IEEE 802.1x 인증과 동적 WEP 키를 사용하는 무선랜 보안 시스템 개발

오경희[0] 강유성 정병호
한국전자통신연구원 무선인터넷보안연구팀
{khoh[0], youskang, cbh}@etri.re.kr

Secure Wireless LAN with IEEE 802.1x Authentication and Dynamic WEP Key

Kyunghee Oh[0] Yousung Kang Byungho Chung
Wireless Internet Security Research Team, ETRI

요 약

IEEE 802.11 규격에 따른 무선랜은 사설망에서 사용됨은 물론, 공중망 사업자들에 의한 핫스팟 서비스까지 제공되면서 널리 사용되고 있어, 이에 대한 보안의 중요성이 더욱 커져가고 있다. IEEE 802.1x는 랜 접속 서비스를 받고자 하는 시스템이 인증을 거쳐 망을 사용할 수 있도록 하며, IEEE 802.11i 키교환 규격은 무선랜에서 암호화를 위하여 사용되는 WEP 키를 교환할 수 있게 한다. 이를 이용하여 타인이 무단으로 망을 사용하거나 도청하는 것을 막는다. 이러한 시스템의 개발을 위하여 기존의 리눅스 용 access point 디바이스 드라이버에 802.1x 가상 포트를 추가하고, 키 교환을 통한 동적 WEP 적용 기술을 설계, 개발하였다.

1. 서 론

그 동안 IEEE 802.11[1] 규격에 따른 무선랜은 기업 등의 사설망에서 뿐만 아니라, 공중망 사업자들이 핫스팟을 통한 공중 무선랜 서비스를 제공하며, 또한 일반 가정과 소규모 사업장에서도 무선랜을 사용하는 수요가 더욱 늘어나고 있다. 무선랜의 사용자들이 늘어나는 만큼, 이에 대한 보안도 더욱 중요하게 되었다. 특히 유선 통신과 달리 무선 통신의 경우, 통신 내용이 공중으로 방송되어 도청 및 침입자에 의한 공격이 더욱 용이하므로 보안의 중요성은 유선망에 비하여 더 크다.

그런데, 기존의 IEEE 802.11 규격의 WEP에 의한 보안에 결함이 있음이 알려져 있다[2]. 이러한 문제점은 IEEE 802.1x[3] 접속 인증과 현재 표준화가 진행중인 IEEE 802.1aa[4]및 IEEE 802.11i[5]의 암호화 키 교환 기술을 채용함으로써, 기존의 무선랜에서의 보안 결함을 상당 부분 해결할 수 있다.

본 논문은 리눅스용 무선랜 access point 디바이스 드라이버에 위에서 언급된 보안 기술을 채용하여, 접속자를 인증하고 각 접속자 별로 동적으로 생성된 WEP 키를 적용한 무선랜 보안 시스템에 대하여 논의한다.

2. 관련 규격

2.1 IEEE 802.1x

802.1X에는 역할에 따라 세 가지 시스템이 있다. 서비스를 제공하고자 하는 포트에 대하여 인증을 수행하는 authenticator, authenticator에서 제공하는 포트의 인증을 받고자 하는 supplicant, supplicant의 신분을 인증하여 authenticator가 서비스를 제공할 수 있도록 알려주는 authentication server로 구성된다.

그림 1은 802.1x에서 각 시스템의 역할을 보여준다. 무선랜 access point는 authenticator의 역할을 수행하게 된다.

authenticator의 비제어 포트는 EAPOL 메시지를 인증 과정 없이 authenticator PAE로 전달하며, supplicant와 authentication server는 이 경로를 통하여 서로 인증하게 된다. 서로 인증이 이루어진 후, authenticator는 제어 포트를 비인증 상태에서 인증 상태로 전환하여 access point로서 유선망에 대한 접속 서비스를 제공하게 된다.

