IEEE 802.1X에 따른 무선랜 Access Point 접속 인증 시스템 개발

오경희, 양대헌, 강유성, 함영환, 정병호

한국전자통신연구원, 무선인터넷보안연구팀

Access Control of Wireless LAN Access Point Based on IEEE 802.1X

Kyung-hee Oh, Dae-hun Nyang, You-sung Kang, Young-hwan Ham, Byung-ho Chung

Wireless Internet Security Research Team, ETRI

요 약

IEEE 802.11 규격에 따른 무선랜은 사설망에서 사용됨은 물론, 공중망 사업자들에 의한 핫스팟 서비스까지 제공되면서 수요가 더욱 늘어나고 있다. 사용자가 늘어남에 따라, 이에 대한 보안의 중요성 또한 늘어났다. IEEE 802.1X는 랜 접속 서비스를 받고자 하는 시스템이 인증을 거쳐 랜을 사용할 수 있도록 함으로써, 허가 받지 않은 사용자가 무단으로 사용하거나 도청하는 것을 어렵게 한다. 기존의 Linux 용 access point 디바이스 드라이버에 802.1X 가상 포트를 추가하고, 이를 제어하는 가상 포트 제어기를 통하여, 사용자 인증 기능이 추가된 access point를 설계, 개발하였다. 개발된 시스템은 embedded Linux 형태의 access point로 사용되어 질 수 있다.

I. 서론

그 동안 IEEE 802.11[1] 규격에 따른 무선랜은 기업 등의 사설망에서 주로 사용되었다. 그런데 최근 공중망 사업자들이 핫스팟을 통한 공중 무선랜 서비스를 제공하면서 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 인증 방식인 공유키 인증 방식에 결함이 있음이 알려졌다[2]. 이러한 문제점은 IEEE 802 계열 규격에 따른 LAN에서의 네트워 접속 인증을 위하여 만들어진 IEEE 802.1X[3] 규격을 채용함으로써, 무선랜 인증 방식의 결함을 해결할 수 있다.

본 논문은 리눅스용 무선랜 access point 디바이스 드라이버에 IEEE 802.1X 규격에 따른 인증 과정을 구현한 시스템에 대하여 논의한다.

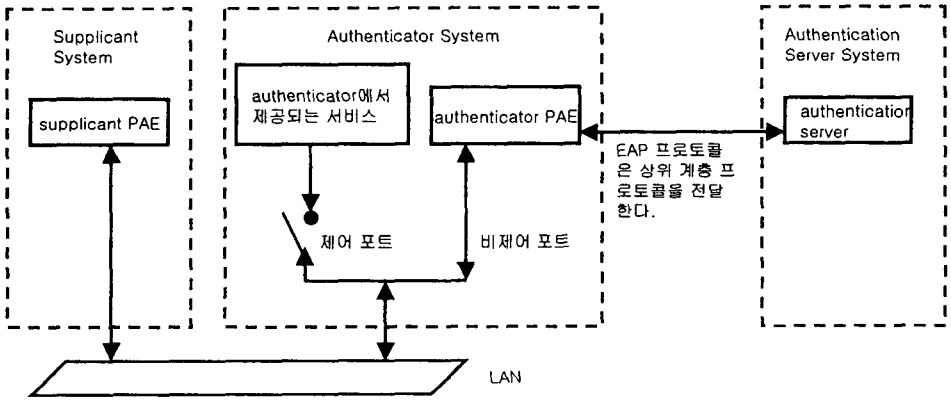

그림 1: IEEE 802.1X 인증 시스템

II. IEEE 802.1X

1. 802.1X에서 각 시스템의 역할

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.

2. EAPOL

EAPOL(Extended Authentication Protocol over LAN)은 supplicant PAE와 authenticator PAE 사이의 LAN 환경에서 EAP 패킷을 전송하기 위한 포맷이다. 무선랜의 경우 EAPOL 프레임의 MAC 계층의 형태는 표 1과 같은 형태를 가진다. {} 안의 값은 EAPOL 프레임에서 항상 같은 값을 유지하는 고정된 값을 16진값으로 나타낸 것이다.

