무선랜 보안기술의 진화동향 및 전망

Trends of the Evolution of Wireless LAN Security Technologies

강유성(Y.S. Kang) 무선인터넷보안연구팀 연구원
오경희(K.H. Oh) 무선인터넷보안연구팀 연구원
정병호(B.H. Chung) 무선인터넷보안연구팀 선임연구원, 팀장

초고속 무선인터넷 사용을 가능하게 하는 무선랜 사용이 확산되면서 무선랜 보안에 대한 관심이 고조되고 있다. 기업 내부망, 가정망에서 뿐만 아니라 공중망 서비스로 진화되면서 무선랜 보안기술은 기존의 비보안 접속 허용 또는 단순한 공유키 형태의 인증 및 암호화 방식에서 벗어나 인증서버를 통한 사용자 인증, 동적 키 교환 및 비도 높은 암호 알고리듬 활용이 요구되고 있다. 본 고에서는 무선랜 보안기술의 표준 규격 제정을 담당하는 국제 표준화 그룹의 현재 활동에 비추어 무선랜 보안기술의 진화동향을 살펴보고, 향후 전망에 관하여 논하고자 한다.

I. 서 론

초고속 무선인터넷에 대한 요구가 급성장하면서 기존의 무선랜(Wireless Local Area Network: WLAN) 시스템이 초고속 무선 공중망의 기반구조로서 그 대안이 되고 있다. 무선랜 시스템이 부각되는 이유는 이동통신 시스템이 가지는 낮은 전송속도를 극복할 수 있으며, 또한 무선랜 시스템의 보안기술 개발이 활발하게 전개되면서 무선랜 사용자의 안전한 통신을 보장할 수 있으리라는 기대 때문이다. 특히 무선구간 전송속도 향상과 더불어 반드시 해결되어야 할 과제가 무선랜 보안기술이며, 이는 무선 공중망을 사용하는 개별 응용에서 지원하는 보안기술과 차별되는 사회 전반적인 보안 인프라로서 구축되어야 한다.

공중망 서비스를 위한 무선랜 구성요소는 무선단말(예, 무선랜 카드가 장착된 노트북 컴퓨터), 액세스포인트(예, Access Point: AP를 지칭하며, 이동통신 시스템의 기지국처럼 다수의 무선단말을 접속시키는 역할도 하고, 무선데이터를 유선인터넷으로 연결시켜 주는 허브/브리지 역할도 수행하는 장치), 그리고 인증서버(예, RADIUS(Remote Authentication Dial In User Service) 서버가 현재 사용 가능한 대표적인 인증서버이며, 사용자 인증 여부를 결정짓는 역할을 수행하는 서버)로 구성된다.

무선단말과 액세스포인트 사이는 무선구간이며, 액세스포인트와 사용자 무선단말에게 인증 서비스를 제공하는 인증서버는 유선구간에 위치한다. 무선단말은 인증과 관련된 정보를 EAPOL(Extensible Authentication Protocol Over LAN) 프레임 형태로 액세스포인트에 전달하고, 액세스포인트는 이들 메시지들 중에 인증서버로 전달하여야 하는 메시지는 AAA(Authentication, Authorization and Accounting) 메시지 형태로 변환하여 전달하고 인증과정을 수행한다. 무선랜은 유선랜과는 달리 기본적으로 모든 단말에 데이터를 전송하는 브로드캐스팅 망이므로, 액세스포인트의 비컨(beacon) 프레임 수신 영역 내에 있는 모든 단말은 다른 사람의 송수신

데이터 내용을 청취할 수 있어서 의도된 수신자 이외의 다른 사람으로부터 데이터를 보호하기 위해서는 기밀성 및 무결성 서비스와 상호인증 서비스가 매우 중요하다.

본 고의 구성은 다음과 같다. II장에서는 무선랜 보안요소와 현재의 무선랜 보안 문제점을 간략하게 살펴보고, III장에서 무선랜 보안기술 표준화를 담당하는 국제 표준화 그룹의 활동을 살펴본다. 그리고, 무선랜 보안기술의 진화동향을 IV장에서 상세히 기술하고, 끝으로 V장에서 향후 전망을 논하며 본 고의 결론을 맺는다.

II. 무선랜 보안 개요

1. 무선랜 보안요소

무선랜 보안을 위한 고려사항은 일반적인 보안 시스템이 지니는 고려사항과 유사하다. 예를 들어, 일반적인 문장 작성에 있어서 기본이 되는 구조가 '언제, 어디서, 누가, 무엇을, 어떻게, 왜'라는 육하원칙에 기반한 문장 구조라면, 일반적인 보안 시스템이 견지해야 하는 기본 구조는 '정당한 사용자가, 정당한 인증을 받고, 정당한 권한으로 접근하여, (사용자가 이동하더라도) 정당한 데이터를 비밀스럽게, 훼손없이 전달하고, 전달된 데이터에 대한 전달 또는 수신 사실 부인을 방지'할 수 있는 보안 서비스 원칙에 기반한 구조여야 한다. 일반적 보안요소에 따라서 다시 정리하면 7가지로 정리할 수 있다.

