IEEE 802.1x EAP-TLS 인증 메커니즘 기반 Wireless LAN 시스템

홍성표* · 한승조**

Wireless LAN System based on IEEE 802.1x EAP-TLS Authentication Mechanism

Seong-pyo Hong* · Seung-jo Han**

요 약

IEEE 802.1x는 802.11b의 사용자 인증 취약성을 보완한 프레임워크로, EAP를 통해 다양한 사용자 인증 메커니즘을 지원하지만 인증 프로토콜의 구조적 원인에 의한 서비스 거부 공격(DoS)과 AP에 대한 인증 및 암호 메커니즘의 부재로 세션 하이재킹 및 중간자 공격(MiM) 등에 취약하다.

본 논문에서는 IEEE 802.1x 프레임워크의 보안 취약성을 보완하여 안전한 통신을 제공하는 시스템을 제안하였다. 제안 시스템은 공개키 암호 기술을 이용하여 무선랜 사용자 및 AP, 인증서버간의 상호인증을 수행함으로써 제3자가 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(Denial of Service), the session hijacking and the MiM(Man in the Middle) attack due to caused by structural of authentication protocol.

In this paper, we propose a WLAN system which can offer safety communication by complement of IEEE 802.1x vulnerabilities. The WLAN 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 the Dynamic WEP key distribution between clients and the AP.

키워드

무선랜 보안, 인증, IEEE 802.1x, EAP-TLS

Key word

Wireless LAN Security, Authentication, IEEE 802.1x, EAP-TLS

* 정회원 : 조선대학교 산학협력단 (hongsp@chosun.ac.kr)
** 종신회원 : 조선대학교 정보통신공학과

접수일자 : 2012. 04. 30
심사완료일자 : 2012. 05. 31

Open Access http://dx.doi.org/10.6109/jkiice.2012.16.9.1983

Ⅰ. 서 론

IEEE 802.11b[1]의 사용자 인증 취약성[2-5]을 보완한 프레임워크로 제안된 IEEE 802.1x[6-10]는 EAP (Extended Authentication Protocol)를 통해 해쉬함수를 이용한 Challenge/Response, Kerberos, 인증서를 기반으로 하는 TLS(Transport Layer Security), OTP(One-Time Password) 등 다양한 사용자 인증 메커니즘을 지원한다. 그러나 IEEE 802.1x 역시 인증 프로토콜의 구조적 원인에 의한 DoS(Denial of Service) 공격과 AP에 대한 인증 및 암호 메커니즘의 부재로 세션 하이재킹 및 MiM(Man in the Middle) 공격 등에 취약하다.

본 논문에서는 기존의 IEEE 802.1x 프레임워크에 AP에 대한 인증과정을 추가하여 상호인증이 수행되도록 하였으며 인증과정뿐만 아니라 인증완료 후 전송되는 모든 데이터에 암호화를 수행함으로써 데이터 보안 중요도가 높은 응용에서 이용이 가능하도록 하였다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구에 대해 기술하고, 3장에서는 본 논문에서 제안하는 시스템의 설계 및 구현 환경에 대해서 기술한다. 마지막으로 4장에서는 결론 및 향후 연구과제에 대해 논의한다.

Ⅱ. 관련 연구

2.1. IEEE 802.1x

IEEE 802.11b 표준에서 제공하는 사용자 인증 메커니즘인 SSID나 공유키 인증의 경우 보안 취약성을 가지고 있다. 이에 따라 IEEE 802.11b의 사용자 인증 취약성을 보완하기 위한 방안으로 개발된 것이 IEEE 802.1x 프레임워크이다. IEEE 802.1x는 그림 1과 같이 사용자가 논리적 포트를 통해 네트워크 자원에 접근할 수 있도록 하며, 그림 2와 같이 EAP를 통해 해쉬함수를 이용한 Challenge/Response, Kerberos, 인증서를 기반으로 하는 TLS, OTP 등 다양한 사용자 인증 메커니즘들을 사용할 수 있도록 지원한다.

