무선랜 환경에서 사용자 인증 및 기밀성 강화 방안에 관한 연구

홍성표* · 이 준**

A Study on Robust Authentication and Privacy in Wireless LAN

Seong-pyo Hong* · Joon Lee**

요 약

IEEE 802.1x는 802.11b의 사용자 인증 취약성을 보완한 프레임워크로, EAP를 통해 다양한 사용자 인증 메커니즘을 지원한다. 그러나 IEEE 802.1x 역시 인증 프로토콜의 구조적 원인에 의한 서비스 거부 공격과 AP에 대한 인증 및 암호 메커니즘의 부재로 세션 하이재킹 및 중간자 공격 등에 취약하다.

본 논문에서는 IEEE 802.1x 프레임워크의 취약성을 보완하여 강화된 사용자 인증 및 안전한 암호통신 서비스를 제공할 수 있는 무선랜 보안시스템을 제안하고자 한다. 무선랜 보안시스템에서 사용자 인증은 공개키 암호 기술을 이용하여 무선랜 사용자 및 AP, 인증서버간의 상호인증을 수행함으로써 제 3자가 무선랜 사용자, AP 또는 인증서버 등으로 위장하여 통신에 개입하는 것을 방지한다. 또한 동적 키 분배를 통해 사용자와 AP간의 안전한 암호통신을 제공한다.

ABSTRACT

The IEEE 802.1x standard provides an architectural framework which can be used various authentication methods. But, IEEE 802.1x also has vulnerabilities about the DoS, the session hijacking and the Man in the Middle attack due to the absence of AP authentication.

In this paper, we propose a WLAN secure system which can offer a robust secure communication and a user authentications with the IEEE 802.1x framework. The user authentication on the WLAN secure system accomplishes mutual authentications between authentication servers, clients and the AP using PKI and prevents an illegal user from intervening in communication to disguise oneself as a client, the AP or authentication servers. Also, we guarantee the safety of the communication by doing secure communication between clients and the AP by the Dynamic WEP key distribution.

키워드

Wireless LAN Security, Authentication, Privacy, IEEE 802.1x

Ⅰ. 서 론

무선랜 보안 서비스는 크게 승인된 사용자에게만 접속을 허용하는 인증(authentication)과, 스니퍼 등과 같은 해킹 툴을 이용해 전송되는 내용 자체를 몰래 보는 도청 행위를 방어할 수 있는 기밀성(privacy)에 관

* 조선대학교 대학원 컴퓨터공학과
** 조선대학교 전자정보공과대학 컴퓨터공학과

접수일자 : 2005. 7. 7

한 것이다. 특히 무선랜은 유선 네트워크와 달리 AP만 설치되어 있으면 누구나 쉽게 네트워크에 접근이 가능하기 때문에 무선랜에서 보다 중요성이 강조되는 보안 문제는 접속에 관한 보안, 즉 사용자 인증이라고 할 수 있다[1].

무선랜 표준인 IEEE 802.11b는 사용자 인증 및 암호화와 관련하여 SSID, MAC 주소 필터링, WEP 등의 메커니즘을 통해 보안서비스를 제공하고 있다[2]. 그러나 IEEE 802.11b에서 사용되는 보안 메커니즘들은 많은 취약성을 가지고 있으며, IEEE 802.11b의 사용자 인증 취약성을 보완한 프레임워크인 IEEE 802.1x 역시 인증 프로토콜의 구조적 원인에 의한 서비스 거부 공격과 AP에 대한 인증 및 암호 메커니즘의 부재로 세션 하이재킹 및 중간자 공격 등에 취약하다[8].

