소프트웨어 구현을 통한 WPA 지원 무선랜 액세스포인트 개발

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

Software Implementation of WPA Wireless LAN Access Point

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

요 약

IEEE 802.11 표준에 포함되어 있는 WEP 방식의 무선랜 보안이 취약한 것으로 알려진 후, WEP을 대치할 새로운 표준이 802.11i 워킹그룹에 의하여 작성되고 있다. Wi-Fi는 중간단계로서 802.11i의 일부만을 구현하는 WPA 규격을 만들었다. 이 규격은 기존의 하드웨어를 그대로 사용하면서 소프트웨어와 펌웨어 갱신만으로 기존의 무선랜 취약점을 제거할 수 있게 한다. WPA 규격을 준수하는 무선랜 액세스포인트의 개발을 위하여 기존의 액세스포인트 디바이스 드라이버를 WPA를 지원하도록 수정하였으며, 사용자 인증 및 키 교환을 수행하는 소프트웨어를 설계 및 개발하였다.

1. 서 론

IEEE 802.11 표준[1]을 따르는 무선랜은 기업의 사설망, 핫스팟과 같은 공중망, 그리고 일반 가정과 소규모 사업장에서도 사용하는 등 사용자가 계속 늘어나고 있다. 그런데, 기존의 무선랜 제품이 사용하여온 WEP 방식에 의한 보안에 취약점이 있음이 알려졌고[2], 이를 해결하는 새로운 보안 표준이 IEEE 802.11i 워킹그룹에 의하여 작성되고 있다[3].

그러나, 표준의 승인이 지연되면서, 무선랜 관련 업체들의 연합체인 Wi-Fi에서 IEEE 802.11i 규격이 완성되기 이전의 중간단계로서 WPA 규격[4]을 발표하여 실제 무선랜 제품 개발에 사용하고 있다. WPA 규격에서는 기존의 무선랜 하드웨어에서 소프트웨어 및 펌웨어만을 수정함으로써 IEEE 802.11i 규격의 일부를 준수할 수 있게 한다.

본 논문은 리눅스 환경에 구현된 기존의 무선랜 액세스포인트 시스템을 기반으로, WPA 규격을 준수하도록 구현한 시스템에 대하여 논의한다. 기존의 액세스포인트 디바이스 드라이버를 수정하여 TKIP 암호 알고리즘을 구현하고, 사용자 인증, 키 교환 기능을 수행하는 소프트웨어를 개발하였다.

2. WPA 규격

WPA 규격은 IEEE 802.11i draft 3.0에서 하드웨어 수정 없이 구현하기 힘든 CCMP 암호 알고리즘을 제외한 나머지 부분을 기반으로 실제 구현과정에서 발견된 몇 가지 오류를 수정한 내용으로 구성된다.

2.1 인증 및 키 교환

사용자 인증 방법은 IEEE 802.1x[5]을 따르는 방식과 PSK 방식이 있다.

IEEE 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. authenticator는 supplicant와 주고받는 EAPOL 프레임으로 supplicant와 authentication server 사이의 EAP 메시지를 중계하여 인증과정을 수행한다. 그리고 인증에 성공한 supplicant들에 대해서만 망으로의 데이터 프레임 전송을 허용한다. WPA에서는 액세스포인트가 authenticator의 역할을 수행하며, 인증이 완료된 후 액세스포인트와 스테이션 사이에 공유키가 생성된다.

기업망이나 공중망과는 달리, 소호 및 홈네트워크에서는 굳이 별도의 인증 서버를 둘 필요가 없다. 이러한 환경에서는 액세스포인터와 스테이션에 미리 공유키를 설정해 두는 PSK 방식을 사용할 수 있다.

액세스포인트와 스테이션은 공유키를 사용해 실제 데이터 프레임의 암호화에 사용되는 임시키를 생성하기 위한 키교환 과정을 수행하며, 각각의 스테이션이 할당되는 pairwise 키와 여러 스테이션이 공유하는 group 키를 생성한다. 이때의 키교환 과정에서 IEEE 802.1x에서 지정한 것과는 다른 IEEE 802.11i에서 지정한 키 프레임 형과 키 교환 절차에 따른다.

2.2 TKIP

암호알고리즘으로는 TKIP과 기존의 WEP을 사용할 수 있다. IEEE 802.11i 표준에서 필수사항인 CCMP 알고리즘의 구현이 WPA 규격에서는 선택사항이다.

CCMP가 AES 알고리즘을 사용하는 것과는 달리, TKIP은 WEP을 확장하는 방법을 사용함으로써, 기존의 하드웨어 교체가 필요 없이 구현할 수 있도록 설계되었다. TKIP에서는 WEP을 이용한 암호화 이전에 별도의 키 생성 과정을 거치게 하여, WEP에 적용되는 키가 각 데이터 프레임마다 변경되도록 하였다. 그리고, 메시지 인증 코드인 MIC를 프레임에 포함시켰다. 이러한 방법으로 알려진 WEP 알고리즘의 취약점을 해결하였다. 그림 1은 TKIP 알고리즘의 암복호화 과정을 보여준다.

