主題

무선 LAN 보안 취약점과 단계적 해결 방안

한국전자통신연구원 강 유 성, 오 경 희, 정 병 호, 정 교 일

차 례

Ⅰ. 서론
Ⅱ. 무선 LAN 보안
Ⅲ. 단계적 해결 방안
Ⅳ. 결론

요약

범 국가적으로 해킹, 바이러스 등 사이버 테러에 대한 관심이 높아지고 있고, 원천적으로 유선 네트워크에 비하여 보안성이 취약하지만 최근 그 활용 범위가 급속히 확장되고 있는 무선 LAN에서의 보안 문제가 사회적인 관심사가 되고 있다. 본 고에서는 일반적인 무선 네트워크의 보안 위협 요인에 비추어 무선 LAN 보안의 취약점을 분석하고, 이를 극복하기 위하여 단기적인 시간에 구축할 수 있는 해결 방안부터 장기적인 관점에서 글로벌 로밍까지 고려한 단계적인 해결 방안을 제시하고자 한다.

Ⅰ. 서론

현재 사용되고 있는 무선 LAN 기술의 표준화를 담당하는 IEEE 802.11 워킹그룹의 초기 목표가 무선 환경에서 데이터 충돌 없이 통신하기 위한 물리계층과 링크계층 정의였음은 잘 알려진 사실이다. 그 결과로써 11Mbps 속도로 통신할 수 있는 IEEE 802.11b 규격의 무선 LAN 카드와 무선 LAN 액세스포인트 제품이 주류를 이루고 있으며, 최대 54Mbps 속도인 IEEE 802.11a, IEEE 802.11g 규격의 제품이 등장하였다.

그러나, 무선 LAN 속도 향상이 해결되었음에도 불구하고 무선 LAN 기술의 저변화를 가로막은 장벽은 바로 보안 문제이다. 무선구간 전송속도 향상과 더불어 반드시 해결되어야 할 과제가 무선 LAN 보안기술이며, 이는 무선 공중망을 사용하는 개별 응용에서 지원하는 보안기술과 차별되는 사회 전반적인 보안 인프라로써 구축되어야 한다. 무선 LAN 서비스의 활용형태를 살펴보면 다음과 같이 구분할 수 있다.

- 기업망 적용
- 가정/SOHO(Small Office Home Office)망 적용

■ 공중망 적용

IEEE 802.11 기반의 무선 LAN 서비스 구조는 크게 Ad-Hoc 모드와 Infrastructure 모드로 구분된다. Ad-Hoc 모드는 각각의 단말이 일대일 통신을 수행하는 형태인 반면, Infrastructure 모드는 각각의 무선단말이 액세스포인트를 통해서 네트워크 환경으로 연결되는 구조이다. 따라서 무선 LAN 사용자가 인터넷 서비스를 받기 위해서는 사용자 단말에서 무선 LAN 카드의 사용모드를 Infrastructure 모드로 설정한 후 무선 LAN 액세스포인트에 접속하여야 한다.

기업망에서 활용되는 무선 LAN 구성요소는 그림 1에 보이는 것처럼 무선단말(예, 무선 LAN 카드가 장착된 노트북 컴퓨터), 액세스포인트(예, AP라고도 불리며, 이동통신 시스템의 기지국처럼 다수의 무선단말을 접속시키는 역할도 하고, 무선데이터를 유선인터넷으로 연결시켜 주는 허브/브릿지 역할도 수행하는 장치), 그리고 인증서버(예, RADIUS 서버가 현재 사용 가능한 대표적인 인증서버이며, 사용자 인증 여부를 결정짓는 역할을 수행하는 서버)로 구성될 수 있다. 이와 같은 구성은 공중망에서도 적용될 수 있다.

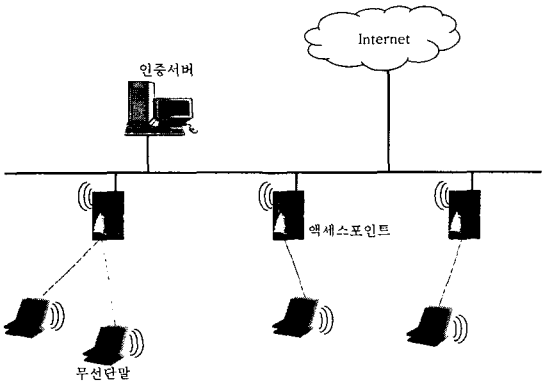


그림 1. 기업망 또는 공중망에서의 무선 LAN 구성요소

가정/SOHO망은 소규모의 한정된 사용자를 위한 시스템이므로 다수의 사용자를 관리하고 인증하는 인증서버를 사용하지 않고 액세스포인트 자체에서 직접 사용자를 관리하는 형태를 갖는다. 그림 2에서 이러한 형태의 무선 LAN 구성요소를 보이고 있다.

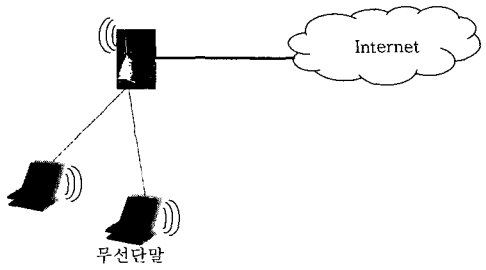


그림 2. 가정/SOHO망에서의 무선 LAN 구성요소

무선 LAN 서비스 활용형태에 따라 구성요소의 차이는 있지만 대부분 공통적인 보안 위협 요인 및 보안 취약점을 갖기 때문에 보안 해결 방식은 동일하다. 따라서 본 고에서는 무선 LAN 보안 취약점을 분석하고 이를 극복하기 위한 단기적인 해결 방안부터 장기적인 관점에서 글로벌 로밍까지 고려한 단계적인 해결 방안을 제시하기 위하여 다음과 같은 구성을 갖는다. II장에서는 무선 LAN 보안에 대한 전반적인 사항으로써 무선 LAN 위협 요인, 무선 LAN 보안 취약점을 분석하고, 보안 기능 제공을 위한 무선 LAN 보안 서비스를 항목별로 살펴본다. III장에서 기술발전과 국제 표준 제정의 진행 정도, 그리고 보안 서비스 효과여부에 따라 8단계로 구분하여 무선 LAN 보안 해결방안을 제시한 후 IV장에서 결론을 맺는다.

