네트워크 보안 기술 동향

▮ 차영태, 권일환 / 시큐아이닷컴

본 논문에서는 네트워 보안에서 중요한 기술인 IPSEC 보안을 중심으로 최근에 많이 논의되고 있는 VoIP와 무선랜의 보안을 살펴본다.

서 론

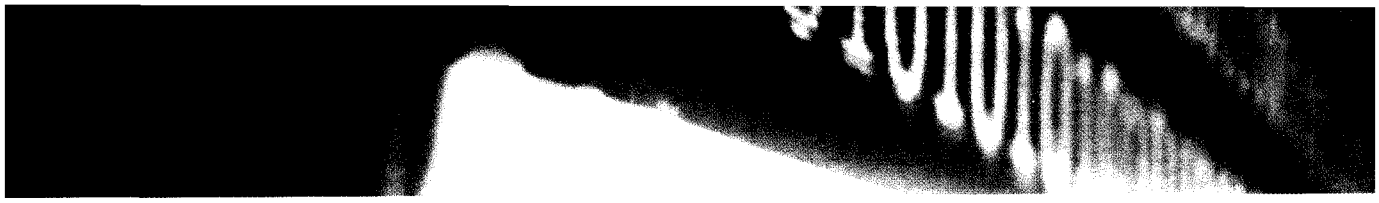
보안 기술은 정보를 교환할 때 원하는 대상에게 원하는 정보를 주기 위한 기술로써 기술적인 용어를 사용하면 다음의 다섯 가지 성질을 부여하기 위한 것이다.

- Secrecy: 정보의 암호성(비밀성)
- Authenticity : 정보의 사용자 인증(확인)
- Integrity: 정보의 순수성 혹은 불변성 확인 (메시지의 인증이라고도 하며, 인증이라는 용어를 사용자 인증과 메시지의 인증을 합하여 사용함)
- Access control: 정보의 사용 허가
- Nonrepudiation: 정보에 대한 부인 봉쇄

이와 같은 성질을 부여하기 위한 보안 기술은 DES, IDEA, AES로 대표되는 비밀키 및 RSA, DSA로 대표되는 공개키의 기본적인 알고리즘을 사용하여 원하는 목적을 얻을 수 있도록 하는 보안 프로토콜을 통하여 이루어진다. 요약하여 말하면 보안 기술은 비밀키, 공개키 알고리즘, 보안 프로토콜 및 전체적인 키관리(key management) 기술로 이루어진다고 할 수 있다.

최근 통신 기술의 급속한 발전으로 전 세계가 네트웍으로 연결되어 정보의 공유가 이루어짐에 따라 보안성의 확보가 매우 중요한 관건으로 떠오르게 되었다. 네트웍에서 보안성을 확보하려면 우선 네트웍을 구성하는 다양한 요소 즉 호스트, 허브, 라우터, 게이트웨이, 스위치에 필요한 보안 기술을 부여하여야 한다. 이를 더욱 자세히 보면 네트웍 구성 요소에 구현된 통신 프로토콜에 보안 기술을 부여하여야 하는 것이며, 통신 프로토콜의 필요한 계층에 필요한 성질을 갖는 보안 기술을 부여하여 전체 네트웍이 사용자가 사용하기 편리하며 secure한 네트웍이 되도록 하는 것이다. 따라서 기술적으로 보면 어떤 계층에 보안성을 부여하느냐가 중요한 선택 요인이 된다.

IPSEC 프로토콜은 IP 계층 즉 네트웍 계층에 보안 기술을 부여하는 것이다. 이 방법의 장점은 호스트 즉 일반 PC 및 서버뿐만 아니라 각종 네트웍 구성 요소 즉 라우터, 게이트웨이, 스위치 등에도 사용이 가능하며 나아가 VPN (Virtual Private Network) 처럼 좋은 application을 제공할 수 있다는 것이다. 이러한 IPSEC의 장점은 다른 여러 네트워크 기술, 즉 최근에 많이 논의가 되고 있는 VoIP (Voice over IP) 및 WLAN (Wireless LAN)의 보안 기술로도 사용이 가능하다. 본 논문에서는 IPSEC을 중심으로 VoIP와 WLAN의 보안 기술을 개괄적으로 소개한다.



