IEEE 802.1x 프레임워크 기반에서의 무선랜 보안 강화 방안에 관한 연구

이 준* · 홍성표** · 신명숙 **

A Study on Intensified scheme to WLAN Secure based on IEEE 802.1x Framework

Joon Lee* · Seong-pyo Hong** · Myeong-sook Shin**

이 논문은 2005년도 조선대학교 학술 연구비의 지원을 받아 연구되었음

요 약

IEEE 802.1x는 EAP(Extended Authentication Protocol)를 통해 해쉬 함수를 이용한 Challenge/Response, Keberos, 인증서를 기반으로 하는 TLS, One-Time Password 등 다양한 사용자인증 메커니즘들을 지원한다. 그러나 AP에 대한 인증 및 암호 메커니즘의 부재와 인증 프로토콜의 구조적 원인에 의해 스푸핑 및 DoS(Denial of Service) 공격 등에 취약하다.

본 논문에서는 IEEE 802.1x 프레임워크의 스푸핑 및 DoS 공격 취약성을 보완하여 안전한 사용자 인증 및 암호통신 서비스를 제공하는 무선랜 보안시스템을 제안하고자 한다. 제안 시스템은 공개키 암호기술을 이용하여 전송 메시지에 대한 무결성 서비스를 통해 안전한 암호통신을 제공하며, 인증초기단계를 통해 DoS 공격을 방지한다.

ABSTRACT

The IEEE 802.1x can be using various user authentication mechanisms: One-Time Password, Certificate-Based TLS, Challenge/Response and Keberos through EAP(Extended Authentication Protocol). 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 safety secure communication and a user authentications by intensified the vulnerability of spoofing and DoS attacks. The suppose system offers a safe secure communication because it offers sending message of integrity service and also it prevents DoS attack at authentication initial phase.

키워드

Wireless LAN Security, Authentication, Privacy, IEEE 802.1x framework

Ⅰ. 서 론

무선랜은 다양한 정보와 자원을 공유할 수 있게 하는 랜의 장점과 제약없는 연결성 제공이라는 편리성을 동시에 제공하는 무선 통신기술의 결정체로서, 신뢰성 있는 데이터 전송뿐만 아니라 유연성과 설치의 용이성이란 장점을 갖고 있다. 그러나 무선이라는 특성은 편리함과 이동성이라는 장점을 제공하는 반면 모든 무선 단말에서

* 조선대학교 전자정보공과대학 컴퓨터공학과
** 조선대학교 대학원 컴퓨터공학과

접수일자 : 2005. 7. 15

송.수신되는 데이터를 청취할 수 있으므로 무선랜을 이용하여 데이터를 전송하는 경우 정당한 송.수신자 이외의 제 3자가 데이터를 알아볼 수 없도록 하는 기밀성과 정당한 사용자가 접속하였는지를 확인할 수 있는 인증기능이 필요하다[1].

무선랜 표준인 IEEE 802.11b는 사용자 인증 및 암호화와 관련하여 SSID, MAC 주소 필터링, WEP 등의 메커니즘을 통해 보안서비스를 제공하고 있다. 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 DoS 공격과 AP에 대한 인증 및 암호 메커니즘의 부재로 스푸핑 공격에 취약하다[2-3].

본 논문에서는 IEEE 802.1x 프레임워크의 DoS 공격 및 스푸핑 공격에 대한 취약성을 보완하여 안전한 사용자 인증 및 기밀성을 제공하는 무선랜 보안시스템을 제안하고자 한다. 제안 시스템은 공개키 암호기술을 이용한 전송 메시지의 무결성 서비스 제공과 인증초기단계를 통해 스푸핑 및 DoS 공격을 방지한다.

본 논문의 구성은 다음과 같다. 2장에서는IEEE 802.1x 프레임워크의 취약성을 보완하기 위해 제안한 메커니즘에 대해서 기술하고 3장에서는 제안 메커니즘의 안전성에대해 평가한다. 마지막으로 4장에서는 결론 및 향후 연구과제에 대해 논의한다.