① 사용자 인증(Authentication) - 정당한 사용자, 정당한 인증
② 접근제어(Access control) - 정당한 사용자, 정당한 인증, 정당한 권한
③ 권한 검증(Authorization) - 정당한 권한
④ 데이터 기밀성(Privacy) - 정당한 데이터를 비밀스럽게
⑤ 데이터 무결성(Integrity) - 정당한 데이터를 훼손없이
⑥ 부인방지(Non-repudiation) - 전달된 데이터에 대한 전달 또는 수신 사실 부인방지
⑦ 안전한 핸드오프(Secure hand-off) - 사용자가 이동하더라도 정당한 데이터를 비밀스럽게, 훼손없이

따라서, 본 고에서는 무선랜 보안 서비스를 위에 정의한 7가지 보안요소에 비추어 무선랜 보안 문제점을 살펴보고, 무선랜 보안기술의 진화동향에 대해서도 각각의 보안요소 만족 여부 및 보안 강도를 중심으로 분석한다.

2. 무선랜 보안 문제점

현재의 무선랜이 가지고 있는 보안요소는 전술한 보안요소 중 2. 접근제어와 4. 데이터 기밀성 지원이다.

접근제어는 사용자 인증을 통해 이루어지는데, 크게 3가지 방법이 있다. 첫째, 허가받은 사용자와 액세스포인트가 동일한 공유 키를 보유하여 접속 요청 시 공유 키 인증방식을 사용하는 방법, 둘째, 허가받은 사용자의 무선랜 카드 MAC(Medium Access Control) 주소를 액세스포인트에 직접 입력시켜 놓는 방법, 끝으로 사용자가 자신의 인증정보를 가지고 인증서버와 인증절차를 수행하는 IEEE 802.1X 인증 방법이다. 데이터 기밀성은 WEP (Wired Equivalent Privacy) 알고리듬을 사용하여 지원되는데, 사용되는 키 길이가 40비트 또는 104비트가 가능하다[1].

만일 무선랜을 기업체 또는 개인이 운용할 경우 허가된 무선랜 카드의 MAC 주소를 액세스포인트에 직접 입력시키고, WEP 알고리듬을 사용하는 등 위의 접근제어 방식과 데이터 기밀성 지원 방식을 사용한다면 무선랜 수신장치만으로 도청을 시도하는 초보 해커의 도청은 막을 수 있다.

그러나, 일반적으로 무선랜 통신기능 자체를 우선시 하기 때문에 액세스포인트의 출고시 상태는 접근제어 관리와 WEP 알고리듬의 사용이 모두 비활성화 되어 있어서 모든 무선랜 카드와 통신을 허락하는 보안상 무방비 상태이다. 따라서 무선랜 관리

자의 세심한 관리가 없으면 어느 누구라도 단지 무선랜 카드가 장착된 노트북 하나만으로 기업체 내부망에서 접근암호를 사용하지 않는 폴더는 모두 들여다 볼 수 있다.

공중망 서비스에서는 공유 키를 사용한다거나 무선랜 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 알고리듬 역시 메시지 도청이 가능한 취약한 알고리듬으로 판명되었기 때문에 현재의 무선랜 보안기능은 전면적으로 보완되어야 한다[2],[3].

무선랜 보안 시스템의 인증서버는 일반적으로 액세스포인트와 안전한 채널을 유지하며, 무선랜 사용자와 EAP 인증 메시지를 교환하여 인증 여부를 판단한다. RADIUS 서버가 대표적인 인증서버이며, 액세스포인트는 RADIUS 메시지를 생성하여 인증서버와 통신하는 RADIUS 클라이언트 역할을 수행한다.

그러나, 최근의 무선랜 환경은 핫스폿(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[4].

III. 무선랜 보안기술 표준화 그룹

무선랜이 공중망 서비스로 발전하고 있는 현 상황에서는 공중망 서비스 사업자, 콘텐츠 제공업체와 사용자 모두의 안전한 통신을 위하여 앞에서 언급한 7가지 보안요소를 모두 만족시키는 새로운 메커니즘이 구현되어야 한다.

무선랜 보안요소 중 1. 사용자 인증, 2. 접근제어, 3. 권한 검증에 대한 국제표준화 활동을 펼치고 있는 곳은 IEEE 802.1X, IEEE 802.1aa 태스크그룹과 IETF EAP, IETF AAA 워킹그룹이며, 4. 데이터 기밀성, 5. 데이터 무결성, 6. 부인방지 기술에 대한 국제표준화 활동은 IEEE 802.11i 태스크그룹이 주도적 역할을 하고 있다. 일반적으로 6. 부인방지 기능은 각각의 응용에서 처리될 수 있으며, 공개키 방식에 기반한 전자서명을 통해 이루어진다. 7. 안전한 핸드오프 기술은 IEEE 802.11i, IEEE 802.11f 태스크그룹이 IETF Seamoby, IETF MobileIP 워킹그룹과 더불어 국제표준 제정을 위해 노력중이다.

1. IEEE 802.1X 태스크그룹

IEEE 802.1X 태스크그룹이 작성하여 2001년 6월에 승인받은 IEEE 802.1X 규격은 사용자 인증을 위한 다양한 인증 프로토콜을 수용하면서 접속포트에 기반한 접근제어 기능을 정의하고 있다[5]. 무선랜 시스템에서도 이러한 포트기반 접근제어를 통해 무선랜 사용자 인증을 수행할 수 있으며, 무선구간 보안에 필요한 마스터 세션 키를 분배할 수 있다. 포트기반 접근제어라 함은 접속허가자(Authenticator)가 접속요구단말(Supplicant)을 각각의 포트로 관리하여 인증서버(Authentication Server)로부터 각 포트별로 접속 허가 여부를 전달받아서 접속요구단말의 네트워크 접근을 제어한다는 것이다. 무선랜 시스템에서는 액세스포인트가 접속허가자 역할을 하게 되고, IEEE 802.1X 인증을 수행하기 위해서는 액세스포인트를 관리하는 네트워크 관리자 영역에 접속요구단말에 대한 인증정보를 가지고 있는 인증서버가 존재하거나 액세스포인트 자체적으로 인증서버 기능을 내장하고 있어야 한다.