IPSEC 기술

네트웍 계층에 보안 기술을 부여하는 것은 암호 및 인증을 IP 패킷을 바탕으로 이루는 것을 뜻하며, IP 패킷은 네트웍 상에서 전송되는 실제 데이터 형태이므로 호스트 뿐만 아니라 라우터나 게이트웨이 등 각 네트웍 구성 요소에 공히 사용될 수 있으며 이를 도시하면 그림 1과 같다. 그림 1에서는 네트웍 계층에 보안 기술을 부여할 때 암호 및 인증이 가능한 4가지 경우를 보여준다. 여기서 중요한 것은 라우터에 보안 기술을 부여하여 각 라우터가 담당하고 있는 영역 (domain) 전체의 보안을 담당하게 할 수 있다는 점이다. 더욱이 호스트 1이 dial-up으로 원격 접속을 원하는 경우에는 그림 1에서 라우터 1을 없앤 경우로 생각할 수 있으며, 이 경우 원격 접속을 원하는 호스트 1과 라우터 2가 보안을 담당하게 되면 원격 접속도 용이하게 할 수 있게 된다. VPN과 원격 접속 문제는 각각이 많은 수요를 가지고 있어 IPSEC 기술이 광범위한 지지를 받고 있다.

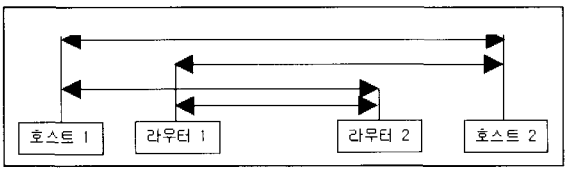


그림 1 가능한 4가지 암호 및 인증 범위

그림 1에서 라우터에 포함되는 보안 기술만 분리하여 독립적인 hardware device가 담당하게 하면 라우터와 보안 장비를 연계하여 사용하게 되며, 이렇게 하는 것이 오히려 보안 측면에서는 선호된다. 그 이유는 라우터가 보안을 담당하게 되면 라우터의 다른 기능을 통하여 해커가 침입하는 것이 가능할 수도 있어 보안에 위협이 되나, 보안 장비와 라우터를 분리하면 보안 장비는 보안만 담당하게 하여 침입을 원천 봉쇄할 수 있기 때문이다.

IPSEC 프로토콜은 IPv4와 IPv6에서 공통적으로 사용되며, 구체적으로 살펴보면 암호를 위한 ESP (Encapsulating Security Payload) 프로토콜, 인증을 위한 AH (Authentication Header) 프로토콜, secure 통신을 담당하는 두 entity간에 정보 공유를 위하여 프로토콜의 framework을 정의한 ISAKMP (Internet Security Association and Key Management Protocol) 프로토콜, 키교환을 위한 프로토콜인 IKE (Internet Key Exchange) 프로토콜 및 전체의 security architecture로 구성되어 있다.

AH 및 ESP 프로토콜과 사용 방법

AH 및 ESP 프로토콜은 header와 trailer로 이루어진 프로토콜로써 각각 IP패킷을 인증 및 암호화하는 프로토콜이며, encapsulation 방법에 따라 ESP 패킷의 payload에 IP패킷의 일부분 혹은 전체가 들어가게 된다. 사용되는 암호 및 인증 알고리즘은 여러 가지 알고리즘 중에서 선택하여 지정할 수 있도록 되어 있다.

ESP와 AH프로토콜을 IP 프로토콜과 연계하여 사용하는 방법인 Encapsulation 방법은 transport mode와 tunnel mode의 두 가지가 있으며 그림 2에 도시하였다. 그림 2에서는 ESP header 와 AH header를 합쳐 IPSEC header라 표시한다. 그림 2에서 쉽게 알 수 있듯이 tunneling mode에서는 기존의 패킷을 모두 새로운 header를 이용하여 encapsulate하는 반면에 transport mode에서는 기존의 패킷에 필요한 header만을 첨가하게 된다. 패킷의 크기 면에서는 transport mode가 장점이 있으나, 보안면에서는 원래 IP header까지 모두 암호화할 수 있다는 면에서 tunneling mode가 장점이 있다. Transport mode는 end-to-end의 보안이 요구되는 상황에서 주로 사용되며 tunneling mode는 패킷

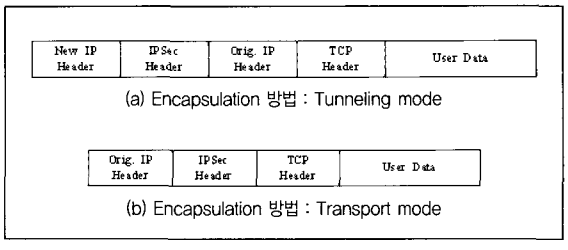


그림 2 Encapsulation의 두가지 방법

을 생성한 기기가 보안 서비스를 적용하는 기기와 다르거나 보안이 유지되어야 하는 마지막 지점이 패킷의 도착점과 다른 경우 쓰인다. 따라서 호스트에서는 두 가지 방법을 모두 사용할 수 있으나 tunneling mode는 주로 게이트웨이에서 쓰인다.