II. 무선 LAN 보안

1. 무선 LAN 위협 요인

무선 LAN 기술의 등장으로 무선 네트워크 환경에서 노트북과 PDA 등 다양한 무선단말을 사용하여 초고속 무선인터넷 접속을 가능하게 하였지만, 기존의 유선 네트워크와 달리 보안상의 위협 요인이 더욱 부각되고 있다. 본 절에서는 무선 LAN 시스템을 위협하는 대표적인 보안 위협 요인들을 살펴본다.

■ 비인가 사용자 접근 (Unauthorized Access)

유선 네트워크와 무선 네트워크의 대표적인 차이는 데이터 전달 매체이다. 무선 LAN 시스템은 유선 네트워크와 달리 기본적으로 모든 단말에 데이터를 전송하는 브로드캐스팅 망이므로, 액세스포인트의 비콘(Beacon) 프레임 수신 영역 내에 있는 모든 단말은 해당 액세스포인트로 접속을 시도할 수 있다. 따라서 만일 해당 무선 LAN 시스템이 사용자 인증과 관련된 보안 기능을 수행하지 못한다면 비인가 사용자의 접근이 허락될 것이며, 이는 보안상 중대한 위협 요인이 되는 것이다.

■ 메시지 도청 (Eavesdropping)

메시지 도청이라 함은 송신자와 수신자가 메시지를 주고받고 있는 사이에 제 3자가 몰래 끼어 들어 송신자와 수신자 사이의 메시지를 엿듣는 경우를 의미한다. 무선 LAN 환경에서는 전파 매체를 통한 데이터 송수신이 발생하므로 도청의 위협은 더욱 크다고 할 수 있다.

■ 데이터 변조 (Injection and Modification of Data)

전송중인 데이터에 변형을 가하여 수신자로 하여금 잘못된 데이터를 수신하게 하는 공격 방법을 데이터 변조라 한다. 데이터 변조 공격은 정당한 송수신 채널을 마비 시킬 수 있으며, 특히 DoS(Denial of Service) 공격에 사용될 수 있는 강력한 위협 요인이다[1].

■ 통신 방해 (Communications Jamming)

무선 네트워크에서 흔히 겪게 되는 통신 장애 중의 하나는 의도된 공격자에 의한 간섭현상이 있다. 전파 특성을 고려한 통신 방해를 일컫는 재밍(jamming)은 무선 LAN 환경에서도 주요한 위협 요인이 될 수 있다.

■ MITM(Man-in-the-Middle) 공격

MITM 공격은 송수신자 사이에 위치하여 데이터에 변형을 가할 수 있다는 점에서 데이터 변조 공격과 유사하다. MITM 공격은 송수신자 사이에서 공격자가 프록시 기능을 수행하여 모든 송수신 데이터를 공격자가 의도하는 대로 변형, 전달, 삭제할 수 있는 보다 더 강력한 위협 요인이다.

2. 무선 LAN 보안 취약점

무선 LAN 보안 위협을 극복하기 위하여 IEEE 802.11 무선 LAN 표준 규격에서는 기본적인 접근제어 방식과 데이터 암호화 방식을 제안하고 있으며, 기존의 IEEE 802.11b 제품들은 기본 보안 기능을 포함하고 있다.

기본적인 접근제어 기능은 사용자 인증을 통해 이루어지는데, 대표적인 3가지 방법이 있다.

- 사용자와 액세스포인트가 동일한 공유 키를 보유하여 접속 요청 시 공유 키 인증방식을 사용하는 방법[2]
- 사용자의 무선LAN 카드 MAC(Medium Access Control) 주소를 액세스포인트에 직접 입력시켜 놓는 방법
- 사용자가 자신의 인증정보를 가지고 인증서버와 인증절차를 수행하는IEEE 802.1X 인증 방법[3]

데이터 암호화 방식은 잘 알려진 바와 같이 WEP(Wired Equivalent Privacy) 알고리즘을 사용하여 지원되는데, 사용되는 키 길이가 40 비트 또는 104 비트가 가능하다[2].

만일 무선 LAN 시스템을 기업체 또는 개인이 운용할 경우 허가된 무선 LAN 카드의 MAC 주소를 액세스포인트에 직접 입력시키고, WEP 알고리즘을 사용하는 등 위의 접근제어 방식과 데이터 암호화 방식을 사용한다면 무선 LAN 수신장치만으로 도청을 시도하는 초보 해커의 접근과 도청은 막을 수 있다.

그러나, 일반적으로 무선 LAN 통신기능 자체를 우선시 하기 때문에 액세스포인트의 출고 시 상태는 접근제어 관리와 WEP 알고리즘의 사용이 모두 비활성화 되어 있어서 모든 무선 LAN 카드와 통신을 허락하는 보안상 무방비 상태이다. 따라서 무선 LAN 관리자의 세심한 관리가 없으면 어느 누구라도 단지 무선 LAN 카드가 장착된 노트북 하나만으로 기업체 내부망에서 접근암호를 사용하지 않는 폴더는 모두 들여다볼 수 있다.