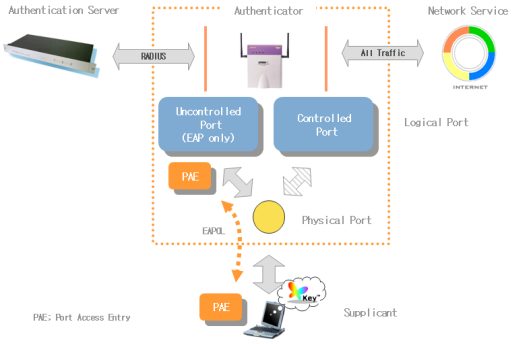

그림 1. IEEE 802.1x 프레임워크
Fig. 1 IEEE 802.1x framework

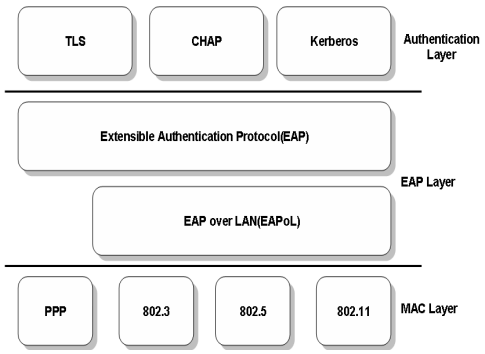

그림 2. EAP 스택구조
Fig. 2 EAP Stack Structure

2.2. EAP-TLS

IEEE 802.1x를 이용해 보다 강력한 무선랜 보안 환경을 구축하기 위해서는 양방향 인증과 동적 암호화 키 혹은 TKIP를 이용할 수 있도록 키 교환 메커니즘을 지원할 수 있는 인증 알고리즘이 필요한데, 이러한 조건들을 만족하는 인증 알고리즘이 EAP-TLS이다. EAP-TLS는 상호인증 프로토콜인 TLS를 EAP 상에서 구현한 것으로, 공개키 기반 인증서를 이용하여 선택적으로 양방향 인증을 수행하며 인증 후 TLS 레코드 레이어에서 제공하는 암호화 키 생성 알고리즘을 이용하여 PMK(Pairwise Master Key)를 생성한다. 생성된 PMK는 암호화 키 혹은 TKIP의 PTK를 생성하는데 사용한다[8-10].

EAP-TLS 인증 프로토콜의 흐름은 그림 3과 같이 우선 클라이언트와 인증자(Access Point)는 802.11b 방식에 의한 인증을 수행한다.

표 1. IEEE 802.1x 인증 메커니즘 비교
Table. 1 Comparison of IEEE 802.1x authentication Mechanism

구 분	서버의 단말기 인증	단말기의 서버 인증	Dynamic WEP	접근제어의 문제점	서버의 자원 할당		DoS 공격
					인증프로토콜 실행 전	인증프로토콜 실행 중	
EAP-MD5	Password	no	불가능	○	사용자의 password	요청 시 무조건 할당	○
EAP-TLS	Certificate	Certificate	가능	○	-	요청 시 무조건 할당	○
EAP-TTLS	Certificate	Password	가능	○	사용자의 password	요청 시 무조건 할당	○

즉 SSID 또는 MAC 주소 필터링에 의한 인증을 수행하고 나서 802.1x 인증에 필요한 정보를 주고받는다. 이 과정까지는 802.1x EAP에 의한 인증이 이루어지기 전이기 때문에 클라이언트는 인증서버 외의 다른 네트워크 자원은 이용할 수 없다. 네트워크 자원은 TLS를 통한 인증이 이루어진 이후에 인증자를 통해 이용할 수 있다.

EAP-TLS 인증과정을 자세히 기술하면 다음과 같다 [10-11].

① 클라이언트와 인증자 사이에 MAC 레벨 인증 및 암호화를 설정하여 기본 접속 절차를 수행한다. (802.11 Authentication, Association)
② 클라이언트가 인증자에게 접속 요청을 한다. (EAPoL-Start)
③ 인증자는 클라이언트에게 신원 요구를 한다. (EAP-Request/Identity)
④ 클라이언트는 자신의 identity를 인증자로 보낸다. (EAP-Response/Identity)
⑤ 인증자는 Access-Request 메시지에 클라이언트의 identity를 포함하여 인증서버로 전달한다. (Access-Request)
⑥ 인증서버와 클라이언트 간의 인증 프로토콜 은 TLS를 사용한다. (TLS-Start)
⑥-1 인증서버는 신원을 확인한 클라이언트에게 인증서를 요구한다. (Server_hello)
⑥-2 클라이언트는 자신의 인증서를 AP를 통해 인증서버에게 보낸다.(Client_hello)
⑦ 응답한 인증서가 인증이 되면 인증서버는 EAP 성공 메시지를 클라이언트에게 전송한다. (EAP-Success)
⑧ 인증자는 인증 완료후 AP와 클라이언트 간의 암호통신에 사용할 WEP 키를 생성한다.
⑨ 인증자는 인증서버로부터 받은 키를 이용하여 WEP 키를 암호화한 후 클라이언트에게 전송한다. (EAPoL-Key)
⑩ 클라이언트와 인증자는 WEP 키를 이용해 암호 통신을 수행한다. WEP 키는 클라이언트가 로그아웃(log-out)을 하거나 재인증 타이머가 초과될 때까지 사용된다.

