한국정보전자통신기술학회논문지(jkiiect)'16-12, Vol.9 No.6
논문 16-09-06-599 http://dx.doi.org/10.17661/jkiiect.2016.9.6.599

WEB 기반의 기업용 RADIUS 무선랜 보안 시스템 개발

정연우*, 손종윤**, 전중창***, 최경선****

Development of a RADIUS WLAN Security System for Industrial Applications Based on WEB

Yeon-Woo Jeong*, Jong-Yoon Sohn**, Joong-Chang Chun***, Kyung-Sun Choi****

요약 : 최근 네트워크 환경이 모바일 사용자의 증가와 기술적 성능향상으로 유선랜에서 무선랜으로 급격하게 교체되고 있다. 그러나 무선랜은 사용의 편리성만큼 의도하지 않은 자료유출과 같은 보안 취약성의 위협에 노출된다. 따라서 내부 사용자에게는 편리성을 극대화하며 해커로부터는 위협을 회피할 수 있는 안전한 무선랜 보안시스템 개발이 요구된다. 본 연구에서는 모든 무선랜 제조사의 제품과 호환이 가능하고 EAP 인증을 수행할 수 있는 기업용 RADIUS 무선랜 보안시스템을 개발하였다. 본 시스템은 웹기반의 인터페이스를 바탕으로 하고 있으며, 사용자 관리를 위한 DB 접속 기능을 제공함으로써 사용자의 PC에서 802.1x 인증접속을 수행할 수 있도록 하였다.

Abstract Recently the wireless LAN system is substituting wired LAN system notably as the number of mobile users increases greatly along the advancement of technology. But the wireless LAN has a critical weakness in the security such as data leakage. Thus a safe security system is imperative to avoid threatening from hackers with offering the best convenience to inner users. In this research, we have developed a RADIUS wireless LAN security system for industrial applications, which performs the EAP authentication with the compatibility for any maker of wireless LAN. The system has interfaces based on WEB, providing DB access function for user management so that users can perform authentication of 802.1x in their computers.

Key Words : Authentication, EAP, MAC+ID, RADIUS, SIP-VoIP, WLAN security

1. 서론

국내 IT 환경에서 스마트 기기의 등장과 함께 컴퓨터 판매량의 50% 이상이 무선랜을 탑재한 노트북이 차지하고 있다. 이에 부응하여 기업 네트워크 접속환경도 유선랜에서 무선랜으로 급격히 교체되고 있다. 기업, 학교 등에서 무선랜 설치가 필수적으로 되었고 신축건물에는 기본적으로 무선랜을 고려하여 설계되고 있다. 이런 환경변화는 모바일 사용자의 증가와 편리한 네트워크 접속성에 기인하고 있으며, 아울러 무선랜은 무선구간의 보안 취약성과 인증서버의 문제점 등으로 인한 해킹 및 자료 유출 등의 위협을 안고 있다. 따라서 내부 사용자에게는 편리성을 극대화하면서 동시에 해커로부터는 위협을 피할 수 있는 안전한 무선랜 환경을 구축이 요구된다.[1]-[2]

인증(Authentication) 처리를 위한 대표적인 프로토콜인 RADIUS(Remote Authentication Dial In User Service)는 특정 AP(Access Point) 또는 Gateway를 통해 접속해 온 사용자를 인증하고 사

*IM-Soft Co.
**Department of Physics, Gyeongsang National University
***Corresponding Author : Department of Electronic Engineering, Gyeongnam National University of Science and Technology(jcchun@gntech.ac.kr)
****Gyeongnam Technopark
Received December 03, 2016 Revised December 13, 2016 Accepted December 19, 2016

용자가 요청한 시스템이나 서비스 사용에 대한 접근 권한을 부여하는 목적으로 사용되는 프로토콜이다. RADIUS 시스템의 적용 사례로서, RADIUS 서버는 DHCP 서버와 연동하여 GPRS망의 ISP 인증 및 IP 할당에 사용된 연구 결과가[3] 발표되었으며, RADIUS 서버의 한계를 극복하고 확장성과 신뢰성을 제고하기 위해 DIAMETER를 사용한 IAPP(Inter Access Point Protocol) 서버가 개발되었다.[4] 또한 IEEE 표준 802.1aa와 802.11i를 지원하는 RADIUS 프로토콜을 사용하여 WEP(Wired Equivalent Privacy) 키를 교환할 수 있는 RADIUS 클라이언트가 구현된 바 있다.[5] 그리고 무선 구간 모니터링 에이전트를 통하여 실시간 모니터링을 수행함으로써, 현재 활성화 되어 있는 액세스 포인트들의 상태 정보와 Rogue AP를 탐지하고 RADIUS 인증 서버를 이용하여 Rogue AP의 네트워크 사용을 차단하는 시스템이 제안되었다.[6] 최근에는 하드웨어 보안기능을 이용하여 RADIUS 프로토콜과 TPM(Trusted Platform Module)칩을 통합한 하드웨어 기반 네트워크 인증 서비스 설계 사례가 발표되었다.[7]-[8]

