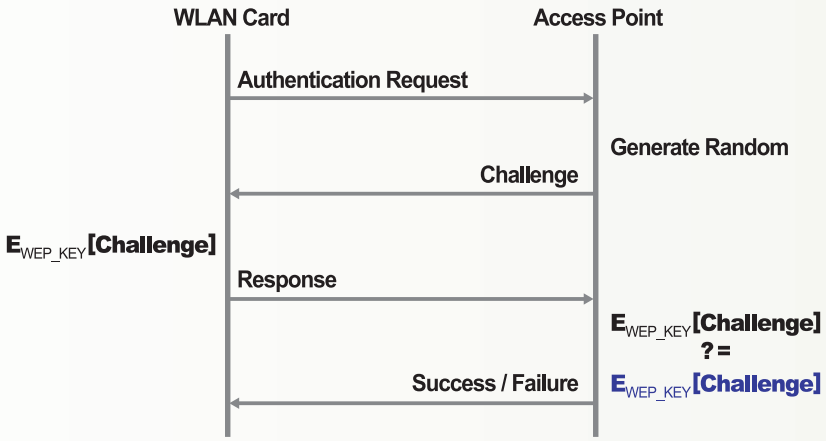



[그림 7] SSID를 이용한 사용자 인증

AP 및 무선랜카드 업체는 SSID를 업체가 설정한 기본값으로 판매한다. 예를 들면, 3COM 제품은 SSID가 '101', Cisco의 제품은 'Tsunami'로 각각 설정되어 있다. AP는 주기적으로 SSID를 브로드캐스트 한다. 무선랜카드는 AP에 접속이 가능한 지역 내에서 브로드캐스트된 SSID를 수신하여 AP에 접속한다.

둘째, 암호기술에 기반한 인증방식은 무선랜카드와 AP가 공유하는 WEP 키를 이용한 챌린져-리스판스(Challenge-Response)방식이다. 이 방식은 [그림 8]과 같이 이루어진다.

# '무선LAN'의 안전한 사용을 위한 보안대책




[그림 8] WEP을 이용한 사용자 인증

① 무선랜 카드는 네트워크 접속을 위해 AP에 인증을 요청한다.
② AP는 임의의 난수값(Challenge)을 무선랜 카드로 전송한다.
③ 무선랜 카드는 수신한 난수값을 자신이 저장하고 있는 WEP 키를 이용해서 암호화하여 생성한 값(Response)을 다시 AP로 전송한다. 암호 알고리즘은 WEP 암호화와 마찬가지로 RC4를 사용한다.
④ AP는 자신이 생성한 난수값을 무선랜 카드가 사용한 것과 동일한 WEP키로 암호화하고, 무선랜 카드가 전송한 값(Response)와 비교하여 동일하면 랜카드를 인증한다.


[그림 9] 무선랜 카드 MAC주소 인증

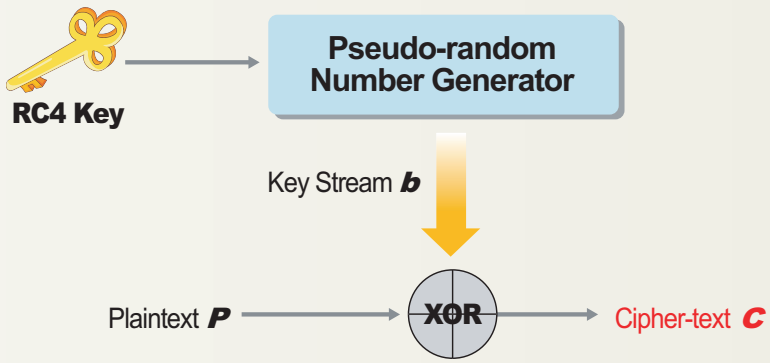
위의 2가지 인증 방법 외에 무선랜에서 사용되는 인증 방법은 MAC 주소 필터링(MAC Address Filtering)이 있다. 이 방법은 무선랜 카드마다 유일하게 할당되는 MAC 주소를 인증에 이용하는 것으로 [그림 9]와 같이 이루어진다.