본 논문에서는 IEEE 802.1x 프레임워크의 취약성을 보완하여 강화된 사용자 인증 및 안전한 암호통신 서비스를 제공할 수 있는 무선랜 보안시스템을 제안하고자 한다. 무선랜 보안시스템에서 사용자 인증은 공개키 암호 기술을 이용하여 무선랜 사용자 및 AP, 인증서버간의 상호인증을 수행하여 제 3자가 무선랜 사용자, AP 또는 인증서버 등으로 위장하여 통신에 개입하는 것을 방지한다. 또한 키분배 메커니즘을 통해 사용자와 인증서버 사이에 동적 키 분배를 지원함으로써 사용자와 AP간의 안전한 암호통신을 제공한다.

본 논문의 구성은 다음과 같다. 2장에서는 IEEE 802.1x 프레임워크의 취약성에 대해 기술하고, 3장에서는 2장에서 기술한 IEEE 802.1x의 취약성을 보완하여 강화된 사용자인증 및 안전한 암호통신을 제공하는 무선랜 보안 시스템의 설계 및 구현 환경에 대해서 기술한다. 마지막으로 4장에서는 결론 및 향후 연구과제에 대해 논의한다.

Ⅱ. IEEE 802.1x 보안 메커니즘 취약성

IEEE 802.1x 인증 메커니즘은 클라이언트와 인증서버에 대한 인증만을 정의하고 있으며, 인증자에 대한 인증은 정의하고 있지 않다. 따라서 악의적인 사용자가 클라이언트에 대해서 정당한 인증자로 위장하거나, 인증서버 또는 클라이언트와 통신하는 인터넷상의 클라이언트/서버에 대해서 클라이언트 위장 공격과 같은 다양한 형태의 스푸핑 공격이 가능하다[7].

그림 1은 스푸핑 공격의 한 형태로 EAP-SUCCESS 메시지 스푸핑을 이용한 중간자 공격이 가능함을 보여준다. 클라이언트에 대한 인증이 성공하였음을 알리는 EAP-SUCCESS 메시지는 무결성 메커니즘이 적용되지 않는다. 따라서 공격자는 EAP-SUCCESS 메시지를 가로챈 후, 정당한 인증자로 위장하여 EAP-SUCCESS 메시지를 클라이언트에게 전송하는 공격이 가능하다. 위장 공격이 성공하면 공격자는 클라이언트로부터 전송되는 모든 데이터의 내용을 알 수 있다.

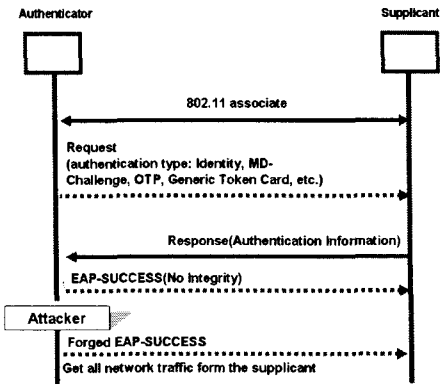


그림 1. EAP-SUCCESS 메시지 스푸핑
Fig. 1 Spoofing of EAP-SUCCESS message

세션 하이재킹 공격 또한 Disassociate 메시지가 무결성 서비스가 적용되지 않는 취약성을 이용한 방법으로, 그림 2와 같이 인증 완료 후 클라이언트와 인증자

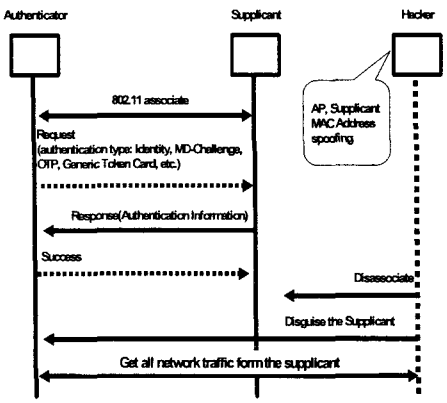


그림 2. Disassociate 메시지 스푸핑
Fig. 2 Spoofing of Disassciate message

의 통신 과정에 인증자의 MAC 주소로 위장한 공격자가 통신 종료를 알리는 Disassociate 메시지를 클라이언트로 전송해서 더 이상 통신을 못하도록 하는 방법이다. 이 후, 공격자는 클라이언트의 MAC 주소를 이용해 클라이언트로 위장하여 인증자와 통신을 계속할 수 있다[3-4].