ISAKMP (Internet Security Association and Key Management Protocol) 와 IKE (Internet Key Exchange) 프로토콜

IPSEC 프로토콜에서 중요한 개념 중 하나인 SA (Security Association) 는 secure 통신을 원하는 양자 혹은 다자간에 필요한 모든 정보를 말한다. SA는 사용되는 IPSec 프로토콜의 종류, 데이터의 변형방법, 암호화 키, 세션 유지기간 등의 정보를 포함하며 단방향성을 갖는다. 단방향성이란 예를 들어 호스트 A와 B가 ESP를 통해서 통신을 할 경우 A와 B는 각각 SAin과 SAout을 생성하며 A의 SAin과 B의 SAout이, 그리고 A의 SAout과 B의SAin이 같은 정보를 공유하게 된다는 뜻이다. SA는 또한 프로토콜 종속적이며 AH와 ESP는 각각의 SA를 만들게 된다. ISAKMP는 인터넷 상에서 보안 서비스를 제공하기 위하여 인증, 키관리 및 SA의 개념을 모두 합하여, SA를 확립 (establish), 협상 (negotiate), 수정 (modify), 삭제 (delete) 하는 프로토콜이다. 자세히 말하면 ISAKMP 프로토콜은 매우 포괄적인 프로토콜로써 여러 가지 키교환 (key exchange) 프로토콜을 사용할 수 있도록 패킷의 형태와 전반적인 과정 (procedure) 을 정의한다. 따라서 패킷의 형태를 보면 ISAKMP header가 새로 정의되고 Security Association Payload, Key Exchange Payload, Certificate Payload등 필요한 여러 가지 payload가 정의된다.

IKE 프로토콜은 구체적인 키교환 프로토콜로써 ISAKMP 프로토콜과 연동하여 사용할 수 있다. 즉 secure 통신을 위하여 필요한 메시지와 각각의 메시지에서 전달되는 구체적인 형태를 이미 설명한 각종 ISAKMP payload를 이용하여 정의한다. 기술적으로 말하면 IKE 프로토콜은 Diffie와 Hellman 키교환 프로토콜의 변형인 STS (Station To Station) 키교환 프로토콜을 ISAKMP의 구조 (framework) 에 맞춰 인터넷에서 사용할 수 있게 한 프로토콜이다.

SA (Security Association) 를 사용하는 방법

이 절에서는 호스트나 보안 게이트웨이에서 사용하는 여러 가지 SA의 사용법을 그림 3에서 설명한다. 이 방법 외에도 SA를 결합하여 사용하는 다른 방법도 사용할 수 있다. 그림 3에서 (a)의 경우는 가장 기본적인 경우이며 각 호스트에서 tunneling mode나 transport mode를 모두 사용할 수 있다. 다음으로 (b)의 경우는 각 영역의 보안을 SG (Security Gateway) 에서 담당하는VPN의 경우이며, 이 경우는 각 게이트웨이에서 tunneling mode만 사용할 수 있다. 다음으로 (c)의 경우는 (a)와(b)를 결합하여 사용하는 경우이며 각 호스트나 게이트웨이에 다른 특별한 조건은 없다. 마지막으로 (d)의 경우는 원격 사용자가 게이트웨이를 거쳐 다른 서버 (H2) 에 접속하는 경우로 호스트 (H1) 와 게이트웨이 (SG2) 사

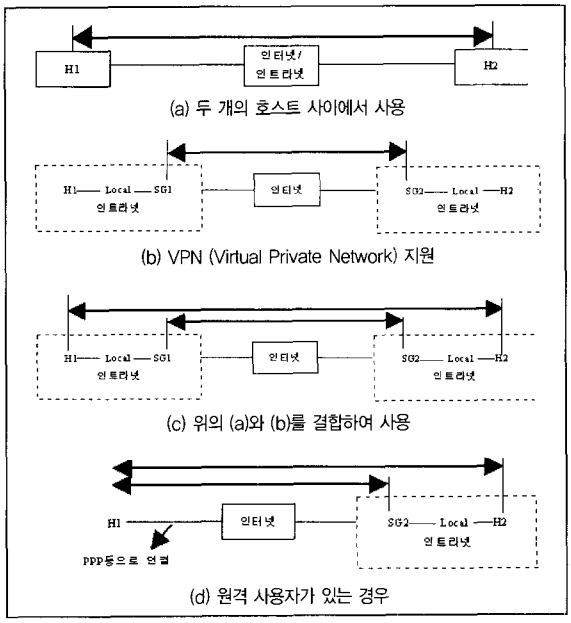


그림 3 Security Association의 사용 방법

이에서는 반드시 tunneling mode만을 사용하여야 한다.