2. IEEE 802.1aa 태스크그룹

IEEE 802.1X 포트기반 접근제어는 무선랜 시스

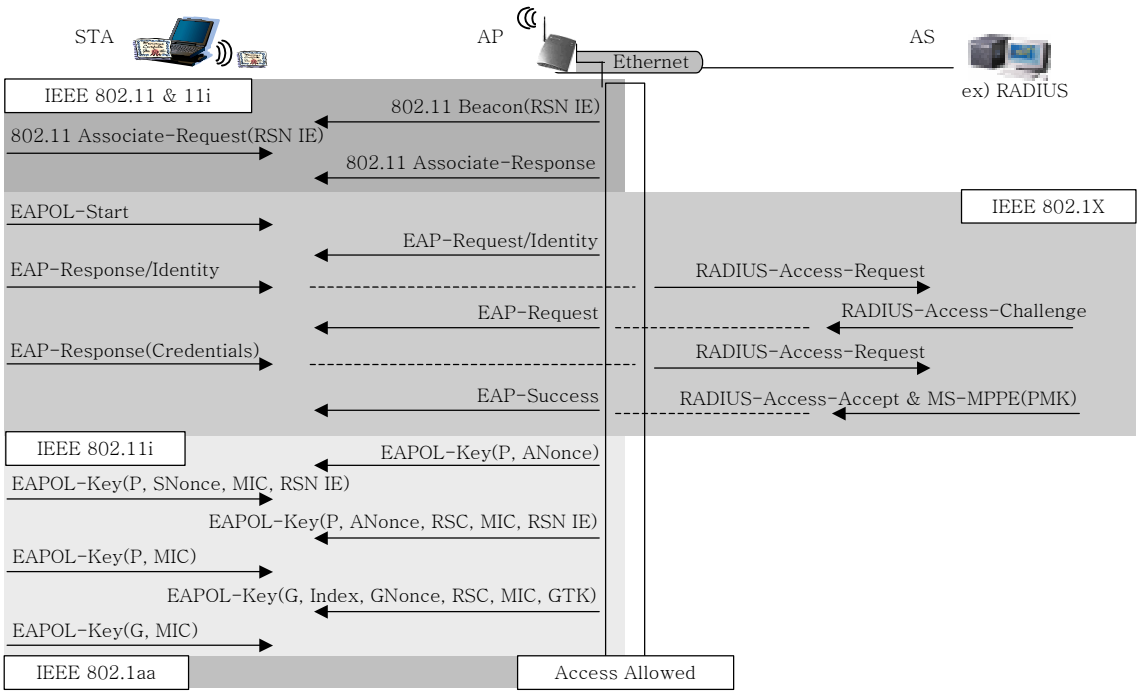
템에서 사용자 인증을 처리하는 중요한 기능임에는 틀림없지만, IEEE 802.1X 규격은 무선구간의 보안을 위한 키 분배 시점 및 키 분배 여부를 사용자 인증에 참조하는 조건을 정의하지 않았기 때문에 IEEE 802.11i 문서에서 규정한 새로운 암호 알고리듬의 암호 키 교환을 지원하기 어렵다. 이는 인증과 키 분배라는 암호학적 프로토콜의 주요 기능을 만족하지 못하는 취약점을 내포하는 원인이 된다. 이를 보완하기 위하여 IEEE 802.1aa 태스크 그룹은 IEEE 802.1aa 드래프트 문서를 발표했는데, 이 문서는 접속요구단말에 대한 인증과 더불어 무선구간 암호 키 분배를 위하여 IEEE 802.11i 규격의 키 서술자(key descriptor)의 수용과 키 분배 상태 머신(state machine)을 정의하고 있는 IEEE 802.1X 규격의 수정 및 추가 문서로 규정할 수 있다[6].

2003년 4월 현재 가장 최신 버전인 2003년 2월 27일에 발표된 IEEE 802.1aa/D5를 살펴볼 때 가장 큰 특징은 portValid라는 변수가 추가되어 port-Status를 제어하는 것인데, 이는 인증과 더불어 무선구간 보호를 위한 암호 키의 교환 여부를 인지하여 무선단말과 액세스포인트 사이에 암호 키 교환이 완료되었을 때 portValid 변수가 동작되어 접속포트를 개방하게 되는 구조로서 무선구간은 무선단말과 액세스포인트 사이에서 교환된 암호 키에 의해 보호받게 된다.

3. IEEE 802.11i 태스크그룹

IEEE 802.11i 규격은 IEEE 802.11 무선랜 시스템이 가지는 무선구간 보안의 취약점을 해결하고자 IEEE 802.1X/1aa 기반 접근제어, 보안 세션 관리, 동적인 키 교환 및 키 관리, 그리고 무선구간 데이터 보호를 위한 새로운 대칭키 암호 알고리듬의 적용 등을 그 내용으로 담고 있다[7].