공중망 서비스에서는 공유 키를 사용한다거나 무선 LAN 카드의 MAC 주소를 직접 입력하여 사용자 인증을 수행하기에는 그 사용자가 너무 방대하여 관리하기가 불가능하며, EAP-MD5 (Extensible Authentication Protocol-Message Digest 5) 방식의 단방향 IEEE 802.1X 인증은 brute force 공격에 취약하고, WEP 알고리즘 역시 메시지 도청이 가능한 취약한 알고리즘으로 판명되었기 때문에 현재의 무선 LAN 보안기능은 전면적으로 보완되어야 한다[4][5].

무선 LAN 보안 시스템의 인증서버는 일반적으로 액세스포인트와 안전한 채널을 유지하며, 무선 LAN 사용자와 EAP 인증 메시지를 교환하여 인증 여부를 판단한다. RADIUS(Remote Authentication Dial In User Service) 서버가 대표적인 인증서버이며, 액세스포인트는 RADIUS 메시지를 생성하여 인증서버와 통신하는 RADIUS 클라이언트 역할을 수행한다.

그러나, 최근의 무선 LAN 환경은 핫스팟(Hot spot) 지역에서 액세스포인트를 통해 직접 인터넷에 접속하는 형태로, PPP 접속에서의 NAS(Network Access Server)와는 다른 방식이므로 기존의 클라이언트/서버 모델 기반의 RADIUS를 인증 및 과금서버로 사용하기에는 적합하지 않다. 즉, 인증서버에 접속하기 위한 NAS로 동작하는 액세스포인트는 PC 통신 서버의 수에 비해서 상대적으로 매우 많고 이를 관리하는 주체도 대단히 많을 것으로 예상되는 상황에서 단순한 프록시 기능만을 지닌 RADIUS를 이용하여 이들을 효과적으로 상호 연계시키는 것이 현실적으로 어렵고, 큰 규모의 적용환경에 취약한 것으로 알려져 있다[6].

위에서 언급된 무선구간 및 인증서버의 문제점에 대하여 IEEE 802.11 워킹그룹은 다음과 같이 정리하고, 그 해결 방안을 표준화에 반영하고자 노력하고 있다.

(1) RC4를 사용하는 WEP 알고리즘 자체가 알려진 평문 공격에 취약하다.
(2) 동적인 키 분배 방법이 없다.
(3) 가입자 인증 및 접속제어 방법이 없다.
(4) 공중망에 적용을 위한 중앙집중형 인증/권한제어/과금(AAA) 방법이 없다.
(5) 인증서, 보안토큰, ID/패스워드, SIM 등을 지원하는 다양한 가입자 인증방식이 없다.
(6) 핸드오프 보안을 지원하지 못한다.

상기의 문제점을 해결하기 위하여 (1)과 (2)는 IEEE 802.11i 태스크그룹, (3)은 IEEE 802.1X 및 IEEE 802.1aa 태스크그룹, (4)는 IETF AAA 워킹그룹, (5)는IETF EAP 워킹그룹, 그리고 (6)은

IEEE 802.11f 태스크그룹과 IEEE 802.11i 태스크그룹에서 표준화를 진행하고 있다.

특히 무선 LAN 제품의 상호호환성을 인증해 줌으로써 무선 LAN 서비스의 상용화에 지대한 역할을 하고 있는 무선 LAN 산업체의 비영리 연합인 Wi-Fi 연합(Wireless-Fidelity Alliance)에서는 무선 LAN 보안에 대한 자체 규격을 제정하였다. Wi-Fi는 이 무선 LAN 보안기술을 WPA(Wi-Fi Protected Access)로 명명하고, 2003년 2월에 WPA 제품에 대한 상호호환성 테스트를 시작하여 2003년 8월부터 Wi-Fi 인증의 필수 항목으로 규정할 계획을 제시한 바 있다[7]. 지난 2003년 4월에 4종의 액세스포인트와 5종의 무선 LAN 카드에 대한 WPA 기능 구현에 대한 인증을 부여하였다[8].

3. 무선 LAN 보안 서비스

무선 LAN 보안 서비스 제공을 위하여 위에서 언급한 표준화 그룹들은 단편적인 분야만을 고려하는 것이 아니라 대부분 상호 연관성을 지니며 무선 LAN 보안, 과금, 안전한 핸드오프의 공통된 목적을 달성하고자 노력하고 있다. 본 절에서는 무선 LAN 보안 서비스 제공을 위한 주요 기능별로 각 표준화 그룹의 표준규격 제정에 대한 향후 전개방향에 대하여 분석한다.

■ 접근제어와 사용자 인증

무선 LAN 시스템의 접근제어는 합법적인 사용자 인증과 동일한 개념이며, 액세스포인트를 경유하는 인터넷 접속허가 여부를 결정짓는 동작으로써 이는 인증된 가입자에게만 인터넷 접속을 허용하여 과금을 부가할 수 있는 토대가 된다.