IPSEC 프로토콜의 사용처

IPSEC 프로토콜은 IPv4에서는 선택 사항으로, IPv6에서는 강제 사항으로 되어 있으므로 우선 인터넷 프로토콜이 IPv6로 이행하면 각종 통신 장비에서 반드시 IPSEC 프로토콜을 지원하여야 한다. IPSEC 프로토콜의 대표적인 응용 분야로는 VPN (Virtual Private Network) 과 원격 접속을 들 수 있다. 뒤에서 설명하는 VoIP와 무선랜 보안 이외에도 mobile-IP에서도 보안을 위하여 IPSEC 프로토콜의 사용을 검토하고 있으며, 멀티미디어 서비스를 위한 RSVP (Resource ReSerVation Protocol) 에서도 원래의 프로토콜을 변형하여 IPSEC 프로토콜의 사용을 검토하고 있다. 따라서 보안을 위하여 IPSEC 프로토콜은 새로운 서비스를 위한 여러가지 인터넷 프로토콜에 공통적으로 사용되리라 본다.

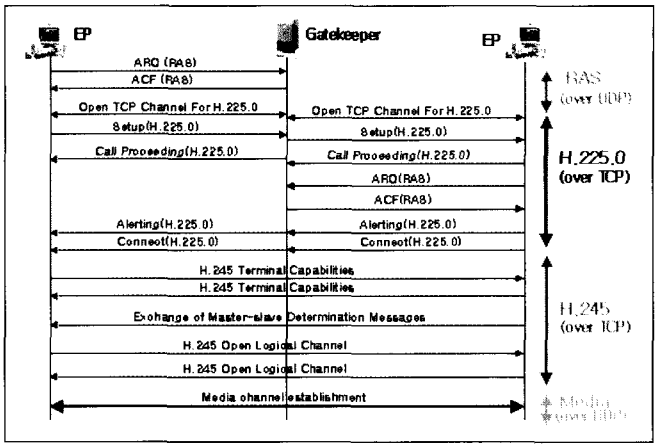


그림 4 Gatekeeper routed model에서의 호 처리 절차

VoIP 보안 기술

VoIP (Voice over Internet Protocol) 기술은 인터넷을 이용하여 전화 및 전화 응용서비스를 구현하는 기술이다. PC-to-PC 방식의 인터넷전화 애플리케이션이 등장한 이래 장거리전화 서비스의 상당 부분을 차지할 정도로 활용이 늘어나고 있으며, 음성품질도 많이 향상되어 이제는 향후의 음성통신을 VoIP 기술이 주도할 것으로 시각이 점차 바뀌어가고 있다. VoIP 기술은 ITU-T가 주도하는 H.323계열과 IETF가 주도하는 SIP 계열이 있다. 현재 표준안의 미흡과 업체간 입장차이로 인해 발걸음이 더딘 상태이나 네트웍의 중요한 기술이므로 H.323 프로토콜 및 이의 보안 기술을 살펴본다.

VoIP 프로토콜 개요

H.323 프로토콜이 그림 4에 표시되어 있다. Gatekeeper는 단말기 및 게이트웨이 등을 위한 주소 변환, 접근 제어 등을 행하는 핵심 구성요소이며, H.225.0에 정해진 RAS (Registration, Admission and Status) 메시지를 이용하여 정보를 교환한다. H.323을 구성하는 프로토콜 스택은 크게 RAS, H.225.0 call signaling, H.245 control signaling, 오디오 코덱, 비디오 코덱 등이다. RAS는 단말기나 게이트웨이가 게이트키퍼에 등록을 하기 위한 메시지와 절차를 정의하고 있다. H.225.0은 상대방을 호출하기 위한 메시지를 송수신하는 규약으로 TCP와 같은 신뢰성 있는 통신 프로토콜을 이용한다. H.245는 단말기의 기능을 주고받는 규약으로써 데이터, 음성 및 영상 정보 송수신을 위한 컨트롤 및 상태 정보를 전송하는 프로토콜이다. 실제 음성 및 영상 정보는 실시간성을 위한 인터넷 프로토콜인 RTP(Real Time Protocol) 와 RTCP(Real Time Control Protocol)를 이용하여 전송하게 된다. RTP는 UDP(User Datagram Protocol)를 기반으로 하여 유니캐스트 및 멀티캐스트를 이용하여 음성 및 영상 정보를 전송하며, RTCP는 RTP를 이용하여 전송되는 데이터의 지연(delay), 지터(jitter) 및 동기를 컨트롤하는 정보를 송수신하기 위한 프로토콜이다.

VoIP 보안 기술

어떤 프로토콜에 보안 기술을 추가하기 위해서는

주어진 프로토콜의 필요한 부분에 보안 메시지를 추가하는 방법과 앞에서 설명한 IPSEC과 같이 검증된 보안 기술을 사용하는 방법이 있다. 전자는 새로운 보안 프로토콜을 설계하는 것이므로 비효율적이며 보안성 검증에 상당한 위험부담이 따른다. 하지만 후자에 비해 주어진 프로토콜을 이용하여 필요한 보안 메시지를 추가하여 설계할 수 있으므로 전체적인 프로토콜을 최적화할 수 있다는 장점이 있다.