다시 정리하면, IEEE 802.1X/1aa 규격이 사용자 인증과 키 교환의 틀을 규정하고 있는 반면, IEEE 802.11i 규격은 사용자 인증과 키 교환의 큰 틀로서 IEEE 802.1X/1aa를 사용할 수 있다고 규정하고,



(그림 1) 무선랜 보안 접속 흐름도

나아가 구체적인 키 교환 방식인 4단계 핸드셰이크(4-way handshake) 방식, 교환된 키의 계층적 사용구조(key hierarchy), 그리고 새로운 무선구간 암호 알고리듬(cipher suites)의 정의를 포함하고 있다. (그림 1)은 IEEE 802.1X/1aa 규격과 IEEE 802.11i 규격이 적용되는 무선랜 보안 접속 흐름도를 보이고 있다. 그림에서 보이는 것처럼 인증과 키 교환을 완료해서 액세스포인트를 통한 외부 네트워크 연결이 허가되기 위해서는 IEEE 802.11/11i 접속, IEEE 802.1X 인증, IEEE 802.11i 키 교환, IEEE 802.1aa 인증이 유기적으로 연결되어야 한다.

IEEE 802.11i 태스크그룹은 2002년 3월 D2.0 버전에서 RSN(Robust Security Network) 보안 구조를 드래프트 표준에 반영함으로써 무선구간에서의 데이터 보호기능을 더욱 강화하였다. RSN은 핫스폿에서 IEEE 802.11과 IEEE 802.11i를 지원하는 액세스포인트들이 공존하는 환경에서 IEEE 802.1X를 이용한 가입자 인증 및 키 관리 메커니즘, 무선구간 암호 알고리듬 그리고, 빠르고 안전한 핸드오프 보안 프레임워크를 제시한 새로운 형태의 보안 구조이다.

2003년 4월 현재 가장 최신 버전인 2003년 4월에 발표된 IEEE 802.11i/D3.2 규격을 살펴볼 때 가장 큰 특징은 기존의 무선랜 상용 제품을 소프트웨어 패치(patch)로서 보안기능을 강화할 수 있도록 배려하고 있다는 점이다. 그 첫번째 근거로 TKIP (Temporal Key Integrity Protocol) 암호 알고리듬을 안정화시키고 있다는 것을 예로 들 수 있다. TKIP은 기존의 WEP 알고리듬을 재활용하면서도 키 교환에 의한 동적인 Temporal key와 MIC key의 사용, 2단계의 key mixing 함수, 그리고 Michael로 명명된 MIC(Message Integrity Code) 함수의 사용으로 인하여 데이터 보안기능을 향상시킨 암호 알고리듬으로서 소프트웨어로 구현이 가능하다. 두번째 근거로는 RSN IE(Information Element)를 4단계 핸드셰이크 메시지에 포함시킨 점이다. RSN IE는 무선단말과 액세스포인트 사이의 인증 메커니즘과 암호 알고리듬에 대한 협상 정보를 지닌 메시지로서 MAC association 단계에서 교환되고 협상된다. 이러한 RSN IE를 4단계 핸드셰이크 메시지에 포함시킴으로써 MAC 상위계층에서 RSN IE 정보를 해석할 수 있도록 했으며, 또한 액세스포인트에서 보내는 핸드셰이크 메시지에 제 2의 RSN IE를 추가시킬 수 있는 방식을 제시하여 액세스포인트가 지원하고자 하는 인증 메커니즘과 암호 알고리듬을 강제할 수 있도록 배려하고 있다.

4. IEEE 802.11f 태스크그룹

무선랜 사용자의 안전한 통신을 보장하기 위해서 요구되는 기능 중의 하나가 액세스포인트 사이의 안전한 핸드오프 기능이다. IEEE 802.11f 태스크그룹이 표준화 작업을 진행중인 IEEE 802.11f 규격은 액세스포인트 사이에서 무선단말 접속과 관련된 정보를 전달하는 IAPP(Inter-Access Point Protocol) 프로토콜을 정의하고 있다[8].

액세스포인트 사이의 IAPP 패킷은 IP 계층을 통해 전달되며, 만일 불법 공격자가 IAPP MOVE 패킷을 가로채어 이동중인 무선단말에 관한 정보를 얻게 되면 해당 ESS(Extended Service Set) 안에서 액세스포인트로 행세할 수 있다. 이러한 공격은 모든 IAPP MOVE 패킷과 IAPP ADD 패킷에 대하여 패킷 인증을 제공하여 보호할 수 있는데, IEEE 802.11f 규격에서는 패킷 인증을 위하여 ESP(Encapsulating Security Payload) 보안 어소시에이션(security association)을 제안하고 있다.

특히 2003년 4월 현재 가장 최신 버전인 2003년 1월에 발표된 IEEE 802.11f/D5 규격에서는 IAPP-CACHE-NOTIFY 프리미티브를 새롭게 정의하고 있다. 이는 현재 접속한 무선단말에 관한 컨텍스트를 이웃하는 액세스포인트의 캐시에 미리 저장할 수 있도록 전달해 주기 위한 프리미티브로서 빠른 핸드오프를 지원할 수 있으며, 또한 사전인증(pre-authentication)을 지원할 수 있는 토대가 된다.