관련된 표준규격으로는 IEEE 802.1X 규격과 IEEE 802.1aa 규격 그리고PSK(Pre-Shared Key) 기술을 정의하고 있는 IEEE 802.11i 규격이다. 2001년 6월에 승인된 IEEE 802.1X 규격에서는 포트기반 접근제어 방식을 규정하면서 사용자 인증만을 요구하고 있는 반면, IEEE 802.1aa 규격은 사용자 인증 및 무선구간 키 교환을 필수적인 접근제어 요소로 규정하고 있다[9]. 이는 무선 LAN 시스템의 보안성을 강화하는 방향으로 IEEE 802.1X 규격을 발전시키고 있음을 보여주고 있다. 더불어 IEEE 802.11i 규격은 IEEE 802.1aa 규격의 무선구간 키 교환을 지원하기 위한 4단계 핸드쉐이크 방식을 정의하고 있으며, 사용자 인증 및 마스터 세션 키 획득을 위해 PSK 기술을 선택사항으로 명시함으로써 가정 또는 SOHO에서 인증서버를 별도로 구비하지 않아도 되도록 배려하고 있다[10].

따라서, 접근제어 기술은 IEEE 802.1X 인증을 기본으로 하여 무선구간 암호 키 교환을 필수적인 구현요소로 지정하는 방향으로 결정될 것으로 보이며, 선택적으로 PSK 방식이 적용될 수 있도록 표준화가 진행될 것으로 판단된다.

■ 데이터 기밀성과 무결성

무선구간 데이터를 보호하기 위해서는 안전성이 보장된 암호 알고리즘의 적용과 키 관리 정책이 구현되어야 한다. IEEE 802.11i 규격에서 무선 LAN 데이터 보호를 위한 새로운 암호 알고리즘을 정의하고 있으며, 더불어 키 관리 정책의 일환으로 마스터 세션 키 획득, 키 교환 방식, 그리고 무선구간 암호 키 생성 및 사용에 대하여 정의하고 있다.

키 관리 정책은 사용자 인증 방식의 선택에 따라 IEEE 802.1X 인증에서는 인증서버로부터 마스터 세션 키를 획득하고, PSK 인증에서는 입력된 패스워드로부터 마스터 세션 키를 얻어서 암호 키를 생성하도록 표준화가 결정된 듯하다. 암호 알고리즘의 적용은 단기적인 해결책으로 TKIP(Temporal Key Integrity Protocol) 알고리즘의 소프트웨어 패치를 제안하고 있지만, 장기

적인 관점에서 볼 때 CCMP(Counter mode with CBC-MAC Protocol) 암호 알고리즘의 하드웨어 구현을 목표로 두고 있기 때문에 표준문서의 확정 이후에도 TKIP 알고리즘의 사용이 당분간 지속될 것으로 보이며 장기적으로는 CCMP 알고리즘이 구현된 무선 LAN 칩셋이 기대된다.

■ 사용 권한 검증 및 과금

사용 권한 검증 및 과금 정책은 무선 LAN 시스템이 공중망 서비스로 확장될 때 무선 LAN 서비스 사업자 측면에서 매우 중요한 기술적 요소가 된다. 기존에 사용중인 RADIUS 서버가 무선 LAN 공중망 서비스에 적합하지 않을 것으로 판단되고, 인증, 사용 권한 검증 및 과금 정책 구현을 통합적으로 관리할 수 있는 안정적이고 효율적인 기술의 요구에 맞추어 IETF AAA (Authentication, Authorization and Accounting) 워킹그룹에서 Diameter 기술 개발과 표준화를 진행하고 있는 상태이다[11].

무선 LAN 서비스 사업자 영역에 위치하게 될 Diameter 서버는 무선 LAN의 공중망 서비스에 목표를 두고 그 기술적 진보를 추구할 것으로 예측된다. 따라서 기능적 모듈화가 추구되고, 상호 호환성 및 기능 확장성이 고려되며 이동단말의 안전한 핸드오프 지원 및 그에 따른 인증과 과금, 무선데이터 보호를 지원할 수 있는 방향으로 표준화가 진행될 것으로 판단된다.

■ 안전한 핸드오프

안전한 핸드오프는 무선 LAN 공중망 서비스에서 중요하게 고려해야 할 기술적 요소로써 사용자 인증, 키 관리정책, 암호 알고리즘 협상, 그리고 과금 정책을 포괄적으로 통합하여 구현되어야 한다.

IEEE 802.11i 규격과 IEEE 802.11f 규격에서는 무선단말이 동일한 서브넷에 위치한 액세스포인트 사이를 이동할 때 제공해야 할 핸드오프 보안에 대한 표준화 논의를 진행하고 있으며, 그 논의 주제는 사전인증된 빠른 핸드오프 지원, 핸드오프 과정에서 보안 접속 유지와 보안 컨텍스트 정의 및 관리 등이다[10][12]. 그리고, 무선 LAN에서 글로벌 로밍 서비스가 제공되기 위해서는 분산인증 및 실시간 패킷 과금에 대한 요구 또한 더욱 중요시된다. 이와 관련하여 이동통신과 무선 LAN이 연동되는 환경에 적합한 Diameter AAA 서버의 표준화를 IETF AAA 워킹그룹에서 진행하고 있다. 무선 LAN 글로벌 로밍 및 핸드오프 보안기술은 지속적으로 연구되고 표준화를 진행해야 하는 분야로써 향후에는 IEEE 802.11i 규격의 보안 컨텍스트 정의, IEEE 802.11f 규격의 IAPP(Inter AP Protocol) 제정과 더불어 IETF AAA 워킹그룹의 Diameter 기술 구현, IETF Seamoby 워킹그룹의 컨텍스트 전송 기술과 IETF MobileIP 워킹그룹의 IP 계층에서의 로밍기술 개발이 무선 LAN 글로벌 로밍 및 핸드오프 보안기술을 더욱 발전시킬 것으로 기대된다.