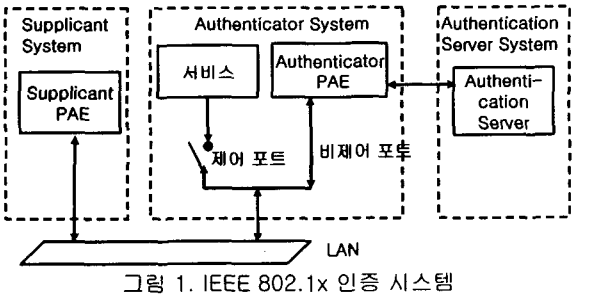

그림 1. IEEE 802.1x 인증 시스템

authenticator에서는 EAP-Packet을 직접 처리하지 않고, supplicant와 authentication server 사이를 중계하

는 역할만 수행한다. supplicant와 authentication server는 authenticator와는 무관하게 EAP-MD5, EAP-TLS 등의 다양한 방식을 통하여 인증할 수 있다.

EAPOL(Extended Authentication Protocol over LAN)은 supplicant PAE와 authenticator PAE 사이의 LAN 환경에서 EAP 패킷을 전송하기 위한 프레임으로, 무선구간에서 인증에 필요한 메시지를 주고 받는데 사용된다. EAPOL 프레임은 전송하는 메시지 유형에 따라, EAP[6] 메시지를 전송하는 EAP-Packet, 인증을 위하여 EAPOL 메시지를 주고 받는 세션의 시작과 끝을 알리는 EAPOL-Start, EAP-Logoff 등의 packet type이 있다.

IEEE 802.1aa는 IEEE 802.1x의 수정안으로 현재 draft 상태이며, IEEE 802.11i에서의 키교환을 위한 키 유형을 규정하고 있다.

2.2 IEEE 802.11i를 동적 WEP 키에 적용

IEEE 802.11i는 IEEE 802.11에서 보안관련 분야를 강화한 수정안으로 현재 draft 상태이다.

802.11i에서는 기존의 WEP을 대체하기 위하여 AES 알고리즘을 사용하는 CCMP와 기존의 WEP을 사용하되 보안 강도를 높인 TKIP 알고리즘을 규정하고 있다. 그리고 supplicant와 access point가 공유하는 키로부터 키 교환 알고리즘에 따라 실제 데이터를 암호화하기 위한 임시키를 생성할 수 있다.

그림 2는 802.1x에 따른 인증과 802.11i에 따른 키교환 과정을 보여준다. supplicant와 access point 사이의 802.11 association이 이루어지면, 이에 해당하는 가상 포트가 access point에 생성된다. 이 가상 포트를 통하여 supplicant는 EAP-TLS 프로토콜에 따라 인증서버인 Radius 서버로부터 인증을 받게 된다. 인증과정을 성공적으로 마치게 되면, 인증과정에서 access point와 supplicant는 공유키를 갖게 되며, 이 키로부터 802.11i에서 규정한 키교환 알고리즘에 따라 임시키를 생성한다.

이러한 과정으로 생성된 임시키를 동적 WEP 키에 적용한 후, supplicant는 access point를 통하여 유선망과 안전한 통신을 할 수 있다.

동적 WEP 키를 적용함으로써, supplicant가 접속할 때마다 매번 새로운 WEP 키가 적용되며, 각 사용자마다 다른 WEP키를 가지게 된다. 따라서 기존의 access point들이 사용자 간에 공유되고 정적인 WEP 키를 사용함으로써 나타나는 보안 취약성을 극복할 수 있다.