AP는 접속이 허용된 MAC 주소 목록을 저장하고 있으며, 관리자는 MAC 주소를 편집할 수 있다. 무선

랜 카드는 자신의 MAC주소를 전송하면 AP는 접속이 허용된 MAC주소 목록에 포함된 주소인지 여부를 확인하고 인증한다.

### 나. 기밀성 및 무결성

802.11b의 보안 메커니즘인 WEP은 기밀성을 위해 [그림 10]과 같이 스트림사이퍼(Stream Cipher) 암호 알고리즘인 RC4를 이용한다. RC4 키를 난수값 발생기에 입력하여 키 스트림을 구한다. 키 스트림이 실제 암호화할 때 사용되는 키 값이다. WEP은 RC4 알고리즘, 비밀키, 전송 데이터를 암호화하여 전송함으로 데이터가 무선 구간에서 유출되더라도 내용을 알 수 없다.

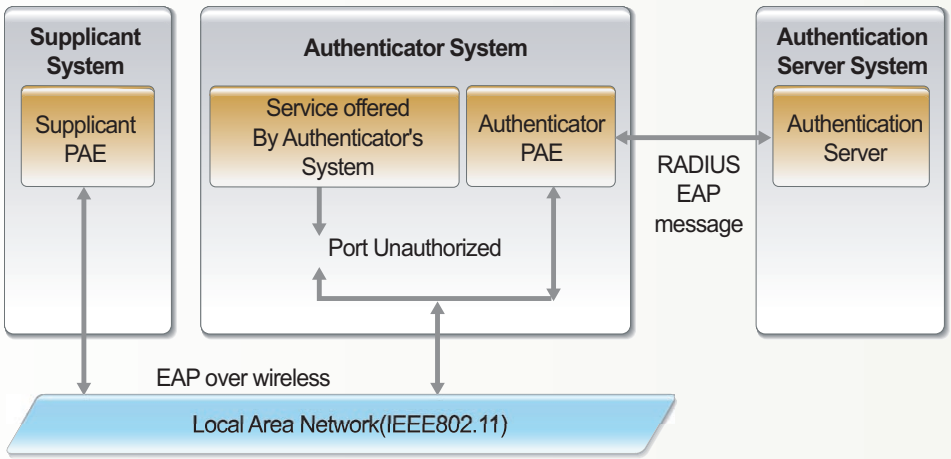



[그림 10] RC4 암호화 과정

자세히 설명하면, AP와 무선랜 카드가 서로 공유하고 있는 키의 테이블이 있고, 데이터 암호화에 사용된 키(WEP Key)의 인덱스를 보내면 상대편도 같은 키 테이블을 가지고 있어서 테이블에서 해당되는 키를 찾아 복호화에 이용한다. WEP은 TCP/IP(Transmission Control Protocol/Internet Protocol), IPX(Internet Packet Exchange), HTTP(Hyper Text Transfer Protocol) 등 무선랜 상위의 모든 데이터에 적용된다.

### 다. IEEE802.1x 보안 메커니즘

SSID나 공유키 인증 방식은 신뢰성이 비교적 떨어지는 방식이다. 802.1x는 802.11b의 사용자 인증 문제의 취약성을 해결할 수 방법으로 고려된다. 802.1x가 동작하는 구조를 살펴보면 [그림 11]과 같다.