Ⅱ. IEEE 802.1x 프레임워크의 취약성 및 보완 방안

2.1 DoS 공격 취약성 및 보완 방안

2.1.1 인증 초기단계

EAP 인증 프로토콜은 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[8].

이러한 문제점을 해결하기 위해 본 논문에서는 인증서버의 현재 상태에 따라 문제(puzzle)를 제시하고 사용자가 문제를 해결할 경우에만 인증 프로토콜을 수행하도록 하는 인증 초기단계를 추가하였다. 인증 초기단계는 인증 요청시 일방적으로 서버 쪽에서만 자원을 할당하는 구조를 사용자 측에서 먼저 자원을 할당하는 방식으로 바꾼 것이다.

문제는 식 (2.1)과 같이 사용자의 아이덴티티 ID_C, 사용자의 난수 N_C, 서버의 난수 N_S, 전사공격 방법을 이용해 계산해야 하는 값 X로 구성된다. Y는 해쉬한 값에서 보안수준 변수 k 만큼의 '0' bit를 제외한 나머지 bit를 나타낸다.

$$h(ID_C, N_S, N_C, X) = 00.....00Y \quad (2.1)$$

인증서버로부터 제시되는 문제의 난이도는 보안수준 변수 k 값에 따라 결정된다. 즉 보안수준 변수 k가 '0' 일 경우 단말기는 연산을 하지 않고, k가 '128' 일 경우에는 MD5 해쉬함수를 이용해서 X 값을 찾을 수 없기 때문에 본 논문에서는 보안수준 변수 k 값으로 '0' 에서 '64' 사이의 값을 사용하였다. 따라서 제안 시스템은 인증서버의 현재 상태에 따라 보안수준 변수 k 값을 유동적으로 책정하여 사용자의 인증 요청을 제어할 수 있다.

2.1.2 프로토콜

인증 초기단계의 프로토콜 흐름은 그림 1과 같이 인증서버는 현재 상태에 대한 보안수준 변수 k를 결정하고 랜덤변수 N_S를 생성하여 사용자에게 보낸다. 보안수준 변수 k 값에 따라 사용자는 랜덤변수 N_C를 생성하고 해쉬함수를 이용하여 전사공격 방법으로 X 값을 계산한 후 사용자의 아이덴티티 ID_C, 사용자의 난수 N_C, 서버의 난수 N_S, 보안수준 변수 k와 함께 인증서버로 전송한다. 인증서버는

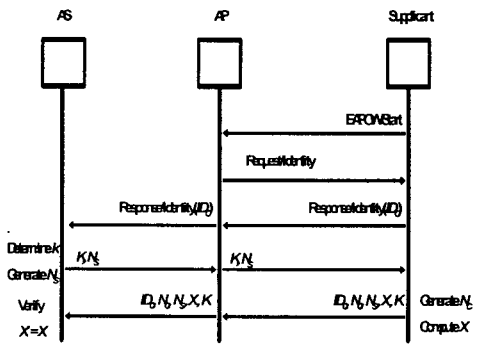


그림 1. 인증 초기단계 프로토콜
Fig. 1 Protocol of authentication initial phase

사용자로부터 받은 인수들을 이용하여 계산된 X' 값과 사용자로부터 받은 X 값을 비교하여 올바른 값이면 인증 프로토콜을 수행한다. 인증 초기단계는 사용자의 인증 요청 시 마다 서버의 난수 N_S와 보안수준 변수 k를 다르게 함으로써 사용자가 미리 X 값을 계산할 수 없다.

2.2 스푸핑 공격 취약성 및 보완 방안

2.2.1 AP와 인증서버간 상호인증

기존 무선랜 사용자 인증 메커니즘의 가장 큰 문제는 AP에 대한 인증을 제공하지 않는다는 것이다. 따라서 공격자가 스푸핑 공격을 이용해 AP의 IP 주소나 MAC 주소를 위장하여 클라이언트와 인증서버 사이에서 중간자 공격을 수행할 수 있다[4-5].