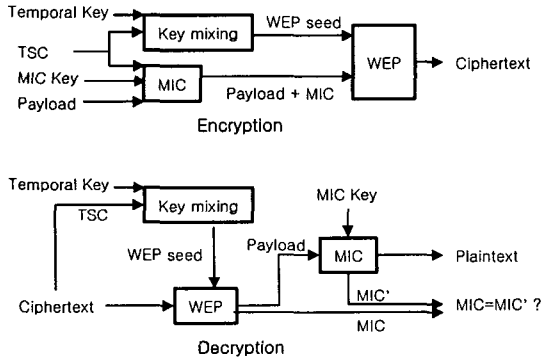

그림 1. TKIP 암복호화 과정

키 교환과정에서 액세스포인트와 스테이션에 동일한 temporal key와 MIC key가 생성되며, TSC는 각 데이터 프레임마다 1씩 증가하는 카운터이다. 프레임을 송신할 경우, temporal key와 TSC를 이용하여 데이터 프레임을 전송할 때마다 다른 WEP seed를 만들어, 메시지 인증코드인 MIC 코드와 함께 WEP으로 암호화 한다. 프레임을 수신한 경우, 암호화된 데이터 프레임의 확장 IV 필드에서 TSC 값을 읽어와 temporal key와 함께 WEP seed를 만들어 복호화한다. 그리고 자체적으로 계산한 MIC 값과 수신 프레임에 포함된 MIC 값을 비교하여 메시지의 무결성을 검증한다.

2.2 IEEE 802.11i와 다른 점

아직 완성된 표준이 아닌 IEEE 802.11i draft 3.0을 실제 제품으로 구현하는 것에는 문제점들이 있어, WPA 규격에서는 TKIP 방식을 사용하는 것 이외에 IEEE 802.11i 내용 중 일부를 좀더 수정하였다. 그 중 중요한 몇 가지는 다음과 같다.

- 향후 표준화가 완성된 후에 사용될 RSN Information Element와 구분하기 위하여, 별도의 WPA Information Element를 management 프레임에서 사용한다.
- 기존의 WEP을 사용하는 스테이션을 함께 사용할 수 있는 mixed-mode를 구현할 수 있다.

이 외에도 draft 내의 오류로 보이는 사항들이 수정되었다.

3. 액세스포인트의 설계 및 구현

3.1 설계

소프트웨어로 구현되는 WPA 지원 무선랜 액세스포인트는 디바이스 드라이버와 이를 제어하는 응용소프트웨어로 구성된다. 그림 2는 기능 블록들 사이의 관계를 보여준다.

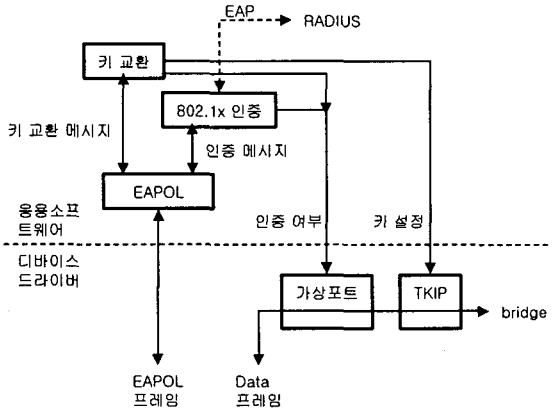

그림 2. 액세스포인트 기능 블록

인증 받지 않은 스테이션의 데이터 프레임들은 가상포트에서 전송되지 못한다. IEEE 802.1x 인증과정과 키 교환 과정을 거친 후에 가상포트를 통하여 데이터 프레임을 전송할 수 있다. IEEE 802.1x 인증 모듈은 RADIUS 서버와 스테이션 사이의 EAP 메시지 중계 기능을 수행한다. 디바이스 드라이버의 TKIP 암복호화 모듈은 스테이션들과의 키 교환과정에서 생성된 각각의 pairwise 키를 보관하고 있어, 송수신 시 이를 이용하여 데이터 프레임의 암복호화를 수행한다. 브로드캐스트 또는 멀티캐스트 되는 프레임들은 group 키를 이용하여 암호화한다.

3.2 구현

운영체제로 리눅스 커널 2.4를 사용하는 노트북 컴퓨터를 개발환경으로 사용하였으며, Prism2 계열의 칩을 사용하고 펌웨어 갱신으로 WPA 기능이 지원되는 스테이션용 PCMCIA 무선랜 카드를 사용하였다. 갱신된 펌웨어는 WPA information element를 management 프레임에 추가할 수 있는 기능을 제공한다.

WPA 규격의 필수 요구사항을 준수하였으며, TKIP과 WEP 알고리즘을 동시에 사용할 수 있는 mixed-mode를 지원한다.

1) HostAP 디바이스 드라이버 수정

HostAP 디바이스 드라이버는 Prism2 계열의 MAC 칩을 사용하는 무선랜 장비에 대한 소스코드가 공개되어 있는 리눅스용 액세스포인트 디바이스 드라이버이다[6].