표 1: EAPOL 프레임 포맷

크기(Octet 수)

무선랜 MAC Header	
SNAP-encoded Ethernet Type {AA:AA:03:00:00:00:88:8E}	8
Protocol Version {01}	1
Packet Type {00~04}	1
Packet Body Length	2
Packet Body	가변
FCS	

전송하는 메시지 유형에 따라, EAP[4] 메시지를 전송하는 EAP-Packet, 인증을 위하여 EAPOL 메시지를 주고 받는 세션의 시작과 끝을 알리는 EAPOL-Start, EAP-Logoff 등의 packet type이 있다.

authenticator에서는 EAP-Packet을 직접 처리하지 않고, supplicant와 authentication server 사이를 중계하는 역할만 수행한다. supplicant와 authentication server는 authenticator와는 무관하게 EAP-MD5, EAP-TLS 등의 다양한 방식을 통하여 인증할 수 있다.

3. 인증과정

1) 프로토콜 스택

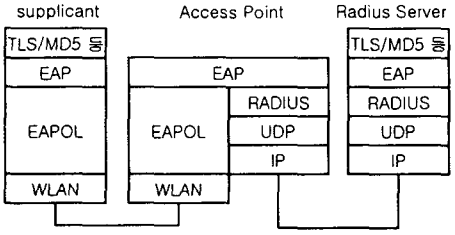

그림 2: 802.1X 프로토콜 스택

그림 2는 802.1X를 사용하는 supplicant와 access point, Radius 서버의 프로토콜 스택을 보여준다. access point는 무선랜 구간에서 EAPOL 프레임으로 전송된 EAP 메시지를 Radius 프레임으로 변환하여 전달하는 역할을 수행한다.

2) 인증 과정

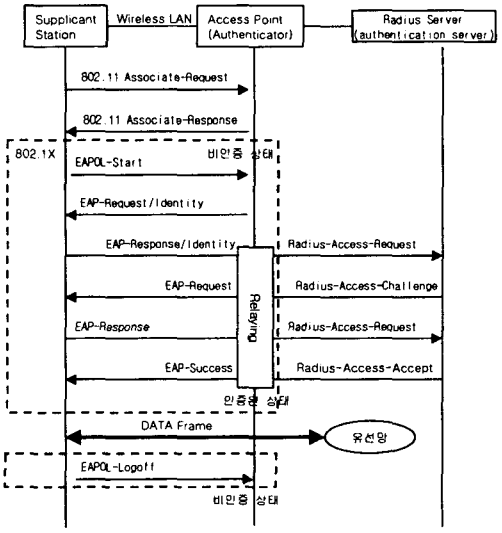

그림 3: 802.1X 인증 과정

그림 3은 802.1X에 따른 인증 과정을 보여준다. 점선으로 둘러 쌓인 부분이 EAPOL 메시지들에 해당한다. supplicant와 access point 사이의 802.11 association이 이루어지면, 이에 해당하는 가상 포트가 access point에 생성된다. 이 가상 포트를 통하여 supplicant는 인증과정을 거치게 된다. 인증과정을 성공적으로 마치게 되면, access point는 가상 포트를 인증된 상태로 바꾸어 supplicant가 일반 data 프레임을 유선망과 주고 받을 수 있게 한다. EAPOL-Logoff 메시지는 가상 포트를 비인증 상태로 바꾸어 access point의 접속 서비스를 종료하도록 한다.

III. Access Point 설계 및 구현

1. 설계

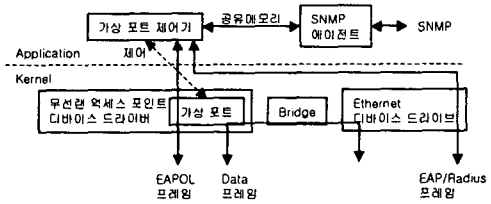

그림 4: 802.1X Access Point 기능 블록

그림 4는 802.1X 인증 기능이 구현된 access point 시스템의 기능 블록들 사이의 관계를 보여준다. kernel에 무선랜과 이더넷 디바이스 드라이버 모듈과, 이 둘을 연결하여 주는 bridge 모듈이 있다. 무선랜 디바이스 드라이버에는 data 프레임의 전달을 제어하는 가상 포트가 구현되어 있다.