Ⅲ. 강화된 사용자 인증 및 기밀성 지원 무선랜 보안시스템

3.1 시스템 설계 및 구현

IEEE 802.1x 프레임워크에서 AP는 전적으로 신뢰하는 요소로 취급된다. 즉 IEEE 802.1x는 사용자와 인증서버에 대해서만 인증을 수행하고 AP 인증은 수행하지 않는다. 따라서 악의적인 사용자가 정당한 AP로 위장이 가능하여 기밀성 서비스가 제공되지 않는 EAP-SUCCESS와 Disassociate 메시지 스푸핑에 의한 중간자 공격 및 세션 하이재킹 공격이 가능하다.

또한 IEEE 802.1x에서 인증 프로토콜은 인증과정의 구조적 원인에 의해 서비스 거부 공격[5]에 취약하다. 즉 사용자가 인증을 요구하면 사용자에 대한 확인없이 서버의 자원을 할당하고 인증 프로토콜을 진행하기 때문에, 악의적인 사용자가 연속적인 접근 요청을 통해 인증서버의 자원을 무한히 할당받도록 함으로써 합법적인 사용자가 서비스를 받지 못하게 할 수 있다. 만약 EAP-TLS[9]나 EAP-TTLS[6]와 같이 공개키 암호시스템을 기반으로 하는 인증방식을 사용하는 경우에는 더

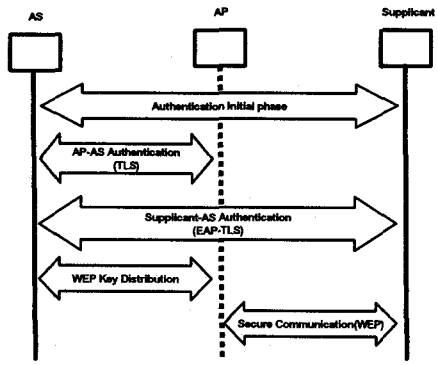


그림 3. 무선랜 보안 시스템
Fig. 3 Proposal Wireless LAN secure system

많은 계산과 자원 할당이 필요하기 때문에 연속적인 접근 요청을 차단할 수 있는 방법을 제공해야 한다.

본 논문에서 제안하는 무선랜 보안시스템의 목표는 IEEE 802.1x의 보안 취약성을 보완하여 강화된 사용자 인증과 안전한 암호통신을 보장하는 것이다.

먼저 서비스 거부 공격 보완 방안으로 사용자 인증 프로토콜을 수행하기 전에 인증서버에서 제시된 문제를 사용자가 해결할 경우에만 인증 프로토콜을 수행하도록 하는 인증 초기단계를 추가 하였다. 인증 초기단계는 일방적으로 서버쪽에서만 자원을 할당하는 구조를 사용자에게도 어느 정도 자신의 자원을 할당하도록 하고, 인증서버가 자신의 상태에 따라 보안수준 변수를 설정하여 사용자의 인증 요청을 제어할 수 있도록 함으로써 악의적인 사용자의 무차별적인 접근을 제한할 수 있다.

스푸핑 공격 보완 방안으로는 AP에 대한 인증 절차를 추가하여 모든 구성 개체에 대해서 상호인증을 제공하고, 전송되는 메시지를 암호화 알고리즘을 이용하여 암호화하였다. 따라서 인증받지 않은 제 3자의 개입에 의한 스푸핑 공격을 차단할 수 있으며, 전송 메시지에 대한 기밀성 제공으로 해킹에 의한 노출을 방지할 수 있다. 사용자와 인증서버간 상호인증 메커니즘은 공개키 암호기술 기반인 EAP-TLS를 이용하고, 추가된 AP와 인증서버간 상호인증 역시 공개키 암호기술을 이용하기 때문에 안전성을 보장받을 수 있다. 또한 IEEE 802.11b 표준에서 지적된 고정된 암호화 키의 장기간 사용으로 인한 취약성 문제는 EAP-TLS 인증과정에서 키 분배 메커니즘을 통해 동적 키 분배를 제공함으로써 사용자와 AP간의 안전한 암호통신을 제공한다.