이 소스코드를 기반으로 가상포트와 TKIP 암복호화 기능을 추가하였다. 또한 응용 소프트웨어가 디바이스

드라이버에 추가된 기능을 제어할 수 있도록 별도의 ioctl 명령을 추가하였다. 그리고 MIC 인증 실패, association 과정에서 처리되어야 할 WPA information element와 같이, 무선랜에서 발생한 이벤트들을 응용 소프트웨어로 전달하는 기능도 추가되었다.

2) 응용 소프트웨어

인증 및 키교환 기능을 수행하는 응용 소프트웨어는 규격에 정의된 state machine들과 가상 포트를 제어하는 thread, EAPOL thread, Radius thread 등, 다중 thread로 구현되어, 이벤트 기반으로 작동하도록 구현되었다.

무선랜 association이 이루어지면, 가상 포트를 생성하고 초기화한다. EAP 메시지를 중계하고, 인증 여부에 따라 디바이스 드라이버의 가상 포트를 제어하고, 키 교환을 통하여 TKIP 또는 WEP에서 사용될 키를 설정한다.

3.3 시험

그림 3는 WPA 액세스포인트 기능을 시험하기 위한 망이다. 스테이션으로는 WPA 인증을 수행할 수 있게 Xsupplicant[7]를 수정한 리눅스 시스템과, Symbol Spectrum 24 카드를 장착한 Windows XP 시스템을 사용하였다. 인증서버로는 FreeRADIUS[8]가 사용되었다. PSK 인증 방식을 사용하는 경우에는, 인증서버 없이 망을 구성한다.

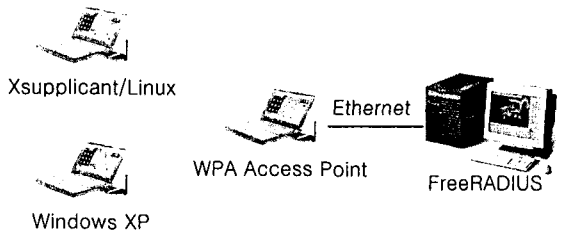

그림 3. 시험망

Xsupplicant/Linux 스테이션을 구현하기 위하여 WPA 액세스포인트에 사용된 디바이스 드라이버를 일부 수정하고 동일한 무선랜 카드를 사용하여 WPA가 지원되는 스테이션으로 작동하도록 하였다. 운영체제 패치와 디바이스 드라이버 갱신으로 Windows XP가 WPA 스테이션으로 구성될 수 있다[9]. Symbol Spectrum 24 카드를 위한 WPA 기능이 지원되는 시험용 디바이스 드라이버를 사용하여 Windows XP 스테이션을 구성하였다.

4. 결론 및 향후 과제

개발된 액세스포인트는 리눅스 환경을 사용하여 제작되었으며, embedded 시스템으로 만들어 질 수 있다. 그리고, 별도의 액세스포인트용 하드웨어를 사용하지 않고 일반 스테이션용 무선랜 카드를 사용하여 제작비를 줄일 수 있다. 단, 데이터 프레임의 암복호화 과정이 디바이스 드라이버에서 이루어지므로, CPU의 성능에 영향을 받을 수 있다. 이러한 영향에 대해서, 암복호화 과정이 하드웨어 내에서 이루어지는 액세스포인트용 펌웨어를 사용하여 성능 문제를 해결할 수도 있을 것이다.

Wi-Fi에서 제정한 WPA 규격을 준수한 무선랜 보안기술을 통하여 사용자 인증, 접근제어, 권한 검증, 데이터 기밀성과 무결성 등의 보안 요소를 만족 시킬 수 있다[10]. 이로써, 기존의 공중 무선랜 망 또는 사설 무선랜 망에서 문제가 제기되어온 보안 결함을 해결할 수 있다.

IEEE 802.11i 표준이 확정되면, WPA보다 강력한 RSN(Robust Security Network)이란 이름으로 무선랜의 보안이 이루어 질 것이다. RSN과 WPA의 가장 큰 차이점은 CCMP 알고리즘을 기본으로 사용한다는 점이다. CCMP를 구현하기 위해서는 기존 장비의 펌웨어만을 갱신하는 것으로는 구현하기가 어려우며 새로운 하드웨어를 사용하여야 하는 것으로 알려져 있다. 그러나, CCMP를 디바이스 드라이버 내에서 구현한다면 하드웨어 변경 없이 소프트웨어로 RSN 기능을 구현할 수 있다. 단, 이러한 방법에는 여전히 성능에 대한 문제가 남아있다.

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

[4] "Wi-Fi Protected Access," version 2.0, Wi-Fi Alliance, April 2003.

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

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

[7] "Open Source Implementation of IEEE 802.1X," http://www.open1x.org/.

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

[9] "Windows XP의 WPA 무선 보안 업데이트 개요," http://support.microsoft.com/?kbid=815485, 2003년 8월.

[10] 강유성, 오경희, 정병호, "무선랜 보안기술의 진화 동향 및 전망", 전자통신동향분석, 제18권 제4호, 2003년 8월.