제안 시스템에서는 그림 2와 같이 AP에 대한 인증 절차를 추가하여 모든 구성 개체에 대해서 상호인증을 수행한다. 따라서 인증받지 않은 제 3자의 개입에 의한 스푸핑 공격을 차단할 수 있으며, 공개키 암호기술과 인증서를 기반인 TLS를 이용하여 인증하기 때문에 안전성을 보장받을 수 있다.

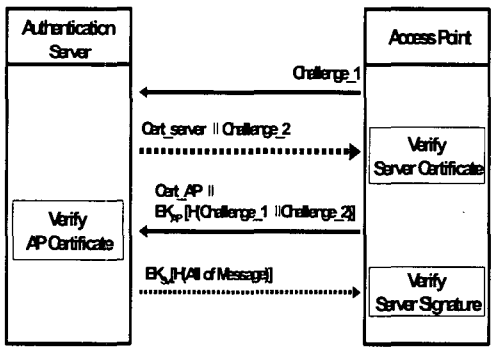


그림 2. AP 인증
Fig. 2 AP authentication

2.2.2 메시지 암호화

클라이언트와 인증서버간 상호인증이 완료되면, 인증서버는 AP에게 인증 성공을 알리는 SUCCESS 메시지를 전송한다. 제안 시스템에서 SUCCESS 메시지는 식 (2.2)와 같이 클라이언트와 인증서버간 상호인증 과정에서 생성된 FINISHED 메시지와 공유키(WEP_Key) 그리고 인증서버의 전자서명으로 구성된다. FINISHED는 인증서버와 클라이언트 간 상호인증 과정에서 인증서버가 클라이언트에게 인증완료를 알리는 메시지이며, 공유키는 클라이언트와 인증서버간 인증과정을 통해 공유한 키이다.

$$EK_{AP}\,[EK_{SERVER}\,[\,h(\text{FINISHED} \parallel \text{WEP\_Key})\,] \parallel \text{FINISHED} \parallel \text{WEP\_Key}] \quad (2.2)$$

SUCCESS 메시지 전달 목적은 AP에게 클라이언트 인증이 성공하였음을 알리고 클라이언트와 AP 간 암호통신에 사용될 공유키를 전달하는 것이다. 즉 공유키는 클라이언트와 인증서버만 알고 있는 정보인데, 인증 완료 후에 WEP 암호통신을 하기 위해서는 AP도 알아야 하므로 공유키를 전달한다. 또한 공유키는 외부로 노출되어서는 안되는 정보이므로 AP의 공개키로 암호화한 후 전송된다.

인증서버로부터 SUCCESS 메시지를 수신한 AP는 그림 3과 같이 SUCCESS 메시지를 복호화한 뒤, 식 (2.3)과 같은 구성을 갖는 EAP-SUCCESS 메시지를 생성하고 이를 다시 공유키로 암호화해서 클라이언트에게 전송한다. 이 때 공유키는 서버로부터 수신한 SUCCESS 메시지를 복호화하여 얻은 값이다.

$$EK_{WEP\_Key}\,[\,EK_{SERVER}\,[\,h(\text{FINISHED} \parallel \text{WEP\_Key})\,] \parallel \text{FINISHED} \parallel \text{WEP\_Key}] \quad (2.3)$$

EAP-SUCCESS 메시지는 클라이언트에 AP가 인증된 AP임을 알리는 목적으로 사용된다. 즉 인증서버와 인증을 수행하지 못한 AP라면 AP의 비밀키를 알지 못하기 때문에 SUCCESS 메시지 전체를 복호화할 수 없고, 공유키 또한 얻지 못하기 때문에 공유키로 암호화된 메시지를 클라이언트에게 전송할 수 없다. 또한 EAP-SUCCE

SS 메시지에는 서버의 전자서명이 포함되어 있다. 따라서 공격자가 공유키를 알아냈다 하더라도 서버의 개인키를 모르면 전자서명을 생성하지 못하기 때문에 식 (2.3)을 생성할 수 없다.