Built-in Security Mechanism 이용

H.323프로토콜에서는 보안을 위해 새로이 설계된 H.235를 제시하고 있다. H.235의 권고안은 인증과 무결성 그리고 비밀성을 제공하기 위한 것이다. 우선 등록 및 호 설정/제어에 관한 보안을 위하여 H.235는 단말의 등록 및 호 설정 및 제어에 관한 메시지 (RAS, H.225.0 그리고 H.245)의 인증 및 무결성만을 제공한다. 이러한 메시지들의 비밀성 기능을 제공하기 위해서는 IPSEC이나 TLS(Transport Layer Security) 등의 IP기반 보안 도구를 추가로 사용해야 한다.

H.235 문서에서 제시하는 보안 서비스를 호 처리 신호의 흐름에 따라 간략히 나타내면 그림 5의 상단과 같이 나타낼 수 있다. RAS 메시지 전송에서는, 패스워드기반의 암호화나 인증서에 의해, 사용자 인증과 메시지 무결성의 기능을 제공한다. H.225.0의 경우도 패스워드나 혹은 인증서 기반의 서명으로 인증과 무결성 보안 서비스를 제공한다. H.245의 경우는 H.225.0과 같은 TCP 채널을 사용하는데 H.245 메시지를 전송을 위한 새로운 TCP 포트를 열지 않고 H.225.0 메시지 전송 포트를 이용하여 H.245 메시지를 터널링하여 전송한다.

음성 데이터의 보안 미디어 채널을 안전하게 하기 위해서 H.323은 RTP의 보안체계를 이용한다. RTP에서는 비밀성 기능을 제공하기 위해 대칭키 블록 암호화 기법 (DES, RC2 compatible, triple-DES)을 사용하고, 미디어 데이터를 암호화하는데 사용되는 세션키는 H.245 메시지 전송 시에 전달된다. 그림 5의 하단은 음성데이터의 보안을 나타내고 있다.

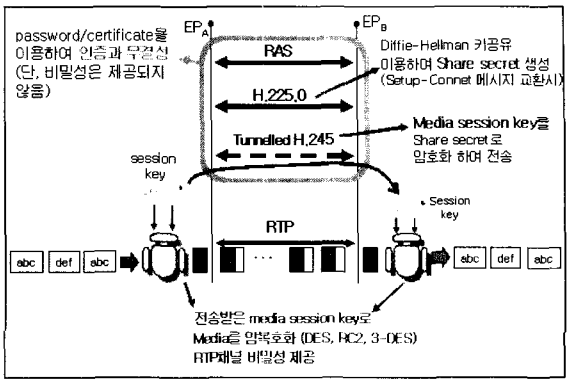


그림 5 Call signalling 과 media stream에 관한 security flow

IP 기반 보안 시스템을 이용

안전한 VoIP 프로토콜을 제공하기 위한 방법론 중의 하나는 IPSec과 같이 잘 정립되어 있고 널리 사용되는 기존의 인터넷 프로토콜 보안기술을 이용하는 것이다. 이는 보안 전문가들에 의해 검증된 기존의 보안 인프라를 재사용함으로써 안전성을 보장받고 개발기간을 단축시킬 수 있으며 중복 투자를 피할 수 있으므로 대부분의 응용 프로토콜에서 추구하는 가장 일반적인 접근방법이다.

H.323 프로토콜은 응용계층으로 보고 보안은 IP 계층에서 처리하여 상호간의 독립적으로 동작하여 상위 계층에서는 보안 프로세스가 전혀 고려하지 않아도 되는 형태가 가능하다. 즉 그림 6과 같이 H.323 단말에서는 보안에 대한 어떠한 동작도 수행하지 않고 IPSec이 미디어 채널의 비밀성과 호 설정 및 제어에 관련된 메시지들의 인증 및 비밀성 기능까지 제공하게 된다. 패킷들은 IPSec의 터널링 모드로 전송된다.

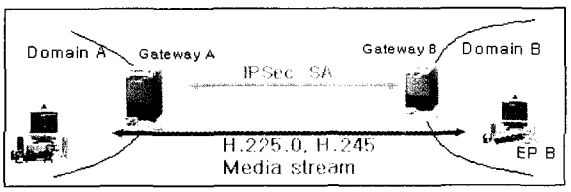


그림 6 IPSec의 터널링 모드를 사용한 H.323

무선랜 보안 기술

무선랜(WLAN)은 IEEE의 802.11x MAC프로토콜에 기반한 근거리 무선통신 체계이며 현재 1997년에 제정된 802.11b가 가장 많이 쓰이고 있다. 802.11b는 2.4GHz대의 대역폭에서 DSSS(Direct Sequence Spread Spectrum) 방식을 사용하여 11Mbps의 속도를 내며 이 외에 OFDM(Orthogonal Frequency Division Multiplexing) 방식으로 같은 2.4GHz대역에서 22Mbps(Turbo mode의 경우 +50Mbps)의 속도를 내는 802.11a와 5GHz대역에서 최대 54Mbps의 속도를 낼 수 있는 802.11a등이 있다.