5. IETF AAA 워킹그룹

무선단말과 액세스포인트가 IEEE 802.1X/1aa

인증을 수행하기 위해서는 액세스포인트 내부에 인증기능을 처리할 수 있는 모듈을 내장하거나 외부 네트워크를 통해 인증 여부를 알려주는 인증서버와 연결되어 있어야 한다. 현재 상용화되어 있는 대표적인 인증서버는 RADIUS 서버이다. 그러나 무선랜 시스템이 공중망 서비스로 확장되면서 중앙집중형 인증/권한제어/과금 기능을 통합한 AAA 서버가 요구되고 있다. 이러한 요구에 맞추어 IETF AAA 워킹그룹에서는 AAA 프로토콜을 Diameter로 명명하고 그 기능을 구현하고자 표준화를 진행하고 있다[9].

Diameter의 기본 구조는 과금 기능을 포함한 기반 프로토콜(base protocol)과 상위의 다양한 응용기술로 나눌 수 있다. Diameter의 기반 프로토콜은 응용에서 필요로 하는 세션 또는 과금에 대한 관리 등의 기본적인 서비스를 제공하고, AVP(Attribute-Value Pair)의 전달, 노드의 능력(capabilities)에 대한 협상 및 에러 통보 등의 기능을 부가적으로 수행한다. 현재 정의되어 있는 응용으로는, PAP/CHAP 등의 전통적인 인증방식 또는 EAP를 이용한 네트워크 인증 응용(Diameter NASREQ Application), Mobile IPv4 응용(Diameter Mobile IPv4 Application), 노드간 보안 및 종단간 보안을 위한 CMS (Cryptographic Message Syntax) 보안 응용(Diameter CMS Security Application)이 있다. 또한 Diameter는 RADIUS의 단점으로 지적받은 확장성을 보장하기 위해 새로운 응용 식별자(application identifier)와 사업자에 의한 특정 AVP의 추가가 용이한 프레임워크를 가지고 있다[10].

6. IETF EAP 워킹그룹

무선랜 보안의 기본적 요구사항인 사용자 인증을 위한 프로토콜은 다양한 인증 프로토콜이 사용될 수 있다. 예를 들면, MD5-Challenge, TLS(Transport Layer Security)와 같은 일반적인 인증 프로토콜이 사용되어 무선랜 사용자와 인증서버 사이에서 인증기능을 수행한다. IETF EAP 워킹그룹에서 표준화를 진행하고 있는 EAP 프로토콜은 무선랜 사용자와 인증서버 사이의 인증 데이터를 전달해 주는 확장 가능한 인증 프로토콜로 정의될 수 있다[11]. 즉, EAP-MD5, EAP-TLS와 같은 형태로 무선랜 인증 프로토콜이 동작될 수 있으며, 이러한 EAP 메시지는 무선구간에서는 EAPOL 패킷에 실려서 교환되고, 유선구간에서는 RADIUS 프로토콜과 같은 별도의 인증정보 전송 프로토콜에 실려 교환된다[12].

IEEE 802.1X의 포트기반 접근제어 구조에서는 액세스포인트가 제어 포트(controlled port)와 비제어 포트(uncontrolled port)의 2개 포트를 유지하여 비제어 포트를 통해 이러한 EAP 인증 데이터를 인증서버로 전달함으로써 인증절차를 수행하게 된다. 만일 무선구간에서 사용될 키 교환 요구가 없는 경우라면 EAP 인증 이후에 제어 포트가 동작 가능 상태가 되어 무선랜 사용자가 해당 액세스포인트를 통해 무선인터넷 서비스를 받을 수 있게 되고, IEEE 802.1aa 규격처럼 무선구간 암호 키 교환이 요구되는 경우라면 EAP 인증과 더불어 키 교환이 완료되어야 제어 포트가 동작 가능 상태가 된다.

7. Wi-Fi 연합

무선랜 제품의 상호호환성을 인증해 줌으로써 무선랜 서비스의 상용화에 지대한 역할을 하고 있는 무선랜 산업체의 비영리 연합인 Wi-Fi 연합(Wireless-Fidelity Alliance)에서는 무선랜 보안에 대한 자체 규격을 제정하여 WPA(Wi-Fi Protected Access)로 명명하고, 2003년 2월에 WPA 제품에 대한 상호호환성 테스트를 시작하여 2003년 하반기에는 Wi-Fi 인증의 필수 항목으로 규정할 계획을 제시한 바 있다[13].

무선랜 보안기술의 사실상 산업체 표준이 될 것으로 예견되는 WPA 규격은 현재의 Wi-Fi 인증된 무선랜 제품을 소프트웨어 업그레이드를 통해 보안성을 향상시키기 위한 노력의 결실로 나타나게 된 무선랜 보안 규격이다. WPA는 인증 및 키 교환, 그리고 무선구간 암호 알고리듬을 대부분 IEEE 802.11i/D3.0 문서를 참조하도록 제시하고 있어서 IEEE

802.11i/D3.0의 서브셋으로 정의될 수 있다. WPA는 그 설계 목표를 몇 가지로 정리할 수 있는데 대략적으로 살펴보면, 강하고, 호환성이 뛰어나고, WEP을 대체할 수 있고, 소프트웨어 업그레이드로 구현 가능하고, 가정과 기업 모두에 적용될 수 있으며, 즉각 상용화가 가능한 구조를 설계하고자 의도했다.