그리고 응용에는 가상 포트를 제어하고 EAP 패킷을 EAPOL 프레임과 Radius 프레임을 서로 변환하여 전달하는 가상 포트 제어기와, access point를 원격 제어할 수 있도록 SNMP 에이전트가 있다. 가상 포트 제어기와 SNMP 에이전트는 공유메모리를 통하여 값을 설정할 수 있다.

2. 구현

운영체제로 Linux kernel 2.4를 사용하는 노트북 컴퓨터를 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 Linux용 access point 디바이스 드라이버이다[5]. 802.1X 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 802.1X에 정의된 state machine과 가상 포트를 제어하는 thread, EAPOL thread, Radius thread, SNMP 메타 에이전트 thread 등, 다중 thread로 구현되었다.

802.11 association이 이루어지면, 가상 포트를 생성하고 초기화 한다. EAP 메시지를 중계하고, 인증 여부에 따라 디바이스 드라이버의 가상 포트를 제어한다.

3) SNMP Agent

원격 제어를 위하여 SNMP 프로토콜에 따라 가상 포트 제어기의 802.1X MIB 변수들을 읽거나 변경할 수 있다. 가상 포트 제어기의 SNMP 메타 에이전트와 공유메모리를 통하여 통신한다.

3. 시험

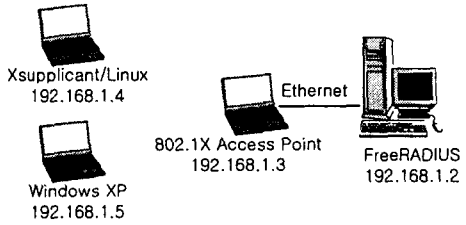

그림 5: 802.1X 시험망

그림 5는 802.1X 시스템의 시험망이다.

supplicant로 Linux 환경에서 Xsupplicant[6]와 Windows XP를 사용하였다. Xsupplicant는 TLS에 의한 인증 방법을 사용한다. Windows XP의 경우 MD5 및 TLS에 의한 인증에 대하여 시험되었다.

authentication server로는 FreeRADIUS[7]가 사용되었다.

각 인증 시험을 통하여 supplicant의 인증 여부에 따라 개발된 802.1X access point에서 이더넷 망으로의 접속 서비스가 제공됨을 확인할 수 있었다.

IV. 결론 및 향후 과제

802.1X를 구현한 access point를 사용하여 허가받지 않은 무단 사용자를 막을 수 있다. 또한 등록된 사용자에 한하여 접속할 수 있게 함으로써 공중 인터넷 접속 서비스도 가능하게 한다.

개발된 access point는 Linux 환경을 사용하여 제작비를 줄일 수 있으며, embedded Linux 형태로 만들어 질 수 있다. 또한 SNMP를 통한 제어가 가능하여, 관리자는 여러 access point를 원격 관리할 수 있다.

현재 구현된 access point는 통신 내용을 보호하기 위하여 data 프레임을 암호화하는데, 기존의 802.11 WEP을 사용하도록 되어 있다. 그러나, WEP에서 사용되는 RC4 알고리즘이 보안에 취약한 것으로 알려졌다[2]. 이러한 문제점을 해결하기 위하여 IEEE 802.11 Working Group/Task Group I에서 WEP을 대치하기 위한 TKIP, WRAP 등의 알고리즘을 적용한 규격을 제정중이다[8]. 802.1X 인증과 함께, 802.11I를 사용하여 무선랜 구간에서의 data를 안전하게 암호화하여 전

송함으로써, 기존의 802.11 규격에서 밝혀진 보안 취약사항들을 해결할 수 있다. 이러한 기능을 access point에 구현하기 위해서, device driver에 TKIP 및 WRAP 암호화 알고리즘을 구현하고, supplicant와 authenticator가 암화화 키를 교환할 수 있는 기능이 추가되어야 한다.

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

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

[6] "Open Source Implementation of IEEE 802.1X - Opne1X," http://open1x.sourceforge.net/.

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

[8] "Specification for Enhanced Security," *IEEE Std* 802.11i/D2.3, September 2002.