제안 메커니즘 테스트를 위한 시스템은 그림 4와 같이 클라이언트, AP, 인증서버 및 CA(Certificate Authority)로 구성된다. 클라이언트는 AP를 통해서 네트워크를 이용하려는 사용자이며, AP는 클라이언트의 네트워크 접속을 중개하는 역할을 한다. 인증서버는 클라이언트와 AP에 대한 인증을 수행하여 인증 받지 못한 사용자 및 AP를 차단하고 정상적으로 인증을 받은 사용자와 AP만 접속을 허용한다. CA는 클라이언트와 AP, 인증서버에 필요한 인증서를 발행한다.

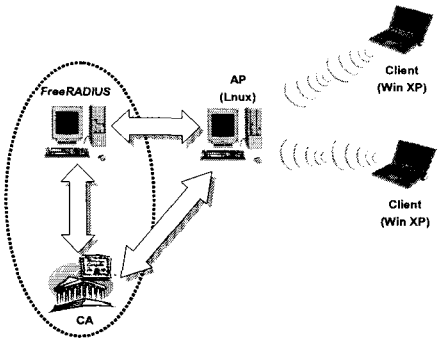


그림 4. 시스템 구성도
Fig. 4 Structure of proposal system

클라이언트는 그림 5와 같이 사용자 인터페이스와 환경설정 모듈, 문제 계산(Puzzle Compute)모듈, 패킷 처리부, EAPoL 패킷 처리부 등으로 구성된다.

EAPoL 패킷 처리부는 무선환경에서 인증서버로부터 인증을 받기위한 EAP-TLS 패킷을 생성하고, 이를 EAPoL 프레임에 담아 전송할 수 있도록 캡슐화(capsulation) 하는 기능과, 반대로 AP로부터 수신된 EAPoL 패킷을 일반 패킷으로 역캡슐화(decapsulation) 하는 기능을 제공한다.

문제 계산 모듈은 인증서버로부터 수신한 보안수준 변수 값에 따라 해쉬함수를 이용하여 주어진 문제를 계산하는 모듈이며, 보안수준 변수 값이 '0' 인 경우 문제 계산 모듈은 실행되지 않는다. 패킷 처리부는 EAPoL 패킷을 AP로 송신하는 기능과 AP로부터 수신한 메시지의 형식을 구분하여 일반 패킷 데이터인 경우에는 패킷 처리부로, EAP 패킷인 경우에는 EAPoL 패킷 처리부로 전송한다. 환경설정 모듈은 무선랜 카드 선택 및 네트워크 이름인 SSID 설정과, 통신과정 중 WEP 사용 여부를 원한다. 그림 6은 클라이언트 프로그램 실행화면을 나타낸 것이다.