2003년 4월 현재 가장 최신 버전인 2002년 12월에 발표된 WPA Version 1.2 문서에서는 전술한 설계 목표를 반영하여 인증 및 마스터 세션 키 생성을 위한 메커니즘으로 IEEE 802.1X 규격을 기본 항목으로 설정하고 있으며, 무선구간 암호 알고리듬은 TKIP 알고리듬을 기본 항목으로 지정하고 있다[14].

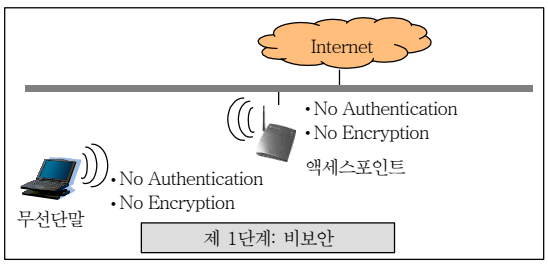
따라서, WPA 구현은 현재 설치되어 있는 무선랜 장치들을 교환하지 않고도 소프트웨어적으로 패치시키는 것만으로도 II장에서 정의한 7가지 무선랜 보안요소 중 1번부터 5번까지를 해결할 수 있으며, 향후 7. 안전한 핸드오프 지원으로 이동성 보안까지 업그레이드 할 수 있는 기반이 된다.

IV. 무선랜 보안기술 진화동향

무선랜 보안기술의 진화과정은 8단계로 요약할 수 있다. 진화단계를 구분하는 주요 요인은 무선랜 보안요소 만족 여부 및 보안 강도이다.

1. 제 1단계: 비보안

II장에서 정의한 무선랜 보안요소 중 아무것도 지원하지 않으며, 보안기능을 요구하지 않는 모든 무선단말과 통신을 허락하는 상태이다. 보안기능 자체가 아예 없는 것으로 볼 수 있다.

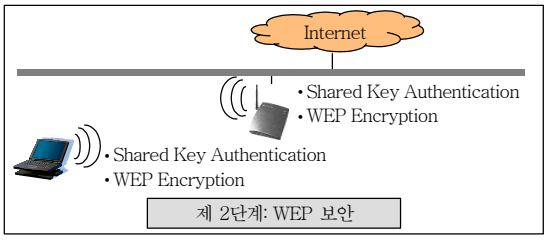


무선랜 액세스포인트를 통한 통신 자체만을 지원하기 때문에 무선랜 카드를 장착한 노트북만으로 네트워크 접근이 가능하다.

2. 제 2단계: WEP 보안

제 2단계 WEP 보안단계는 가장 초보적인 보안기능 제공 상태로서 무선단말과 액세스포인트가 WEP 키를 공유하여 공유 키 인증방식과 WEP 암호화 기능을 수행하는 상태이다. 7가지 보안요소 중 1. 사용자 인증, 2. 접근제어, 4. 데이터 기밀성 기능을 지원한다. 그러나, WEP 알고리듬 자체가 IV(Initialization Vector)의 평문 전송, 키 스트림의 단순성으로 인하여 악의적인 공격자에 의해 WEP 키 값이 노출될 수 있는 취약한 알고리듬인데다 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 무선랜 카드는 제 2단계 WEP 보안을 수행할 수 있다. 따라서 WEP 보안의 사용은 초보적인 무선랜 보안의 시작이다. 그러나, WEP 사용은 데이터 오버헤드로 인한 전송속도의 저하를 가져온다.

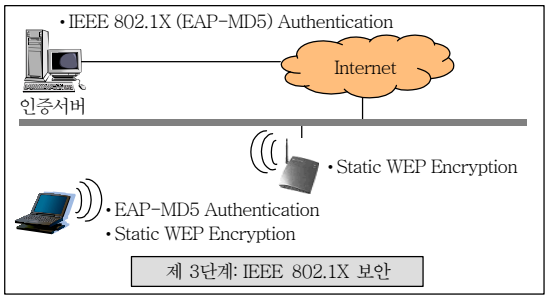


3. 제 3단계: IEEE 802.1X 보안

제 3단계 IEEE 802.1X 보안단계는 인증서버가 사용자 인증을 수행하여 그 결과에 따라 네트워크 접속을 제어하는 방식으로서 공중망 서비스에 적용 가능한 가장 낮은 수준의 보안정책으로 볼 수 있다. 7가지 보안요소 중 1. 사용자 인증, 2. 접근제어, 3. 권한 검증 등 3가지 보안요소를 만족한다. 인증서버

를 별도로 두고 EAP-MD5 인증을 수행하며, 데이터 암호화를 위해 WEP 알고리듬 사용이 가능하다.