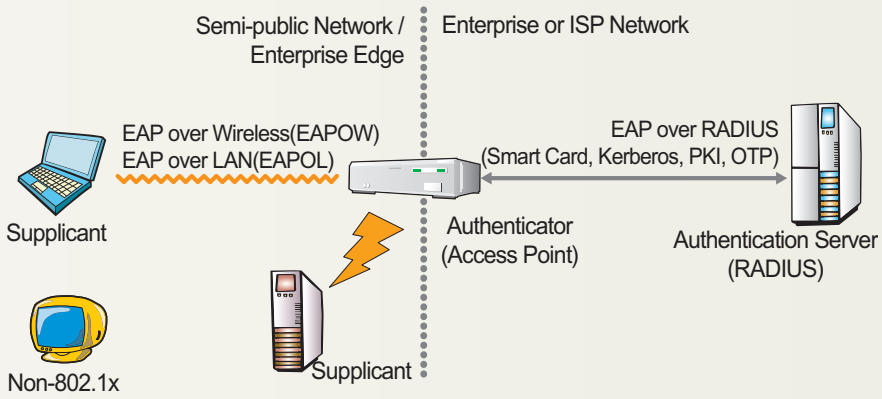

[그림 11] 802.1x 구조

802.1x는 제어 포트(Controlled Port)와 비제어 포트(Uncontrolled Port)가 있다. 사용자(Suppliant)는 AP나 브릿지가 가상적으로 정의한 비제어 포트를 통해서 AP 뒤에 있는 인증 서버(Authentication Server)에 인증을 요청한다. 사용자가 인증을 받게 되면 비제어 포트로는 인증 서버 이외의 네트워크 자원에 접근할 수 없다.

제어 포트는 인증이 성공했을 때 개방되는 포트이다. 인증을 획득한 사용자는 제어 포트를 통해서 모든 네트워크 자원에 접근할 수 있다. 인증 서버는 RADIUS(Remote Authentication Dial In User Service)라는 AAA (Authentication Authorization Accounting)서버가 이용되고 있으며, 향후에는 Diameter 서버의 이용이 예상되고 있다.

802.1x는 [그림 12]와 같이 EAP를 채택하여 인증을 수행한다. 802.11b는 사용자 인증을 AP가 하지만, 802.1x EAP에서는 AP가 단 히 사용자와 인증 서버 간의 중개 역할만 하며, 사용자 인증은 인증 서버가 수행한다.

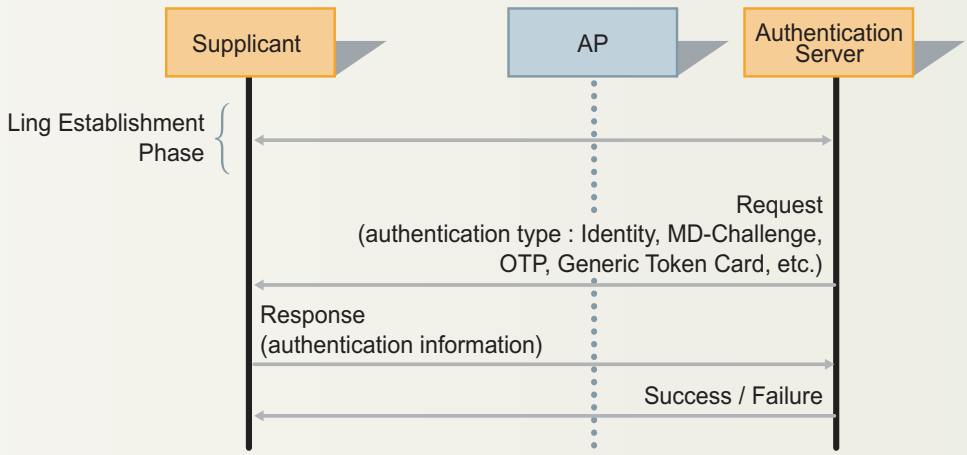
사용자와 AP, 인증 서버 간에 송수신하는 메시지는 EAP 규격을 따라야 한다. 사용자와 AP 간의 통신은 EAPOL(EAP over LAN) 또는 EAPOW(EAP over Wireless)을 사용하며 무선랜은 EAPOW를 사용한다. 802.1x는 구체적인 인증 방법을 정의하고 있지 않고 있으며, 인증에 필요한 스킴만 제공한다. 따라서 스마트카드를 이용한 인증, 커버로스 (Kerberos), TLS(Transport Layer Security), OTP(One Time Password) 등 다양한 방법 가운데 선택하여 사용할 수 있다.




[그림 12] EAP를 이용한 인증

### 라. EAP 인증 구조

802.1x EAP에 의해서 인증이 이루어지는 과정은 [그림 13]과 같다.