무선랜과 유선랜의 차이는 크게 전송 미디움(medium)과 사용자의 mobility로 구분할 수 있다.

■ 전송 미디움

무선랜 망은 하나의 AP를 중심으로 형성되는 셀(Cell)을 기본단위로 한 BSS(Basic Service Set)과 이 BSS들이 모인 ESS(Extended Service Set)으로 구성된다. 유선랜 망에서는 특정 목적지 주소를 갖는 데이터 패킷의 경우 통신선로를 타고 그 목적지로만 전달되는 반면, 무선 망에서는 AP(Access Point)에 의해서 불특정 다수에게 방송된다.

■ Mobility

유선랜 상에서의 사용자는 움직이지 않고 고정된 위치에서 통신을 하는 특성이 있는 반면, 무선랜 사용자는 BSS들을 자유롭게 돌아다니며 통신이 가능하다.

위에서 살펴 본 것과 같이 방송이라는 무선랜의 전송특성 때문에 무선랜은 도청 및 packet hijacking의 공격에 항상 노출되어 있다. 이는 TV를 생각하면 쉽게 이해할 수 있는데, TV가 수신 가능한 지역에서 간단하게 TV를 켜는 것 만으로 TV를 시청할 수 있듯이 무선랜에서는 하나의 BSS에 속한 사용자는 단순한 조작만으로 같은 BSS에 속한 다른 사용자들의 통신내용을 쉽게 수신할 수 있다. 또한 사용자는 한 BSS에서 다른 BSS로 자유롭게 움직일 수 있기 때문에 사용자의 관리가 어려우며 관리되지 않는 AP를 설치 할 경우 보안의 back-door로 작용하게 된다.

유선 망에서는 외부로부터의 공격은 방화벽으로 막고 외부와의 통신은 VPN으로 막는 이중화 구조가 전부였다. 반면 무선랜에서는 내부망에 위치해 있더라도 암호화가 필요하며 각각의 AP에 접근하기 위해서 사용자의 인증 및 식별이 필요함과 동시에 AP 역시 관리되어야 하는 보다 복잡한 구조를 갖는다. 무선랜에서의 보안 이슈를 정리하면 크게 다음의 세 가지로 구분될 수 있다.

- 사용자 식별 및 인증 : 무선랜에 접근하는 사용자는 접근 권한이 있는지 식별 및 인증을 거쳐야 한다.
- 암호화 : 무선랜을 통해서 이루어지는 모든 통신은 비밀성을 위해서 암호화되어야 한다.
- 관리 : 무선랜을 사용하는 사용자 및 AP들은 망 관리자에 의해서 관리 되어야 한다.

802.11b에서의 표준보안 체계

802.11b에서는 보안을 위해서 WEP와 SSID라는 두 가지의 표준을 제공하고 있다.

■ SSID (Service Set ID)

SSID는 유선랜에서의 네트웍 이름과 같은 계념으로 주로 네트웍을 분리하여 사용할 때 사용한다. AP는 자신이 속한 네트웍 세그먼트에 해당하는 SSID로 모든 패킷을 전송하고 같은 SSID를 갖고 있는 무선랜 카드만이 이 데이터를 받아볼 수 있기 때문에 가장 기본적인 사용자 인증 및 식별 기능을 제공한다.

■ WEP(Wired Equivalent Privacy)

WEP은 RC-4 대칭키 알고리즘을 이용한 암호와 알고리즘이다. WEP을 사용할 경우 AP와 사용자 사이의 모든 패킷은 암호화되어 방송되며 AP와 동일한 WEP 키를 사용하지 않는 사용자는 패킷을 복호화 할 수 없으며 AP에서 패킷을 받아주지 않기 때문에 암호화기능과 식별 및 인증 기능을 제공한다.

위에서 살펴본 것과 같이 802.11b 표준은 SSID와 WEP을 통해서 기본적인 사용자 식별 및 인증기능과 암호화 기능을 제공한다. 하지만 SSID의 경우 도청

을 통해서 금방 알아낼 수 있으며 WEP에서 사용하는 RC-4 알고리즘은 매우 약한 알고리즘으로 고성능 노트북으로 45분 만에 암호화된 패킷을 복호화 시킬 수 있다. 하지만 무엇보다 근본적인 문제는 802.11b에서 키 분배를 제공하고 있지 않다는데 있다.