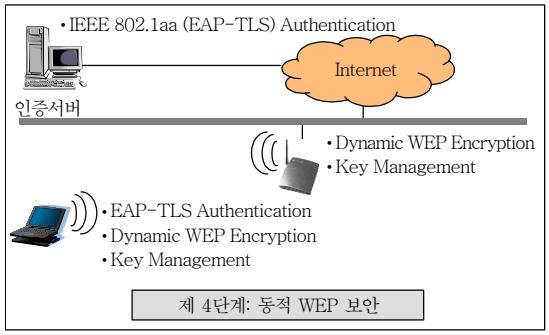
EAP-MD5를 사용하는 IEEE 802.1X 인증 기능을 수행하는 제 3단계 보안단계는 무선랜 공중망 서비스를 위한 기초적인 보안 정책이다. 그러나, WEP 키 공유가 없기 때문에 4. 데이터 기밀성 지원은 없는 상태이며, WEP 키 공유를 한다고 하더라도 동일 사업자의 액세스포인트를 사용할 경우 모두가 동일한 키를 가지게 되어 보안의 의미가 없어진다. 또한 EAP-MD5 인증 방식은 brute force 공격을 통해 사용자의 패스워드가 노출될 수 있는 취약한 방식으로 판명되었기 때문에 무선랜 공중망 서비스를 위해서는 다음에 소개되는 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 적용이 지원되는 보안 단계이다. 7가지 보안요소 중 1. 사용자 인증, 2. 접근제어, 3. 권한 검증, 4. 데이터 기밀성 지원 등 4가지 보안요소를 만족하는데, 제 3단계 보안과는 다르게 EAP-TLS를 사용하는 IEEE 802.1aa 인증을 통해 상호인증이 가능하고, 접속하는 각각의 무선단말마다 IEEE 802.11i 규격의 4단계 핸드셰이크 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 계산 능력을 가지고 공격해야 하는 악의적인 공격자의 WEP 공격을 무력화시킬 수 있다.

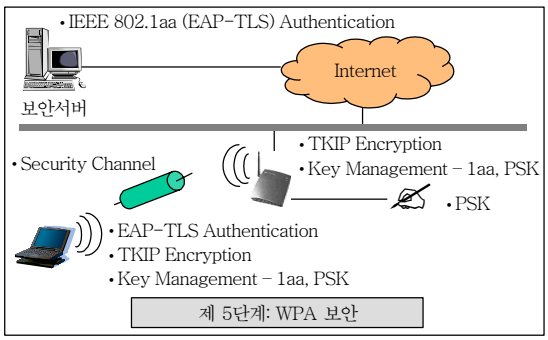
무선랜 사용자 인증과 무선구간 암호 키 교환 기술이 적용된 제 4단계 동적 WEP 보안단계는 현재의 무선랜 시스템이 가지는 보안상의 취약점을 상당 부분 해결할 수 있다는 점에서 의의가 있다. 또한 무선단말과 액세스포인트에 소프트웨어적으로 패치하여 손쉽게 사용할 수 있기 때문에 향후 가정망, 기업망, 그리고 공중 액세스망 등에서 안전한 통신 보안성 강화에 크게 기여할 수 있는 무선랜 보안 시스템이다.

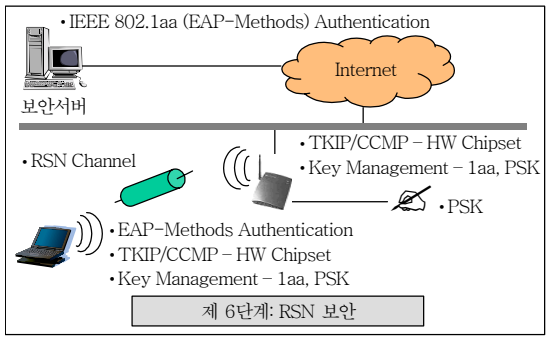


5. 제 5단계: WPA 보안

제 5단계 WPA 보안단계는 Wi-Fi에서 제정한 무선랜 보안 규격인 WPA 규격을 준수한 보안기술로서 제 4단계 무선랜 보안기술에 덧붙여 무선구간 암호 알고리듬으로 TKIP을 사용하는 보안 단계이다. 7가지 보안요소 중 1. 사용자 인증, 2. 접근제어, 3. 권한 검증, 4. 데이터 기밀성, 5. 데이터 무결성 등 5가지 보안요소를 만족한다. EAP-TLS를 사용한 IEEE 802.1X 인증 및 IEEE 802.11i 4단계 핸드셰이크 키 교환이 완료된 이후에 동적으로 결정된 키를 TKIP 알고리듬에 적용함으로써 무선데이터를 보호하며, TKIP 알고리듬에는 메시지 무결성 확인 기능이 추가되어 있어서 데이터 무결성이 지원된다.

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 (Pre-Shared Key) 인증방식을 가정 또는 SOHO





(Small-Office Home-Office) 무선랜 시스템에 적용하는 모드를 규정함으로써 그 시장성을 넓힘과 동시에 향후 홈 네트워킹으로 진화할 수 있는 여지를 남겨두고 있다.

6. 제 6단계: RSN 보안

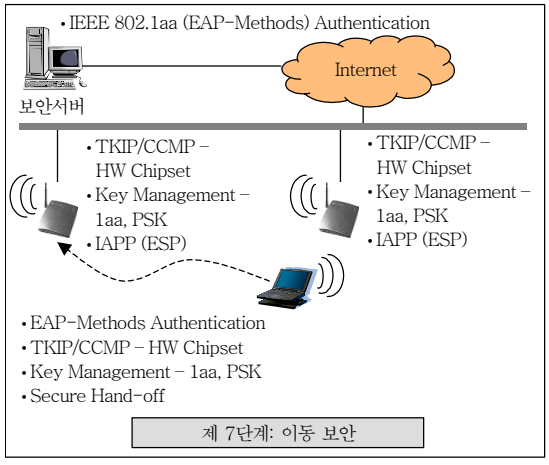
RSN은 상호인증을 통한 접근제어, 동적인 키 갱신과 강력한 암호 알고리듬을 사용한 새로운 형태의 보안 구조이다. 제 6단계 RSN 보안단계는 RSN 네트워크를 구축한 보안단계로서 무선랜 보안요소 중 1. 사용자 인증, 2. 접근제어, 3. 권한 검증, 4. 데이터 기밀성, 5. 데이터 무결성 등 5가지 보안요소를 만족한다. 제 5단계 WPA 보안기술과 다른 점은 보다 강력한 암호 알고리듬인 CCMP 알고리듬을 기본 알고리듬으로 정의하고 있으며, 장기적인 관점에서 암호 알고리듬 처리 모듈을 하드웨어 칩셋으로 구현하고자 노력한다는 것이다.