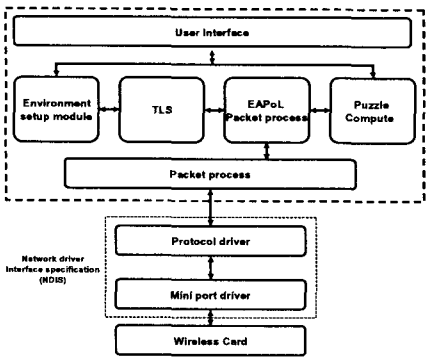


그림 5. 클라이언트 모듈
Fig. 5 Client module

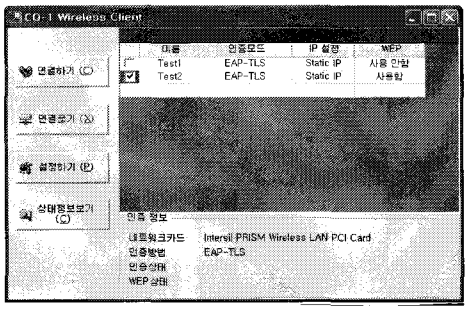


그림 6. 클라이언트 프로그램
Fig. 6 Client program

AP는 그림 7과 같이 TLS 모듈과 EAP-RADIUS 모듈, 패킷 처리부 등으로 구성된다. TLS 모듈은 인증서버와 상호인증을 수행하며, EAP-RADIUS 모듈은 클라이언트로부터 수신한 EAP 메시지를 RADIUS 패킷으로 캡슐화하는 RADIUS Encapsulation 루틴과 RADIUS 서버로부터의 응답 메시지를 EAP 패킷으로 역캡슐화하는 RADIUS Decapsulation 루틴으로 구성된다.

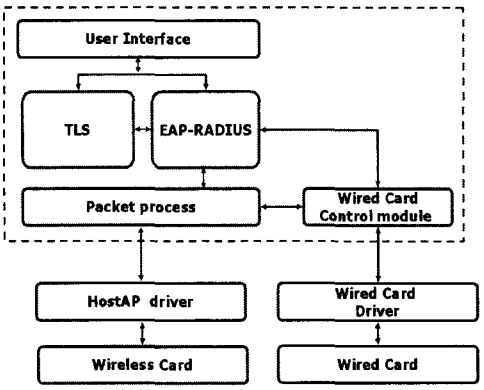


그림 7. AP 모듈
Fig. 7 AP module

3.2 시스템 평가

본 논문에서 제안한 무선랜 보안 시스템은 구성 개체 모두에 대한 상호인증을 수행하기 때문에 클라이언트, AP, 인증서버로의 위장이 불가능한 매우 안전한

사용자 인증을 제공한다. 또한 EAP-SUCCESS 메시지를 암호화하여 무결성 서비스를 제공하고, 키 분배 메커니즘을 통해 인증을 수행할 때마다 전수조사 공격에 안전한 128 bit의 새로운 키가 분배되기 때문에 안전한 암호통신을 제공한다.

그러나 제안 시스템은 AP 인증이 추가되고, 인증 알고리즘 또한 공개키 기술을 기반으로 하기 때문에 AP 인증을 제공하지 않는 기존 인증 메커니즘에 비해 인증완료까지 비교적 많은 시간이 소요되었다. 또한 서비스 거부 공격을 방지하기 위해 추가된 인증 초기단계에서 보안수준을 높일 경우, 인증 초기단계의 추가 의도대로 악의적인 사용자의 무차별적인 접근은 차단할 수 있으나, 정상적인 사용자의 경우는 인증시간이 더 길어지는 문제가 발생하였다.

Ⅳ. 결 론

무선랜은 배선이 필요 없어 단말기의 재배치가 쉽고 이동 중에도 통신이 가능할 뿐만 아니라 빠른 시간 안에 네트워크 구축이 용이한 장점을 가지고 있으나 사용 매체의 공개성에 따른 해킹 및 접근이 용이하기 때문에 보안에 매우 취약하다.

IEEE 802.11b의 사용자 인증 취약성을 보완한 IEEE 802.1x 프레임워크는 논리적 포트 개념을 도입하여 최종단 망 시스템인 브릿지 또는 AP에서 인증을 수행한 다음 사용자가 네트워크에 접근할 수 있도록 하는 포트 기반 접근제어 메커니즘으로써, EAP를 통해 다양한 사용자 인증 메커니즘을 사용할 수 있도록 하고 있다. 그러나 IEEE 802.1x 역시 인증 프로토콜의 구조적 원인에 의한 서비스 거부 공격과 AP 인증 및 암호 메커니즘의 부재로 세션 하이재킹 및 중간자 공격 등에 취약하다.