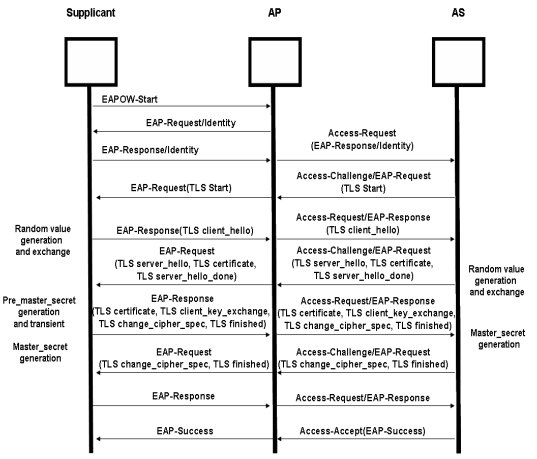

그림 3. EAP-TLS 프로토콜 흐름
Fig. 3 Flows of EAP-TLS protocol

Ⅲ. EAP-TLS 인증 메커니즘 기반 무선랜 시스템

3.1. 시스템 설계

IEEE 802.11b의 사용자 인증 취약성을 보완한 IEEE 802.1x 프레임워크는 EAP를 통해 해쉬함수를 이용한 Challenge/Response, Kerberos, 인증서를 기반으로 하는 TLS, OTP 등 다양한 사용자 인증 메커니즘을 지원한다. 그러나 IEEE 802.1x는 사용자 인증에 대해서만 정의하고 기밀성에 대 해서는 정의하고 있지 않다.

IEEE 802.1x 프레임워크에서 AP는 전적으로 신뢰하는 요소로 취급된다. 즉 IEEE 802.1x는 사용자와 인증서버만 인증을 수행하고 AP 인증은 수행하지 않는다[8-9]. 따라서 악의적인 사용자가 정당한 AP로 위장이 가능하여 기밀성 서비스가 제공되지 않는 EAP-SUCCESS 메시지 스푸핑에 의한 중간자 공격 및 Disassociate 메시지 스푸핑에 의한 세션 하이재킹 등과 같은 다양한 형태의 스푸핑 공격이 가능하다. 또한 IEEE 802.1x에서 인증 프로토콜은 인증과정의 구조적 원인에 의해 서비스 거부 공격에 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.

본 논문에서 제안하는 시스템은 그림 4와 같이 IEEE 802.1x를 기반으로 인증 초기단계를 거쳐 인증서버와 AP간 상호인증, 인증서버와 클라이언트간 상호인증, 공유 키(WEP_Key) 분배 등 4단계를 거쳐 인증이 수행된다.

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.

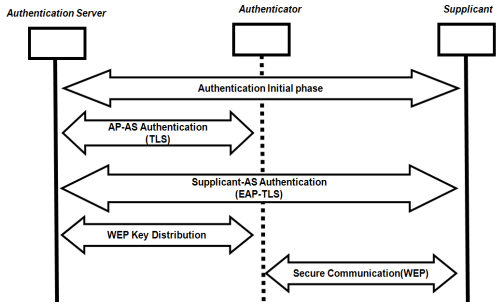

그림 4. 제안 시스템 인증 구조
Fig. 4 Structure of authentication in proposal system

스푸핑 공격 취약성 보완 방안으로는 그림 5와 같이 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.

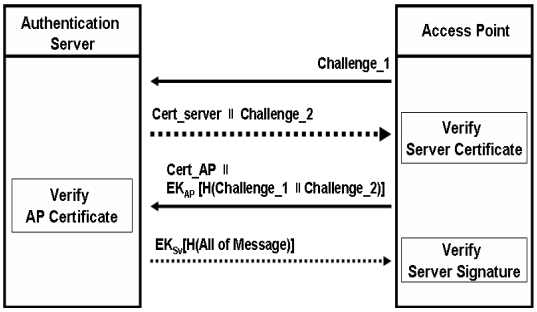

그림 5. AS-AP 상호인증
Fig. 5 Process of AP authentication

사용자와 인증서버간 상호인증 메커니즘은 그림 6과 같이 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 인증 과정에서 키 분배 메커니즘을 통해 동적 키 분배를 제공함으로써 사용자와 AP간의 안전한 암호통신을 제공한다.