모든 WEP Key는 수동으로 관리되기 때문에 모든 AP와 사용자 디바이스(device)들의 WEP 키는 빠르게 갱신될 수 없으며 이는 모든 무선랜에서 모든 공격이 가능한 근본적인 원인을 제공한다. 또한 WEP은 사용자 기반의 식별 및 인증이 아닌 디바이스에 대한 식별 및 인증을 제공하기 때문에 사용자 디바이스의 분실은 네트워 보안의 문제로 연결된다. 즉, 802.11b 표준은 위에서 설명한 3가지 보안이슈 중 아주 기본적인 식별 및 인증 과 암호화 기능은 제공하지만 관리 기능을 제공하지 않고 있다.

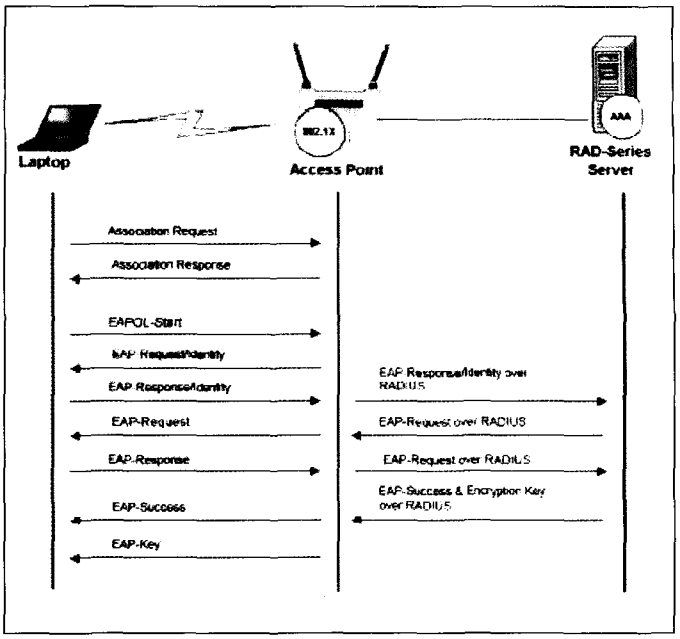


그림 7 802.1x의 동작 절차

802.1x 보안 체계

802.1x는 환경에서 key분배 메커니즘을 제공하는 RADIUS기반의 EAP(Extensible Authentication Protocol) 인증 프로토콜을 제공하는 표준이다. 802.1x는 유선망에서의 사용을 위해서 개발되었으나 802.1x를 지원하는 AP를 사용할 경우 무선랜 환경에서의 적용이 가능하다. 그림 7은 802.1x의 동작을 설명하고 있다.

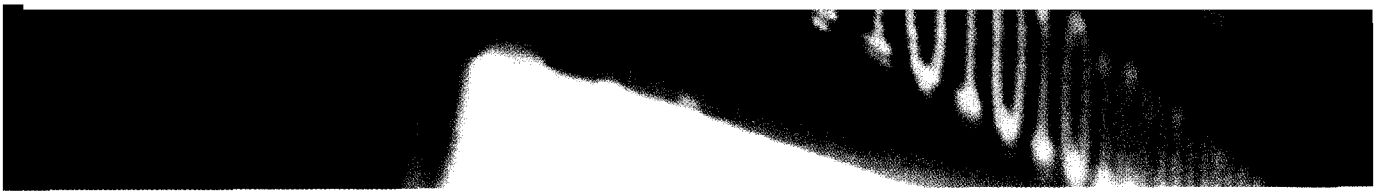
무선랜 client가 AP에 접근할 경우 client는 EAPOL 메시지를 이용하여 인증을 요청하고 AP는 EAP를 이용하여 인증서버와 통신하여 사용자의 인증 및 식별이 이루어진다.

802.1x는 여러가지 형태로 사용될 수 있는데 client의 MAC주소를 이용하여 client 디바이스만을 식별 및 인증할 수 있으며 사용자의 ID/Password를 이용한 사용자 인증을 할 수 있다. 또한 EAP는 인증정보의 보호를 위해서 MD-5, 인증서, 터널링을 이용할 수 있는데 어떠한 방법을 사용하느냐에 따라서 EAP-MD5, EAP-TLS, 그리고 EAP-TTLS로 구분된다.

사용자에 대한 식별 및 인증이 이루어지면 인증서버는 AP와 client 모두에게 WEP key를 전송하여 암호화된 통신이 이루어질 수 있게 한다. 이러한 동적인 WEP key생성과 분배 메커니즘을 이용하여 주기적으로 WEP Key를 변경 함으로써 기존의 802.11b에서의 많은 보안 문제들을 해결할 수 있다. 하지만 802.1x역시 효율적인 client 및 망 관리에 대한 기능을 제공하고 있지 않다.