본 논문에서는 IEEE 802.1x 프레임워크의 보안 취약성을 보완하여 강화된 사용자 인증 및 안전한 암호통신 서비스를 제공할 수 있는 무선랜 보안시스템을 제안하였다.

무선랜 기술이 널리 확산되고 더불어 사용자가 증가하고 있는 시점에서 제안 시스템은 의도되지 않은 제 3자가 AP를 이용하거나, 사용자와 AP 사이의 통신에 개입하여 도청, 위조, 변조를 수행하는 공격으로부터 안전한 무선랜 환경을 제공하는데 활용될 수 있다. 다만 제안 시스템은 AP 인증이 추가되고, 인증 알고리즘 또한 공개키 기술을 기반으로 하기 때문에 기존 인증 메커니즘에 비해 인증에 비교적 많은 시간이 소요되었다. 또한 인증 초기단계에서 보안수준 변수 값을 높일 경우, 인증 초기단계의 추가 의도대로 악의적인 사용자의 무차별적인 접근은 차단할 수 있으나, 정상적인 사용자의 경우는 인증시간이 더 길어지는 문제가 발생하였다.

향후 연구방향으로 인증과정에 RSA 알고리즘보다 더 작은 길이의 키를 이용하면서도 동일한 보안강도를 제공하는 ECC(Elliptic Curve Crypto system)와 같은 암호화 알고리즘을 지원하여 인증시간을 단축시키는 방안과 기존 인증 프로토콜에서 패킷 잃어버림 등이 발생할 때 올바른 패킷이 전송되도록 하기 위해 보장된 재전송을 이용한 서비스 거부 공격 대응방안에 대한 연구가 필요하다.

참고문헌

[1] William A. Arbaugh, N. Shankar, 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, pp. 1-13, 2001.

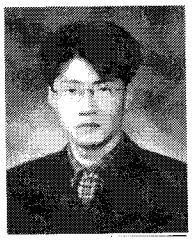
[2] J.R. Walker, "Unsafe at Any Key Size; An Analysis of the WEP Encapsulation", IEEE 802.11 Committee, pp. 1-9, 2000.

[3] InterLink Networks, *Securing Hotspots with RADIUS*, InterLink Networks White Paper, 2004.

[4] IEEE, *Draft P802.1X/D11: Standard for Port based Network Access Control*, IETF Network Working Group, 2001.

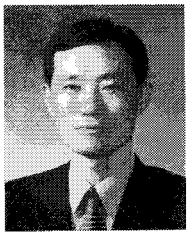
[5] Joshua Hill, "An Analysis of the RADIUS Authentication Protocol", Joshua Hill, pp. 1-12, 2001.
[6] P. Funk, S. Blake-Wilson, *EAP Tunneled TLS Authentication Protocol (EAP-TTLS)*, IETF PPPEXT Working Group, 2005.
[7] Arunesh Mishra, William A. Arbaugh, "An Initial Security Analysis of the IEEE 802.1X Standard", University of Maryland, pp. 1-12, 2002.
[8] B. Aboba, D. Simon, *PPP EAP TLS Authentication Protocol*, IETF Network Working Group, 1999.
[9] L. Blunk, J. Vollbrecht, *PPP Extensible Authentication Protocol(EAP)*, IETF Network Working Group, 1998.

저자소개



홍성표(Seong-pyo Hong)

1997년 광주대학교 전자계산학과(공학사)
2001년 2월 조선대학교 컴퓨터공학과(공학석사)
2005년 조선대학교 컴퓨터공학과 (공학박사)
※관심분야: 시스템 보안, 운영체제, 무선랜 보안



이 준(Joon Lee)

1979년 조선대학교 전자공학과 (공학사)
1981년 조선대학교 대학원 전자공학과(공학석사)
1997년 숭실대학교 대학원 전자계산학과(공학박사)
1982년 - 현재 조선대학교 전자정보공과대학 컴퓨터공학과 교수
※관심분야: 운영체제, 정보보호, 유비쿼터스 컴퓨팅