AP로부터 EAP-SUCCESS 메시지를 수신한 클라이언트는 EAP-SUCCESS 메시지가 인증서버와의 인증과정에서 교환된 공유키로 복호화되지 않을 경우 통신을 종료한다. 복호화에 실패한 경우는 AP가 인증서버로부터 정당한 공유키를 분배받는데 실패한 것을 뜻하며, 이는 AP 인증이 이루어지지 않았다는 것을 의미하므로 통신을 종료

한다. 또한 복호화에 성공하였더라도 복호화된 내용에서 인증서버의 전자서명이 없거나 전자서명 확인에 실패한 경우에도 AP가 인증서버로부터 인증을 받는데 실패하여 인증서버의 전자서명을 획득하지 못하였다는 것을 의미하므로 마찬가지로 통신을 종료한다.

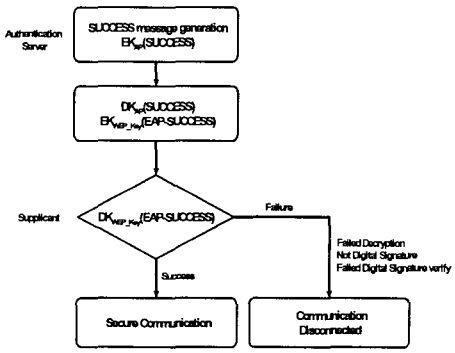


그림 3. WEP_Key 분배 및 암호통신 과정
Fig. 3 Process of WEP_Key disrtibution and secure communications

Ⅲ. 제안 메커니즘 안전성 평가

3.1 스푸핑 공격에 대한 안전성

IEEE 802.1x 인증 메커니즘은 클라이언트와 인증서버에 대한 인증만을 정의하고 있기 때문에 악의적인 사용자가 클라이언트에 대해서 정당한 인증자로 위장하거나, 인증서버 또는 클라이언트와 통신하는 인터넷상의 클라이언트/서버에 대해서 클라이언트 위장과 같은 다양한 형태의 스푸핑 공격이 가능하다[7][9].

본 논문에서는 부정한 사용자의 위장 공격에 의한 스푸핑 공격을 방지하기 위해 AP에 대해서도 상호인증을 수행하도록 하였다. AP 인증은 안전성에서 이미 입증된 공개키 암호기술을 기반으로 하는 TLS 메커니즘을 이용함으로써 위장 공격에 안전하다고 할 수 있다. 또한 EAP-SUCCESS 메시지의 무결성 서비스 부재로 인한 스푸핑 공격을 방지하기 위해 EAP-SUCC

ESS 메시지를 암호화하여 전송하도록 하였다. 따라서 공격자는 AP로 위장이 불가능할 뿐만 아니라 EAP-SUCCESS 메시지 생성 자체도 불가능하기 때문에 제안 시스템은 위장 공격에 안전하다.

3.2 DoS 공격에 대한 안전성

IEEE 802.1x에서 지원하는 인증 프로토콜 중 EAP-TLS나 EAP-TTLS는 공개키 암호시스템을 기반으로 하기 때문에 많은 계산량과 자원 할당이 필요하다. 만약 인증과정에서 악의적인 사용자가 연속적인 접근 요청을 보내게 되면, 인증서버는 요청에 대한 불필요한 암호학적 연산을 수행하게 되어 인증서버의 자원을 낭비하게 된다. 따라서 인증 및 키 교환 과정에서 악의적인 사용자의 무차별적인 접근 요청을 방지할 수 있는 보다 능동적인 대처방안이 필요하다. 즉 인증서버가 사용자의 인증 요청을 제어할 수 있는 방법이 필요하다[6].

본 논문에서 제안하는 보안수준 변수를 이용한 인증 초기단계는 인증서버가 제시한 문제를 사용자가 해결할 경우에만 인증 프로토콜을 실행하게 하였다. 이는 인증 요청 시 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. 또한 보안수준 변수는 그림 4와 같이 인증서버의 현재 상태에 따라 값을 유동적으로 설정할 수 있다. 즉 평소에는 k가 '0' 으로 설정되어 X 값 계산 없이 인증이 수행되다가 연속적인 인증 요청이 들어오거나 서버 자원의 여유가 부족할 때 보안수준 변수 k 값을 증가시키면 사용자는 X 값을 찾기 위한 연산량이 많아지기 때문에 악의적인 사용자의 무차별적인 접근을 막을 수 있다.