[그림 13] 802.1x를 이용한 인증

사용자(Supplicant)가 네트워크 연결 요청을 하면, AP는 인증 서버에게 송신한다. 이 상태에서 사용자는 AP를 통해 인증 서버와의 통신만이 가능하며, 다른 네트워크 자원에는 접근할 수 없다. 다음 단계에서 인증 서버는 인증 방법을 지정하여 사용자에게 인증에 필요한 정보를 요구한다. 이 요구를 받은 사용





자는 인증에 필요한 정보를 인증 서버에게 전송하고, 인증 서버는 전송 받은 정보를 검증하여 사용자를 인증한다. 인증이 실패할 경우에는 사용자는 네트워크에 접근할 수 없고, 인증에 성공한 경우에 사용자는 AP를 통해 네트워크 자원을 이용할 수 있다.

### 마. 802.11i 보안 메커니즘

WEP 방식의 보안 문제점이 WEP키와 IV(Initial Vector, 초기값) 사이즈가 작고 모두에게 알려진 공유키를 사용하여 암호, 알고리즘과 무결성 알고리즘이 근본적으로 보안에 취약하다. 무선 LAN 보안 표준화 그룹인 IEEE 802.11i는 이러한 문제점을 해결하기 위해 MAC 계층위에 IEEE 802.1x를 적용하여 키 관리와 인증 서비스를 제공해주는 RSN (Robust Security Network)을 제안하였다. RSN은 다음과 같은 보안 특징을 가지고 있다.

- 802.1x 기반 인증: 포트기반접근제어(Port-based Access Control)를 통한 사용자 인증 및 무선 네트워크 접근 제어
- 데이터 프라이버시 알고리즘: AES-OCB, TKIP 사용
- 보안 어소시에이션 관리: 동적인 키 생성 및 분배 매커니즘과 키교환(Re-Keying) 프로토콜을 이용하여 단말-AP간 적용 가능한 Cipher Suite 정보를 교환하고 설정

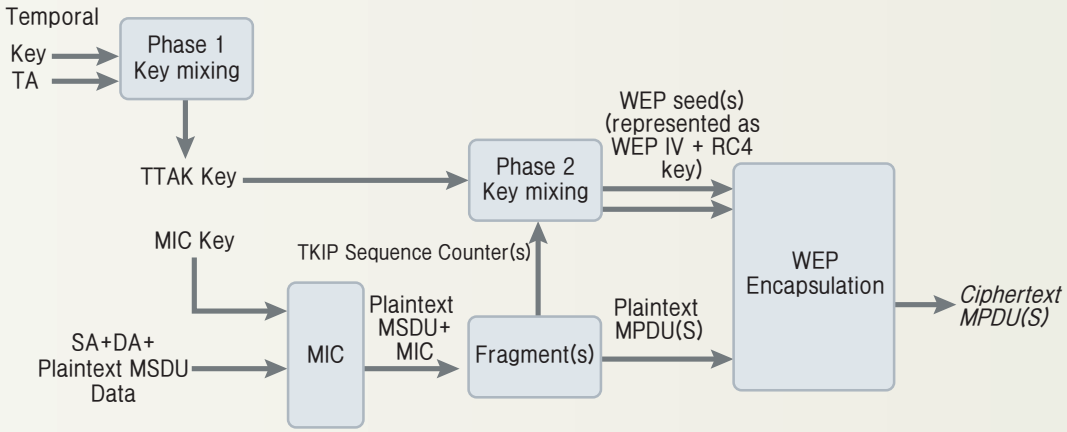
Wi-Fi 그룹은 IEEE 802.11i 보안 그룹의 표준화 진행 속도가 산업 시장 요구 일정을 만족시키지 못하자 2003년 1분기에 IEEE 802.11i 보안 규격의 일부 기능인 TKIP를 준용하여 단체 표준규격 WPA(Wi-Fi Protected Access)를 채택하였다. WPA의 핵심 기술인 TKIP은 기존의 WEP RC4 보안의 문제점을 소프트웨어적으로 개선하여 무선랜 카드와 AP에 패치하여 사용할 수 있게 함으로 기존의 IEEE 802.11b 장비와 호환 가능하다. WPA는 현재의 WEP을 대체하여 강력한 데이터 무결성과 접근 제어 기능을 제공할 수 있도록 제정된 표준으로 다음과 같은 부분이 향상되었다.