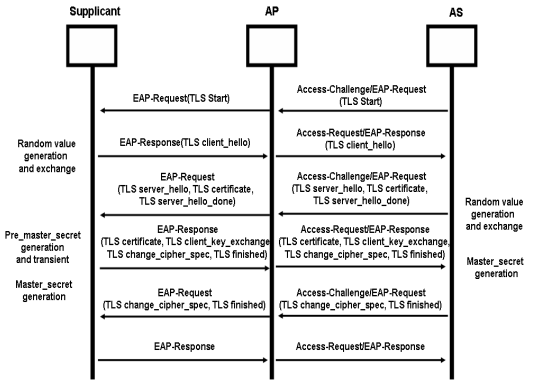

그림 6. Supplicant-AS 상호인증
Fig. 6 Supplicant-AS Mutual Authentication

3.2. 구현

본 논문에서 제안한 인증 메커니즘을 지원하는 시스템은 그림 7과 같이 클라이언트, AP, 인증서버 및 CA(Certificate Authority)로 구성된다.

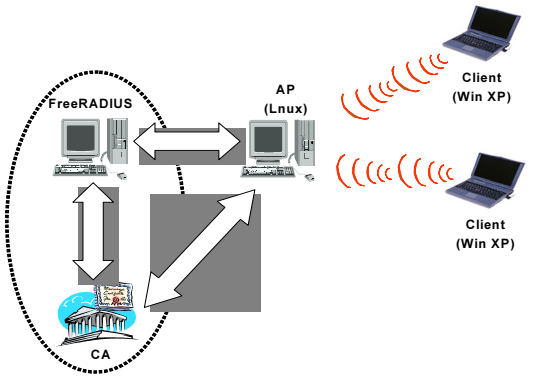

그림 7. 시스템 구성도
Fig. 7 Structure of proposal system

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 할 수 있도록 한다. CA는 클라이언트와 AP, 인증서버에 필요한 인증서를 발행한다.

시스템 개발 환경은 표 2와 같이 클라이언트는 WIRE1x v1.0[13] 오픈소스를 수정하여 구현하였으며, AP는 리눅스 운영체제가 설치된 PC에 Prism2 계열의 칩을 사용하는 무선랜 카드와 유선랜 카드를 동시에 장착하고 HostAP 드라이버를 설치하여 에뮬레이션 하였다. HostAP는 Prism2/2.5/3 계열의 MAC 칩을 사용하는 PCMCIA 무선랜 카드를 AP로 동작시키기 위한 리눅스용 Access Point 디바이스 드라이버이다.

인증서버는 공유키(WEP_Key)를 AP로 전달할 SUCCESS 메시지를 생성하고 암호화하기 위한 모듈과 인증 초기단계에서 클라이언트로부터 전송받은 값을 검증하는 모듈을 오픈소스로 공개된 FreeRADIUS[11-12, 15]에 추가하여 구현하였다. 모든 구성요소에서 암호 라이브러리 역시 오픈소스인 OpenSSL[14]을 사용하였다.

표 2. 구현 환경
Table. 2 Implementation environments

항 목	Client	AP	Authentication Server
OS	Windows XP	Linux	Linux
Language	C++	C/C++	C/C++
Secure Library	OpenSSL -0.9.7g	OpenSSL -0.9.7g	OpenSSL -0.9.7g
CA System	OpenSSL -0.9.7g	OpenSSL -0.9.7g	OpenSSL -0.9.7g
Open Source	WIRE1x	HostAP	FreeRADIUS

3.3. 시스템 평가

제안 시스템은 IEEE 802.1x의 취약성인 스푸핑 공격을 방지하기 위해 구성 개체 모두에 대한 상호인증을 수행하기 때문에 표 3에서 보는 바와 같이 클라이언트, AP, 인증서버로의 위장이 불가능한 매우 안전한 사용자 인증 메커니즘을 제공한다. 또한 EAP-SUCCESS 메시지를 암호화하여 무결성 서비스를 제공하고, 사용자 인증과정에서 키 분배 메커니즘을 통해 인증을 수행할 때마다 새로운 키가 분배되며, 분배되는 키의 길이가 전수조사 공격에 안전한 128 bit이기 때문에 안전한 암호통신을 제공한다. 그리고 인증 초기단계에서 사용자의 인증 요청을 인증서버가 제어할 수 있기 때문에 악의적인 사용

자의 무차별적인 접근요청에 의한 서비스 거부 공격을 방지할 수 있다.