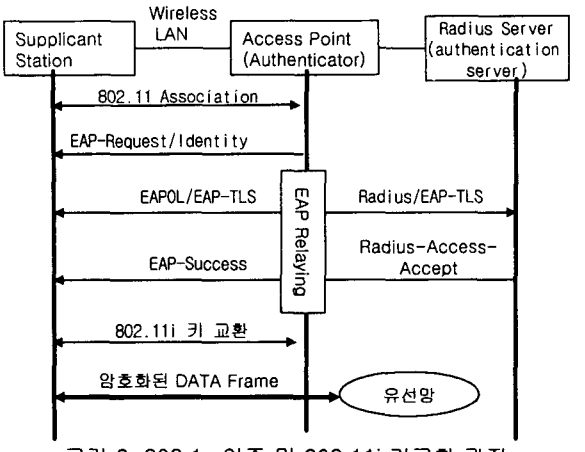

그림 2. 802.1x 인증 및 802.11i 키교환 과정

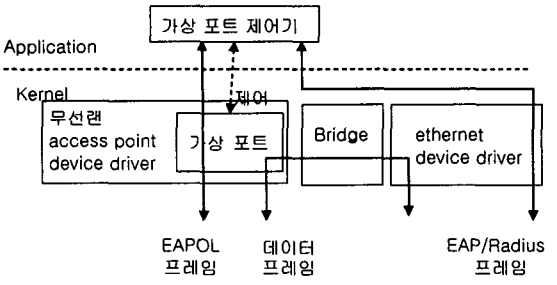

그림 3. access point 기능 블록

그리고 응용에는 가상 포트를 제어하고 EAP 패킷을 EAPOL 프레임과 Radius 프레임을 서로 변환하여 전달하는 가상 포트 제어기가 있다. 가상 포트 제어기에는 802.1x 인증과 802.11i 키 교환을 수행하는 state machine들이 구현되어 있다. 가상포트제어기는 인증여부에 따라 가상포트의 데이터 전송 허용여부를 결정하며 또한 동적 WEP 키를 설정한다.

3. Access Point 설계 및 구현

3.1 설계

그림 3은 리눅스를 운영체제로하는 802.1x 인증 및 802.11i 키 교환 기능이 구현된 access point 시스템의 기능 블록들 사이의 관계를 보여준다. 리눅스 커널에 무선랜 및 이더넷 디바이스 드라이버 모듈과, 이 둘을 연결하여 주는 브릿지 모듈이 있다. 무선랜 디바이스 드라이버에는 데이터 프레임의 전달을 제어하는 가상 포트가 구현되어 있다.

3.2 구현

운영체제로 리눅스 커널 2.4를 사용하는 노트북 컴퓨터를 access point 개발환경으로 사용하였으며, Prism2 계열의 칩을 사용한 pcmcia 무선랜 카드를 사용하였다.

1) HostAP 디바이스 드라이버

HostAP 디바이스 드라이버는 Prism2 계열의 MAC 칩을 사용하는 무선랜 장비에 대한 리눅스 용 access point 디바이스 드라이버이다[7]. 802.1x 및 802.11i 기능을 위하여, 이 디바이스 드라이버에 가상 포트를 추가하고 가상 포트 제어기의 명령을 수행하는 ioctl 명령을 추가하였다. 또한 무선랜에서 발생한 이벤트들을 가상 포트 제어기로 전달하는 기능도 추가되었다.

2) 가상 포트 제어기

가상 포트 제어기는 802.1x 및 802.11i에 정의된 state machine들과 가상 포트를 제어하는 thread, EAPOL thread, Radius thread 등, 다중 thread로 구현되어, 이벤트 기반으로 작동하도록 구현되었다.

802.11 association이 이루어지면, 가상 포트를 생성하고 초기화 한다. EAP 메시지를 중계하고, 인증 여부에 따라 디바이스 드라이버의 가상 포트를 제어하고 동적 WEP을 설정한다.

3) Windows 접속 소프트웨어

Windows XP 운영체제에 내장되어 있는 무선랜 인증 기능에서는 802.1x 인증만이 지원된다. 따라서 802.1x와 802.11i 키교환 및 동적 WEP을 지원하기 위하여 Windows NT/XP 운영체제에서 작동하는 접속소프트웨어를 개발하였다. 개발된 소프트웨어는 Radius 서버로부터 EAP-TLS로 인증을 받기 위하여 인증서를 관리하며, NDIS API를 이용하여 무선랜 장비에 동적 WEP 기능을 구현하였다.