■ 사전인증(Pre-Authentication)

사전인증 방식은 표준문서의 드래프트 버전에서 소개된 바는 없지만 향후 빠른 핸드오프 지원과 사용자 인증 절차의 간소화를 위하여 제기된 기술로써 IEEE 802.11 표준화 회의에서 제안되어 논의되었던 방식이다.

사전인증의 의미에 대해서 아직도 명확하게 정의한 것은 아니지만 현재 논의되고 있는 사전인증이란 현재 하나의 액세스포인트에 접속하여 정상적인 무선 LAN 서비스를 받는 무선단말이 이동하게 될 제 2의 액세스포인트와 미리 사용자 인증절차를 수행하여 마스터 세션 키를 교환해 놓는 기술을 의미한다[13]. 이런 경우에 제 2의 액세스포인트를 감지하는 방법, 사전인증절차를

수행하는 메커니즘 그리고 AAA 서버의 역할 등이 또 다른이슈가 될 수 있으며, 향후 주요 연구 과제가 될 것으로 예측된다.

Ⅲ. 단계적 해결 방안

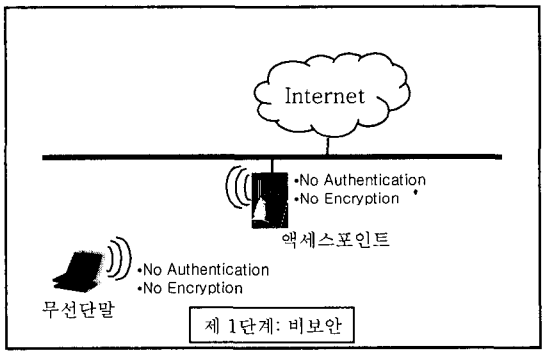
공개된 무선 환경인 무선 LAN 시스템의 보안 위협 요인인 비인가 사용자 접근, 메시지 도청, 데이터 변조, 액세스포인트에 대한 DoS 공격, 이동하는 위장 단말에 의한 고의적인 통신 방해, 위장 액세스포인트의 MITM 공격, 그리고 내외부 단말기로부터의 정보 해킹을 방어하기 위해서는 상호인증 및 접근제어, 데이터 기밀성과 무결성, 사용 권한 검증 및 과금, 그리고 안전한 핸드오프 등의 보안 서비스를 유선 네트워크 수준으로 제공하기 위한 보안 기술 제공이 필수적으로 요구된다. 뿐만 아니라 인터넷 웹 응용 서버가 전송계층 또는 응용계층에서 보안 서비스를 제공하지 않는 경우일지라도, 사용자는 적어도 상대적으로 도청 확률이 높은 무선구간에서 만큼은 정보가 노출되지 않도록 무선구간에서의 데이터 기밀성을 보장 받아야 한다.

본 장에서는 기술 발전과 국제 표준 제정의 진행 정도, 그리고 보안 서비스 효과여부에 따라 무선LAN 보안기술 단계를 8단계로 구분하여 설명한다. 단계가 올라갈수록 제공되는 보안 서비스 항목이 많아지거나 보안 강도가 강하며, 구현되는 무선 LAN 보안관련 국제 표준 규격이 많아진다. 다음 표 1은 무선 LAN 보안 기술의 각 단계별 해결 방안을 요약한 것이다.

표 1. 단계별 해결 방안 요약

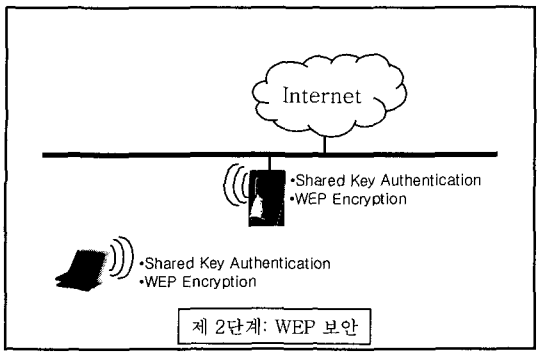
	Nickname	관련 규격	보안 서비스
제 1단계	비보안	802.11	없음
제 2단계	WEP 보안	802.11	접근제어와 사용자 인증, 데이터 기밀성
제 3단계	IEEE 802.1X 보안	802.11, 802.1X, EAP, AAA	접근제어와 사용자 인증, 사용 권한 검증
제 4단계	동적 WEP 보안	802.11, 802.1aa, EAP, AAA	접근제어와 사용자 인증, 데이터 기밀성, 사용 권한 검증
제 5단계	WPA 보안	802.11, 802.1X, EAP, AAA, WPA	접근제어와 사용자 인증, 데이터 기밀성과 무결성, 사용 권한 검증
제 6단계	RSN 보안	802.11, 802.1aa, EAP, AAA, 802.11i	접근제어와 사용자 인증, 데이터 기밀성과 무결성, 사용 권한 검증
제 7단계	이동 보안	802.11, 802.1aa, EAP, AAA, 802.11i, 802.11f	접근제어와 사용자 인증, 데이터 기밀성과 무결성, 사용 권한 검증, 안전한 핸드오프
제 8단계	무선 네트워크 보안	논의 사항	글로벌 로밍 서비스 포함이 예상됨.

① 제 1단계: 비보안



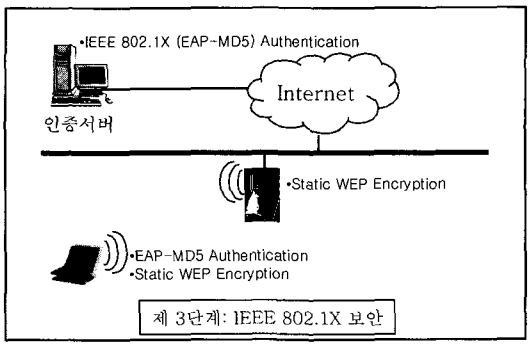
무선 LAN 보안 서비스 항목 중 어느 것도 지원하지 않으며, 보안기능을 요구하지 않는 모든 무선단말과 통신을 허락하는 상태이다. 보안기능 자체가 아예 없는 것으로 볼 수 있다. 무선 LAN 액세스포인트를 통한 통신 자체만을 지원하기 때문에 무선 LAN 카드를 장착한 노트북만으로 네트워크 접근이 가능하다.