올바른 무선랜 보안구성

위에서 살펴본 바와 같이 무선랜은 보안에 있어 많은 문제점들을 안고 있으며 이러한 문제들을 표준만으로는 해결하기가 쉽지 않다. 세계 유수 기관들이 제안하는 올바른 무선랜 구축방안을 살펴보면 먼저 무선랜으로부터 유선망을 보호하고 외부로부터 무선랜을 보호하기 위해서 모든 무선랜 client들을 DMZ로 구성하라고 권고하고 있다. 하지만 이러한 구성은 client의 수가 많아질 경우 무선 client들간에 발생하는 트래픽에 의한 broadcast storm이 발생하



여 같은 DMZ에 위치한 서버들의 응답 속도를 느리게 할 우려가 있어 아주 작은 규모의 무선랜에 적합하다.

다른 권고안은 방화벽으로 보호되는 내부망에 무선랜을 설치할 경우, 별도의 방화벽을 설치하고 그 외부에 무선랜을 설치하며 무선랜 구간은 802.1x를 이용한 Dynamic WEP이나 IPSec과 같은 VPN 기술을 이용하여 보호하는 것이다. 이러한 방법 역시 client와 망 관리가 없으면 보안의 허점을 들어내기 때문에 무선랜 관리 소프트웨어를 따로 설치하거나 간단한 방화벽/VPN 기능과 망 관리 기능이 통합된 전용 기기를 방화벽의 위치에 두어 무선랜 보안을 구성하는 것이 권장되고 있다.

결 론

본 논문에서는 네트웍 보안에서 중요한 기술인 IPSEC 보안을 중심으로 최근에 많이 논의되고 있는 VoIP와 무선랜의 보안을 살펴보았다. IPSEC 기술은 VPN(Virtual Private Network)이라는 주요한 응용 기술을 제공할 뿐만 아니라 다른 네트웍 기술에도 보안 기술로 많이 사용된다. VoIP 기술은 수십년간 발전해 온 전화 기술을 인터넷 기술을 이용하여 대체하는 기술로써 차세대 네트웍의 주요한 진화 방향이다. VoIP 보안 기술은 관련된 표준에서 제공하는, 호처리 과정에 보안 기능을 추가하는 방법과 IPSEC과 같은 기존 보안 방법을 사용하는 방법이 있다. 무선랜 보안은 단말부터 AP(Access Point) 까지의 무선 구간이 유선 구간에 비해 상대적으로 도청이 쉽고, 802.11b의 WEP의 보안상 취약점 때문에 끊임없이 문제가 지적되어 왔다. 현재는 802.1x의 dynamic WEP과 IPSEC을 사용하는 방법이 가장 좋은 방법으로 보인다. 아직도 보안 기술은 특정 기술로 정립이 되지 않고 있으며 앞으로도 상당 기간 동안 여러 가지 표준이 상호 경합하며 발전해 나아가리라 본다.

[참고 문헌]

[1] S. Kent and R. Atkinson, "Security Architecture for Internet Protocol," IETF RFC 2401, Nov. 1998.

[2] S. Kent and R. Atkinson, "IP Authentication Header," IETF RFC 2402, Nov. 1998.

[3] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," IETF RFC 2406, Nov. 1998.

[4] D. Harkins and D. Carrel, " The Internet Key Exchange (IKE)," IETF RFC 2409, Nov. 1998.

[5] Vineet Kumar, Markku Korpi and Senthil Sengodan," IP Telephony with H.323, WILEY Computer Publishing

[6] 임채훈,"VoIP 시스템에서의 보안기술", 정보처리 제8권 제2호 2001. 3

[7] ITU-T, ITU-T Recommendation H.235 (02/98), Security and encryption for H-Series(H.323 and other H.245-based) multimedia terminals, 1998.

[8] http://www.cs.columbia.edu/sip/

[9] "IEEE 802.11 Wireless Local Area Networks", Brian P. Crow, Indra Widjaja, Jeong Geun Kim, Prescott T. Sakai, P116~P126 IEEE communications magazine, September 1997

[10] "Intercepting Mobile Communications : The Insecurity of 802.11", Borisov, Goldberg, and Wagner, The proceesings of Seventh Annual International Conference on Mobile Computing and Networking, July, 2001

[11] "Weaknesses in the Key Scheduling Algorithm of RC4", Fluher, Mantin, and Shamir Eighth Annual Workshop on Selected Areas in Cryptography Aug 2001

[12] "An Initial Security Analysis of the IEEE 802.1x Standard", Mishra and Arbaugh, Univ. of Maryland College Park Technical report. UMIACS-TR-2002-10 Feb 2002

13. "Mobile and Wireless Security : Worst and Best Practices" Gart Report 2002