- TKIP을 통하여 향상된 데이터 무결성: 데이터의 무결성을 향상시키기 위하여 WPA는 TKIP(Temporal Key Integrity Protocol)을 채택하였다. TKIP는 Key Mixing, MIC(Message Integrity Check), 개선된 IV, Re-Keying 메커니즘 등을 포함한다.
- EAP를 이용한 사용자 인증: WPA는 강력한 사용자 인증을 위하여 EAP(Extensible Authentication Protocol)을 구현하고 있다. EAP는 중앙인증서버인 RADIUS를 이용하여 사용자가 네트워크에 접속하기 전에 사용자 인증을 수행한다.

### (1) TKIP 암호화 과정

TKIP는 [그림 14]와 같이 Key Missing 과 Michael 함수를 이용하여 WEP 암호화를 강화한다. 아래는 암호화 과정을 나타낸다.

- TKIP 는 MSDU근원지 주소, 목적지 주소, 데이터를 이용하여 MIC 계산하며 MSDU 프레임에 MIC 를 덧붙인다.
- TKIP는 MSDU 프레임을 MPDU로 분할한다. TKIP는 각 MPDU에 증가된 IV값을 할당한다. 같은 MSDU(Message Service Data Unit)에서 분할된 모든 MPDU는 같은 48bit의 카운터 공간의 카운터 값을 사용한다.
- MPDU에 TKIP는 Key Mixing 함수를 이용하여 WEP seed를 계산한다.
- TKIP는 WEP seed를 WEP IV와 Rc4 Key로 이용한다. WEP는 WEP seed를 임시 키와 관련된 키 ID인 WEP default key로 이용한다.




[그림 14] TKIP 암호화 과정

### (2) 키 교환 및 동기화

802.1x 절차를 거쳐 사용자 인증 과정이 완료되면 RADIUS서버는 EAPOL-Key 메시지를 이용하여 PMK를 AP에 전달한다. AP는 PMK로부터 TKIP의 세션키를 생성한 후 PMK로 암호화 하여 무선 단말에 전달한다. AP는 키교환 시점, 키 유형, PTK 생성에 필요한 난수, 메시지 인증 MIC 코드, Sequence Counter에 대한 정보를 관리한다.





## 5. 결 론

본 글은 점차 확산되는 무선랜 사용에 따라 기본적인 무선랜 개념, 구성요소, 표준화 현황, 보안 메커니즘 및 보안 서비스를 개괄적으로 설명하였다. 무선랜의 이동성, 편의성, 확장성, 고속서비스 및 표준화 활동 등의 뒷받침은 무선랜 시장의 활성화 시키고 사용자를 지속적으로 확장시키고 있다. 이미 민간 부문은 무선랜을 도입하여 업무에 적극적으로 활용하고 있는 추세이며, 국가 및 공공 기관도 무선랜을 일부 도입하여 사용하고 있지만, 무선랜 보안 대책의 미흡으로 충분히 업무에 적용시키지 못하고 있는 실정이다. 다음 연재에서는 무선랜 도입을 가로막고 있는 무선랜의 보안 취약성을 살펴본다.

### 참고문헌


1. 무선랜 WPA 보안 핵심기술, [IT 리포트], 한국기술거래소, 2004.10
2. 무선 LAN 보안 체크리스트, on the net, 2005.3.
3. 무선 LAN 보안 기술, 정보과학회
4. IEEE 802.11을 중심으로 한 무선 LAN 바이블, 세화, 2003.
5. Tom Katygiannis, Les Owens, "Draft Wireless Network Security", National Institute of Standards and Technology (NIST), 2002
6. "IEEE802.11b Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification", IEEE Standard 802.11b, 1999
7. James T. Geier, Jim Geier, "Wireless LANs (2nd Edition)", SAMS, 2001
8. Nikita Borisov, Ian Goldberg, David Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11", Proceedings of the 7th International Conference on Mobile Computing and Networking, 2001. 7
9. Rigney, C., Willens, S., Rubens, A., and W. Simpson, 'Remote Authentication Dial In User Service (RADIUS)', RFC 2865, June 2000.