3.3 시험

그림 4는 802.1X 시스템의 시험망이다. 인증서버로는 FreeRADIUS[8]가 사용되었다.

각 supplicant는 개발된 접속소프트웨어를 이용하여 성공적으로 인증 및 키 교환을 수행한 후, 개발된 access point를 통하여 이더넷 망으로 각각 다른 WEP 키로 암호화된 데이터 프레임을 송수신함으로써 안전한 접속 서비스가 제공됨을 확인할 수 있었다.

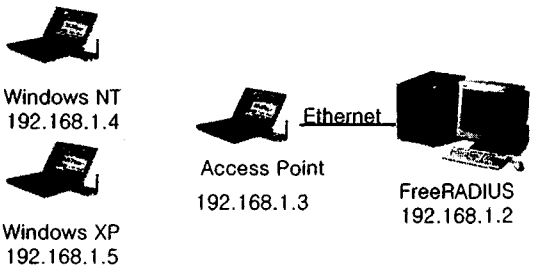

그림 4. 시험망

4. 결론 및 향후 과제

802.1x를 구현한 access point를 사용하여 허가 받지 않은 무단 사용자를 막을 수 있다. 또한 등록된 사용자에 한하여 접속할 수 있게 함으로써 공중 인터넷 접속 서비스도 가능하게 한다. 그리고, 802.11i 키교환을 통한 동적 WEP 기능은 임시키를 통한 암호화와 사용자마다 다른 키를 사용하게 함으로써 기존의 무선랜의 보안 취약점을 상당부분 해결할 수 있다.

개발된 access point는 리눅스 환경을 사용하여 제작비를 줄일 수 있으며, embedded 리눅스 형태로 만들어 질 수 있다.

IEEE 802.11i에서 진행중인 무선랜 보안 규격은 일시적으로 TKIP을 사용하며, 궁극적으로는 AES 알고리즘을 사용하는 CCMP를 표준으로 하고 있다. 그러나 TKIP이 구현되기 위해서는 device driver 뿐만 아니라 무선랜 카드의 firmware도 갱신되어야 한다. 그리고, CCMP가 구현된 무선랜 카드는 아직 출시되지 않고 있다.

동적 WEP이 TKIP이나 CCMP에 비하면 보안 강도가 상대적으로 약하지만, 사용자들이 무선랜카드의 device driver 및 firmware의 갱신 없이 접속소프트웨어만 설치하여 사용함으로써, 기존의 WEP이 가진 취약점들은 극복할 수 있게 한다. 따라서 새로운 규격의 무선랜 제품들이 보급되기 이전에도 무선랜 환경의 보안을 강화할 수 있다.

그러나 이러한 방법은 TKIP 및 CCMP를 적용한 제품이 널리 보급되기 이전에 일시적으로 사용되는 것이 바람직하며, 802.11i 규격이 승인된 이후에는 그에 따르는 제품을 개발하여 사용하는 것이 바람직할 것이다.

참고문헌

[1] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," IEEE Std 802.11-1997, June 1997.

[2] W. A. Arbaugh, et al. "802.11 Security Vulnerabilities," http://www.cs.umd.edu/~waa/wireless.html.

[3] "Port-Based Network Access Control," IEEE Std 802.1X - 2001, June 2001.

[4] "Port-Based Network Access Control - Amendment1," IEEE Draft 802.1aa/D4, November 2001.

[5] "Wireless Medium Access Contro(MAC) and Physical Layer(PHY) Specifications: Specification for Enhanced Security, " IEEE Draft 802.11i/D3.0, November 2002.

[6] 1L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)," RFC 2284, March 1998.

[7] "Host AP driver for Intersil Prism2/2.5/3," http://hostap.epitest.fi/.

[8] "FreeRADIUS," http://www.freeradius.org/.