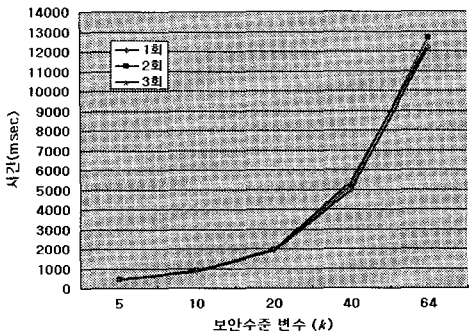


그림 4. k에 따른 X 값 계산 시간
Fig. 4 Times of X value computation to k

Ⅳ. 결 론

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 Challenge/Response, Kerberos, TLS, OTP 등 다양한 사용자 인증 메커니즘을 사용할 수 있도록 하고 있다. 그러나 IEEE 802.1x 역시 인증 프로토콜의 구조적 원인에 의한 DoS 공격과 AP 인증 및 암호 메커니즘의 부재로 스푸핑 공격 등에 취약하다.

본 논문에서는 IEEE 802.1x 프레임워크의 DoS 공격 및 스푸핑 공격에 대한 취약성을 보완하여 안전한 사용자 인증 및 암호통신 서비스를 제공하는 무선랜 보안시스템을 제안하였다. 제안 시스템은 인증 초기단계를 통해 사용자의 인증 요청을 제어함으로써 악의적인 사용자의 무차별적인 접근을 통한 DoS 공격을 차단할 수 있으며, 전송되는 메시지에 대한 암호화를 수행하기 때문에 도청, 위조, 변조 공격으로부터 안전한 무선랜 환경을 제공하는데 활용될 수 있다.

향후 연구방향으로 기존 인증 프로토콜에서 패킷 잃어버림 등이 발생할 때 올바른 패킷이 전송되도록 하기 위해 보장된 재전송을 이용한 DoS 공격 대응방안에 대한 추가적인 연구가 필요하다.

참고문헌

[1] Danai Patiyoot, S. J. Shepherd, "Cryptographic security Techniques for wireless networks", ACM SIGOPS Operating Systems Review, pp. 36-50, 1999.

[2] Daniel B. Faria, David R. Cheriton, "DoS and authentication in wireless public access networks", WiSe'02 Conference, pp. 47-56, 2002.

[3] P. Funk, S. Blake-Wilson, *EAP Tunneled TLS Authentication Protocol (EAP-TTLS)*, IETF PPPEXT Working Group, 2005.

[4] Arunesh Mishra, William A. Arbaugh, "An Initial Security Analysis of the IEEE 802.1X Standard", University of Maryland, pp. 1-12, 2002.

[5] Wi-Fi Alliance, *Wi-Fi Protected Access*, Wi-Fi Alliance White Paper, 2003.

[6] William A. Arbaugh, *802.11 Security Vulnerabilities*, University of Maryland, 2003.

[7] J.-C. Chen, M.-C. Jiang, Y.-W. Liu, "Wireless LAN Security and IEEE 802.11i", IEEE Wireless Communications, pp. 1-19, 2004.

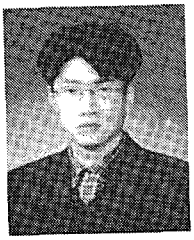
[8] John Vollbrecht, Robert Moskowitz, *Wireless LAN Access Control and Authentication*, InterLink Networks White Paper, 2002.

[9] Changhua He, John C. Mitchell, "Security analysis: Analysis of the 802.11i 4-way handshake", WiSe'04 Conference, pp. 43-50, 2004.

저자소개

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



홍 성 표(Seong-pyo Hong)

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

신 명 숙(Myeong-Sook Shin)

1992년 광주대학교 전자계산학과 (공학사)
1996년 광주대학교 대학원 컴퓨터학과(공학석사)
2006년 조선대학교 대학원 컴퓨터공학과 수료
※ 관심분야: 시스템소프트웨어, 유비쿼터스 컴퓨팅, 정보보호