② 제 2단계: WEP 보안



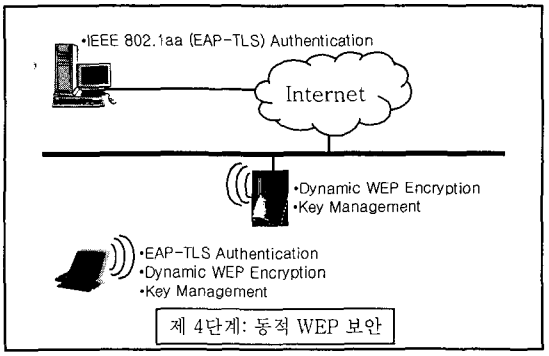
제 2단계 WEP 보안단계는 가장 초보적인 보안기능 제공 상태로써 무선단말과 액세스포인트가 WEP 키를 공유하여 공유 키 인증방식과 WEP 암호화 기능을 수행하는 상태이다. 그러나, WEP 알고리즘 자체가 IV(Initialization Vector)의 평문 전송, 키 스트림의 단순성으로 인하여 악의적인 공격자에 의해 WEP 키 값이 노출될 수 있는 취약한 알고리즘인데다 하나의 액세스포인트를 사용하는 다수의 사용자가 동일한 WEP 키를 사용하기 때문에 공중망 서비스에서 개별 사용자 보호라는 측면에서 볼 때는 보안기능의 의미가 없게 된다. 현재 사용되는 대다수의 액세스포인트와 무선 LAN 카드는 제 2단계 WEP 보안을 수행할 수 있다. 따라서 WEP 보안의 사용은 초보적인 무선 LAN 보안의 시작이다.

③ 제 3단계: IEEE 802.1X 보안



제 3단계 IEEE 802.1X 보안단계는 인증서버가 사용자 인증을 수행하여 그 결과에 따라 네트워크 접속을 제어하는 방식이다. EAP-MD5를 사용하는 IEEE 802.1X 인증 기능을 수행하는 제 3단계 보안단계는 무선 LAN 공중망 서비스에 적용 가능한 가장 기초적인 보안 정책이다. 그러나, WEP 키 공유가 없기 때문에 데이터 기밀성 지원은 없는 상태이며, WEP 키 공유를 한다고 하더라도 동일 사업자의 액세스포인트를 사용할 경우 모두가 동일한 키를 가지게 되어 보안의 의미가 없어진다. 또한 EAP-MD5 인증 방식은 brute force 공격을 통해 사용자의 패스워드가 노출될 수 있는 취약한 방식으로 판명되었기 때문에 무선 LAN 공중망 서비스를 위해서는 다음에 소개되는 제 4단계 동적 WEP 보안 이상의 보안단계로 발전해야 한다.

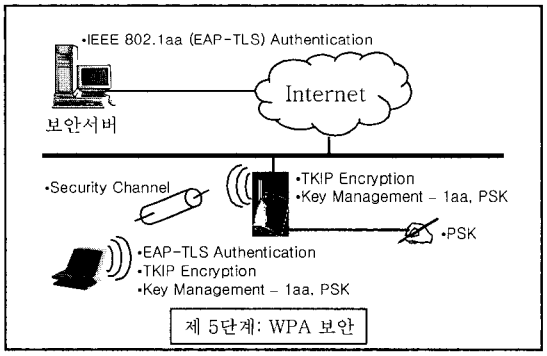
④ 제 4단계: 동적 WEP 보안



제 4단계 동적 WEP 보안단계는 EAP-TLS를 사용한 상호인증과 동적 WEP 키 적용이지원되는 보안 단계이다. 제 3단계 보안과는 다르게 EAP-TLS를 사용하는 IEEE 802.1aa 인증을 통해 상호인증이 가능하고, 접속하는 각각의 무선단말마다 IEEE 802.11i 규격의 4단계 핸드쉐이크 메커니즘으로 새로운 키를 생성하여 동적 WEP 키로 사용하기 때문에 악의적인

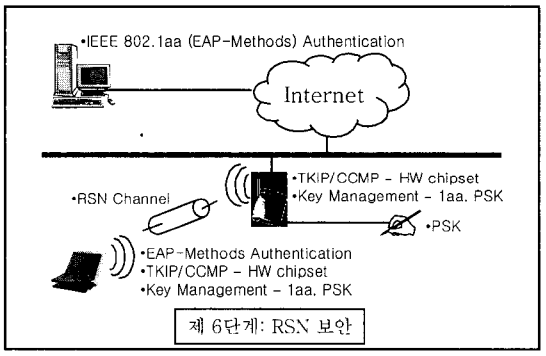
공격자가 합법적인 사용자로 위장할 수 없게 된다. 그리고, 동적 WEP 키의 키 갱신 주기를 적절하게 선택함으로써 고성능 계산능력을 가지고 공격해야 하는 악의적인 공격자의 WEP 공격을 무력화 시킬 수 있다. 무선 LAN 사용자 인증과 무선구간 암호 키 교환 기술이 적용된 제 4단계 동적 WEP 보안단계는 현재의 무선 LAN 시스템이 가지는 보안상의 취약점을 상당 부분 해결할 수 있다는 점에서 의의가 있다. 또한 무선단말과 액세스포인트에 소프트웨어적으로 패치하여 손쉽게 사용할 수 있기 때문에 향후 기업망과 공중망에서 안전한 통신 보안성 강화에 크게 기여할 수 있는 무선 LAN 보안 시스템이다.