표 3. 제안 메커니즘과 기존 메커니즘의 비교
Table. 3 Comparison of proposal mechanism and existing mechanism

항 목	IEEE 802.11b	IEEE802.1x	제안 시스템
AP 위장	매우 취약	취약	안전
인증서버위장	해당사항 없음	안전	안전
DoS 공격	취약	취약	인증서버에서 제어 가능
인증 메커니즘의 안전성	매우 취약	안전	안전
암호통신의 안전성	Static WEP Key	Dynamic WEP Key	Dynamic WEP Key
소요시간	적음	보통	많음

Ⅳ. 결 론 및 향후 과제

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 있으나 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 서비스 거부, 세션 하이재킹 및 중간자 공격에 대한 취약성을 보완하여 강화된 사용자 인증 및 안전한 암호통신 서비스를 제공할 수 있는 무선랜 보안시스템을 제안하였다. 제안 시스템은 보안 수준변수를 사용한 인증 초기단계를 인증 프로토콜에 추가하여 클라이언트의 인증 요청을 인증서버가 제어할 수 있도록 함으로써 악의적인 사용자의 무차별적인 접근에 의한 서비스 거부 공격을 방지할 수 있다. 그리고 클라이언트 및 AP, 인증서버 인증은 공개키 암호 기술 기반 인증 메커니즘을 통해 수행하기 때문에 제3자가 클라이언트 또는 AP, 인증서버 등으로 위장하여 통신에 개입하는 것이 불가능하다. 또한 키 분배 메커니즘을 지원하는 EAP-TLS 인증을 통해 전송 데이터의 암호화에 사용되는 키를 동적으로 분배함으로써 사용자와 AP 간의 안전한 암호통신을 제공한다.

향후 기존 인증 프로토콜에서 패킷 잃어버림 등이 발생할 때 올바른 패킷이 전송되도록 하기 위해 보장된 재전송을 이용한 서비스 거부 공격 에 대한 대응방안을 연구할 예정이다.

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

[3] 송창렬, 정병호, 조기환, "무선랜 보안구조," 한국정보과학회지, 제 20권 4호, pp. 5-13, 2002

[4] 양형규, "무선 PKI 환경에서 보안 모듈에 관한 고찰", 강남대학교 산학기술연구소 논문집, 제 14호, pp. 123-140, 2002.

[5] 강유성, 오경희, 정병호, "무선랜 보안기술의 진화 동향 및 전망", 전자통신동향분석, 제 18권 제4호, pp. 36-46, 2003.

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

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

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

[9] P. Funk, S. Blake-Wilson, *EAP Tunneled TLS*

Authentication Protocol (EAP-TTLS), IETF PPPEXT Working Group, 2005.
[10] L. Blunk, J. Vollbrecht, *PPP Extensible Authentication Protocol(EAP),* IETF Network Working Group, 1998.
[11] Joshua Hill, "An Analysis of the RADIUS Authentication Protocol", *Joshua Hill,* pp. 1-12, 2001.
[12] Joseph Davies, *RADIUS Protocol Security and Best Practices,* Microsoft Corporation, 2002.
[13] WIRE1x, "Open Source Implementation of IEEE 802.1X", http://wire.cs.nthu.edu.tw/wire1x
[14] OpenSSL Project, Open Source implementing the Secure Sockets Layer(SSL v2/v3) and Transport Layer Security(TLS v1), ttp:/www.openssl.org/
[15] FreeRADIUS Project, Open Source Implementation of RADIUS, http://www.freeradius.org/

저자소개

홍성표(Seong-Pyong Hong)

2001년 조선대학교 컴퓨터공학과(공학석사)
2005년 조선대학교 컴퓨터공학과(공학박사)
2012년~현재: 조선대학교 산학협력단 BK21 연구교수
※관심분야 : 시스템 보안, 운영체제, 무선랜 보안

한승조(Seung-Jo Han)

1980년 조선대학교 전자공학과 (학사)
1982년 조선대학교 전자공학과 (공학석사)
1994년 충북대학교 전자계산학과 (공학박사)
1986년 6월 ~ 1987년 3월: 뉴올리언즈대학 객원교수
1995년 2월 ~ 1996년 1월: 택사스대학 객원교수
2000년 12월 ~ 2002년 3월: 버클리대학 객원교수
1998년 3월 ~ 현재: 조선대학교 정보통신공학과 교수
※관심분야 : 통신보안시스템설계, S/W 불법복제방지 시스템, ASIC 설계