국제표준이 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 무선랜 카드는 모두 교체되어야 할 것이다.

7. 제 7단계: 이동 보안

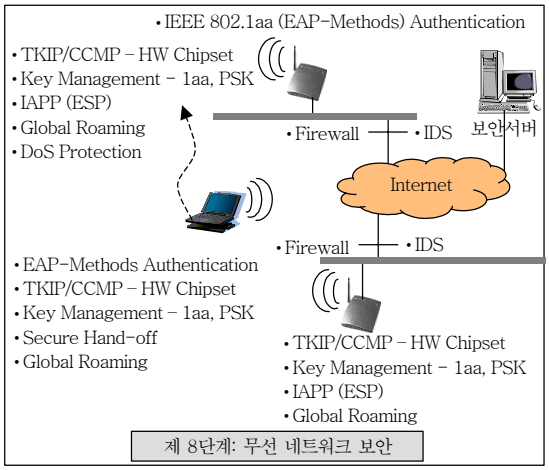
제 7단계 이동 보안단계는 제 6단계 RSN 보안기능을 지닌 액세스포인트에 IEEE 802.11f 규격인 IAPP(Iner-AP Protocol) 기능을 추가하여 무선랜 사용자의 안전한 이동성을 보장하는 보안 단계이다. 제 7단계 보안기술이 구현되면 7가지 보안요소 중 1. 사용자 인증, 2. 접근제어, 3. 권한 검증, 4. 데이터 기밀성, 5. 데이터 무결성, 7. 안전한 핸드오프 지원 등 6가지 보안요소를 만족하게 된다. 제 7단계 이동 보안기술의 구현은 무선랜 공중망 서비스 사업자가 자사의 무선랜 인프라를 보호할 수 있는 가장 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

무선랜 보안기술의 최종적인 목표는 무선랜 보안



요소 만족과 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.

V. 결 론

무선랜 공중망 서비스에서 안전한 보안 인프라 구축은 무선랜 사용자들에게 신뢰성 보장이라는 사이버 세상의 유지조건을 만족시키는 중요한 과제이다.

이상의 무선랜 보안기술의 표준화 활동과 무선랜 보안구조의 진화동향에서 살펴 보았듯이 무선랜 보안은 단일 기술의 구현이 아니라 IEEE 802.11 워킹그룹의 다양한 연구과제와 IETF 산하 관련 워킹그룹들의 표준화 활동, 그리고 Wi-Fi의 표준화 활동이 종합적으로 통합 구현되어야 한다. 이는 안전하고 신뢰성있는 무선랜 보안 인프라를 구축하고 향후 유무선 통합 네트워크 보안 시스템을 위한 초석을 마련하는 길이다.

IV장에서 설명한 무선랜 보안기술의 진화단계 중 제 8단계 무선 네트워크 보안단계는 방화벽, 침입탐지 기능, 그리고 서비스 거부 공격 방어와 같은 유선 네트워크에서 사용되던 다양한 보안기능을 통합, 융합하여 무선랜 사용자에게 신뢰성있는 무선 접속을 보장할 수 있는 무선랜 보안 구조이다. 무선랜 보안 기술 표준 규격은 제 8단계 무선 네트워크 보안을 목표로 표준화 작업이 진행될 것이다.

그리고, 향후에도 고속의 무선랜 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.

참 고 문 헌

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

[2] J.R. Walker, *Unsafe at Any Key Size; An Analysis of the WEP Encapsulation,* Tech. Rep. 03628, IEEE 802.11 Committee, Mar. 2000.

[3] 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.

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

[5] IEEE, *Standard for Local and Metropolitan Area Networks-Port-Based Network Access Control*, IEEE Std 802.1X, June 2001.

[6] IEEE, *Standard for Local and Metropolitan Area Networks-Port-Based Network Access Control-Amendment 1: Technical and Editorial Corrections,* IEEE P802.1aa/D5, Feb. 2003.

[7] IEEE, *LAN/MAN Specific Requirements- Part 11: Wireless Medium Access Control(MAC) and Physical Layer(PHY) Specification: Specification for Robust Security*, IEEE Std 802.11i/D3.2, Apr. 2003.

[8] 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.

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

[10] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "Diameter Base Protocol," draft-ietf-aaa-diameter-17.txt, IETF Work in progress, Dec. 2002.
[11] http://www.ietf.org/html.charters/eap-charter.html, Jan. 2003.
[12] L. Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol(EAP)," RFC 2284, Mar. 1998.
[13] B. Carney, "Wi-Fi Alliance Update to IEEE 802.11 Publicity Committee," doc.: IEEE 802.11-02/744r0, Nov. 2002.
[14] Wi-Fi Alliance, "Wi-Fi Protected Access," WPA Version 1.2, Dec. 2002.