⑤ 제 5단계: WPA 보안



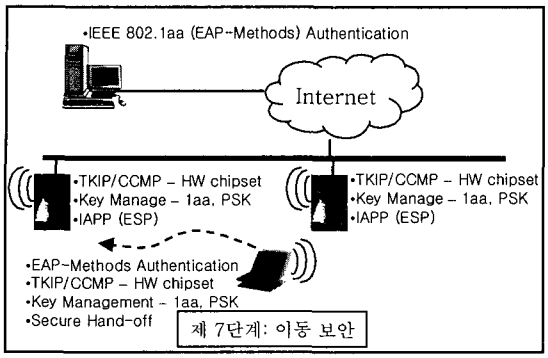
제 5단계 WPA 보안단계는 Wi-Fi에서 제정한 무선 LAN 보안 규격인 WPA 규격을 준수한 보안기술로써 제 4단계 무선 LAN 보안기술에 덧붙여 무선구간 암호 알고리즘으로 TKIP을 사용하는 보안 단계이다. EAP-TLS를 사용한 IEEE 802.1X 인증 및 IEEE 802.11i 4단계 핸드쉐이크 키 교환이 완료된 이후에 동적으로 결정된 키를 TKIP 알고리즘에 적용함으로써 무선데이터를 보호하며, TKIP 알고리즘에는 메시지 무결성 확인 기능이 추가되어 있어서 데이터 무결성이 지원된다[14]. 특히, 제 5단계 WPA 보안단계는 상용화 가능성이 가장 높을 것으로 판단되며, 무선단말과 액세스포인트에 사용자가 직접 입력하는 패스워드를 사용하여 인증과 마스터 세션 키 생성을 수행하는 PSK 인증방식을 가정 또는 SOHO 무선 LAN 시스템에 적용하는 모드를 규정함으로써 그 시장성을 넓힘과 동시에 향후 홈 네트워킹으로 진화할 수 있는 여지를 남겨두고 있다.

⑥ 제 6단계: RSN 보안



RSN(Robust Security Network)은 상호인증을 통한 접근제어, 동적인 키 갱신과 강력한 암호 알고리즘을 사용한 새로운 형태의 보안 구조이다. 제 6단계 RSN 보안단계는 RSN 네트워크를 구축한 보안단계로써 제 5단계 WPA 보안기술과 다른 점은 보다 강력한 암호 알고리즘인 CCMP 알고리즘을 기본 알고리즘으로 정의하고 있으며, 장기적인 관점에서 암호 알고리즘 처리 모듈을 하드웨어 칩셋으로 구현하고자 노력한다는 것이다. 국제 표준이 안정화되는 시점에서 칩셋 제조업체의 하드웨어적인 구현이 뒷받침되어질 때 상용화 가능성이 열릴 것이므로 실제 일반 사용자들이 널리 사용할 수 있기까지는 상당한 시일이 걸릴 것으로 예측되며, 현재 사용되고 있는 액세스포인트와 무선 LAN 카드는 모두 교체되어야 할 것이다.

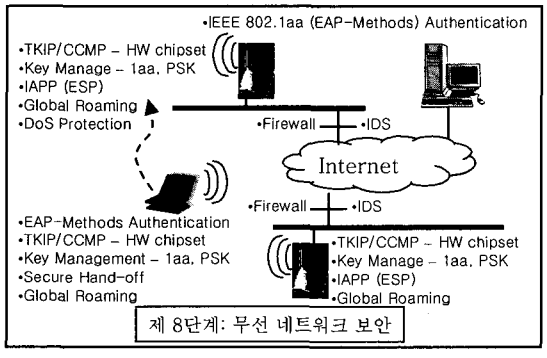
⑦ 제 7단계: 이동 보안



제 7단계 이동 보안단계는 제 6단계 RSN 보안기능을 지닌 액세스포인트에 IEEE 802.11f 규격인 IAPP 기능을 추가하여 무선 LAN 사용자의 안전한 이동성을 보장하는 보안 단계이다. 제 7단계 이동 보안기술의 구현은 무선 LAN 공중망 서비스 사업자가 자사의 무선 LAN 인프라를 보호할 수 있는 가장 높은 단계의 보안정책으로 볼 수 있다.

제 6단계 RSN 보안기술이 하드웨어 칩셋 구현이 필수적인 구현 조건인데 반해 제 7단계 이동 보안기술은 소프트웨어 구현이 가능하므로 제 5단계 WPA 보안단계에 이어 제 7단계 이동 보안기술 상용화로 진화할 수 있을 것으로 예견된다.

⑧ 제 8단계: 무선 네트워크 보안



무선 LAN 보안 기술의 최종적인 목표는 무선 LAN 보안 서비스 제공과 더불어 무선 네트워크 전체를 보호하는 것이다. 이는 동일 사업자 영역에서의 사용자 이동성 지원뿐만 아니라 사업자 영역이 상이한 무선 네트워크를 안전하게 사용할 수 있는 글로벌 로밍 서비스를 포함한다.

Ⅳ. 결론

무선 LAN 서비스의 활용형태가 기업망, 가정/SOHO망, 공중망 등 다양한 장소에서 초고속 무선인터넷 접속 서비스의 인프라로 자리매김하고 있는 추세이다. 무선 LAN 시스템이 공중망 서비스로 진화하여 초고속 무선인터넷 서비스를 제공하기 위해서 반드시 해결되어야 할 과제가 무선 LAN 보안 기술이라는 것은 주지의 사실이다. Ⅲ장 단계적 해결 방안에서 설명하였듯이 무선 LAN 보안 기술의 구현은 단일 기술의 구현이 아니라 IEEE 802.11 워킹그룹의 다양한 연구과제와 IETF 산하 관련 워킹그룹들의 표준화 활동, 그리고 무선 LAN 제품의 상호호환성과 상용화 가능성을 인증하는 Wi-Fi 연합의 표준화 활동이 종합적으로 어우러짐으로써 안전하고 신뢰성있는 무선 LAN 보안 인프라 구축이 실현될 수 있다.

무선 LAN 보안 기술의 단계적 구분이 단순히 보안 강도 강화의 측면에서 구분된 것이 아니라 보안 서비스의 효과여부와 국제 표준의 준용여부를 포괄하여 각 단계를 설정하였기 때문에 실제 무선 LAN 운용을 기획하는 기업체, 가정 또는 공중망 사업자는 현재의 기술개발 수준과 요구되는 보안 서비스 항목을 고려하여 어느 단계의 보안성을 제공할 것인지를 판단해야 한다. 일반적인 보안 요구사항의 최소 항목이라 할 수 있는 사용자 인증과 데이터 기밀성 보장 측면에서 볼 때, 무선 LAN 활용 장소에 상관없이 최소한 제

4단계 동적 WEP 보안 단계는 구현되어 있어야 무선 LAN 위협 요인인 비인가 사용자 접근, 메시지 도청, 데이터 변조, DoS 공격, MITM 공격을 무력화 시킬 수 있다.

고속의 무선 LAN 환경을 보다 더 안전하고 믿을 수 있는 통신 채널로 유지하기 위하여 비도 높은 무선구간 보안기술, 글로벌 로밍을 위한 분산인증, 실시간 패킷 과금, 그리고 본 고에서 예측하지 못한 유무선 통합 네트워크 진화에 따라 발생할 수 있는 보안상의 문제점을 극복하기 위한 지속적인 연구가 필요할 것이다.

참고문헌

[1] Merritt Maxim and David Pollino, "Wireless Security", McGraw-Hill, 2002.

[2] ISO/IEC, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", ISO/IEC 8802-11, ANSI/IEEE Std 802.11, 1999.

[3] IEEE, "Standard for Local and metropolitan area networks- Port-Based Network Access Control", IEEE Std 802.1X, Jun. 2001.

[4] J. R. Walker, "Unsafe at any key size: An analysis of the WEP encapsulation", Tech. Rep. 03628, IEEE 802.11 committee, Mar. 2000.

[5] W. A. Arbaugh, N. Shankar, and Y.C. Justin Wan, "Your 802.11 Wireless Network has No Clothes", Proceedings of the First IEEE International Conference on Wireless LANs and Home Networks, Dec. 2001.

[6] "http://www.interlinknetworks.com/references/Introduction_to_Diameter.html", Feb. 2002.

[7] B. Carney, "Wi-Fi Alliance Update to IEEE 802.11 Publicity Committee," doc.: IEEE 802.11-02/744r0, Nov. 2002.

[8] Wi-Fi Press Release, "http://www.wi-fi.org/OpenSection/ReleaseDisplay.asp?TID=4&ItemID=137&StrYear=2003&strmonth=4", Apr. 2003.

[9] IEEE, "Standard for Local and metropolitan area networks- Port-Based Network Access Control- Amendment 1: Technical and Editorial Corrections", IEEE P802.1aa/D6.1, Jun. 2003.

[10] IEEE, "LAN/MAN Specific Requirements-Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specification: Medium Access Control (MAC) Security Enhancements", IEEE Std 802.11i/D4.0, May. 2003.

[11]"http://www.ietf.org/html.charters/aaa-charter.html," Jan. 2003.

[12] IEEE, "Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation," IEEE Std 802.11f/D5, Jan. 2003.

[13] B. Aboba, "IEEE 802.1X Pre-Authentication," doc.: IEEE 802.11-02/389r1, Jun. 2002.

[14] Wi-Fi Alliance, "Wi-Fi Protected Access," WPA Version 1.2, Dec. 2002.

강 유 성

1997년 전남대학교 전자공학과 학사
1999년 전남대학교 전자공학과 석사
1999년 - 현재 한국전자통신연구원 무선인터넷보안연구팀 연구원

오 경 희

1999년 연세대학교 컴퓨터과학과 학사
2001년 연세대학교 컴퓨터과학과 석사
2001년 - 현재 한국전자통신연구원 무선인터넷보안연구팀 연구원

정 병 호

1981년 3월 1988년 2월 전남대학교 전산통계학과 학사
1998 년 3월 2000년 2월 충남대 컴퓨터과학과 석사
2000년 3월 - 현재 충남대 컴퓨터과학과 박사수료
1988년 2월 2000년 6월 국방과학연구소 선임연구원
2000년 6월 - 현재 한국전자통신연구원 팀장

정 교 일

1981년 2월한양대학교 전자공학과 공학사
1983년 8월한양대학교 산업대학원 전자계산학과 공학석사
1997년 8월한양대학교 대학원 전자공학과 공학박사
1980년 12월 1981년 11월 엠시스템즈 사원
1981년 12월 1982년 2월한국전기통신연구소 위촉연구원
1982년 3월 현재 한국전자통신연구원 정보보호기반연구부장/책임연구원