본 연구에서는 기업 무선 네트워크를 위한 RADIUS 무선랜 보안 시스템을 개발하였으며, 포트 기반의 접근제어가 가능한 IEEE 802.1x를 사용하여 클라이언트와 서버 간에 암호화된 인증정보를 인터넷망을 통하여 공유함으로써 보다 강화된 인증기법을 구현하였다. 그리고 모든 인증정보가 클라이언트와 서버 간에서 생성되게 하여 타 기관의 인증관련 시스템과 연계되지 않도록 함으로써 독자적이고 보안성이 더욱 강화되도록 하였다. 또한 본 연구에서 개발된 시스템은 별도의 인증 처리용 하드웨어를 구비하지 않고도 소프트웨어만으로 인증 처리가 이루어지므로 저가의 시스템 구축이 가능하다.

2. RADIUS 인증 시스템의 설계

본 연구에서는 국제표준의 IEEE 802.1x 인증을 사용한 사용자 접근제어 및 무선 데이터 암호화를 수행하는 무선랜 보안시스템을 설계하였으며, 그림 1과 같이, RADIUS 인증모듈, 사용자 DB, 웹 기반 관리화면 그리고 DHCP 서버로 구성된다. 사용자는 무선랜으로 EAP 인증을 보내고, 무선랜은 이 사용자 인증정보를 RADIUS 프로토콜로 무선랜 보안 시스템으로 전송한다. 무선랜 보안 시스템은 사용자의 정보를 통해 사용자의 접근허가를 결정하며, 무선 구간의 암호화를 수행하는 Master 키 값을 사용자 PC로 내리는 역할을 한다. 무선랜 보안 시스템은 IEEE 802.1x EAP 인증수행을 표준에 맞게 수행해야 하고, IEEE 802.11i의 표준에 따라 무선구간의 암호화를 할 수 있는 킷값 생성 및 RADIUS 표준을 모두 만족해야만 한다.

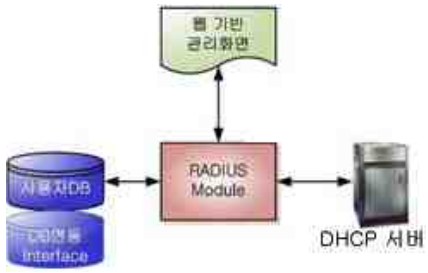

그림 1. RADIUS 무선랜 보안 시스템의 구성도
Fig. 1 System configuration of RADIUS WLAN

설계된 시스템은 Davin-Air Throne Linux BSP(Board Support Package)에서 구현되었으며, 개발에 필요한 호스트는 GCC(GNU Compiler Collection) 4.1 이하의 버전과 10GB 이상의 HDD 용량이 필요하다.

그림 2는 Wi-Fi Alliance에서 제시하는 무선구간암호화 내용이며, 기본적으로 암호화 기능은 무선랜에서 수행하며, 암호화를 위한 키값도 무선랜에서 관리가 가능하게 설계되어 있으나, Dynamic WEP 방식에서부터 가장 최신의 암호화 방식인 WPv2 AES 방식의 사용을 위한 표준은 인증서버에서 키값을 부여받도록 설계되어 있다. 802.1x 및 AES 암호화 기법을 사용하여 Tgi를 완벽하게 구현할 수 있을 때까지 가장 안전한 랜보안 방법은 VPN 게이트웨이를 통해 통신하도록 하는 것이다.

즉 기업방화벽 외부에 엑세스 포인트를 설치하고, 사용자가 원격 사용자인 것처럼 VPN 게이트웨이를 통해 통신하도록 하는 것이다.

항목	Static WEP Key	Dynamic WEP Key	WPA v1	WPA v2
보안키 적용 방식	WEP(24Bit IV)	WEP(24Bit IV)	TKIP(48Bit IV)	CCMP
암호화 알고리즘	RC4	RC4	RC4	AES
암호 비트	40/128bit	128bit	128bit	128bit
보안 레벨	하(매우 취약)	중/상	상	최상

그림 2. Wi-Fi Alliance 무선구간 암호화 기준
Fig. 2 Secret code standard in Wi-Fi Alliance

2.1 RADIUS 인증모듈

RADIUS 모듈은 EAP 인증 처리 및 EAP 인증 처리 후에 키를 전송하고 표준 RADIUS 프로토콜을 수행하며, SIP-VoIP 인증, MAC+ID 조합 인증 및 공인인증서와의 연동 기능을 수행한다. Linux 운영체제(OS)에서 구현된 주요 암호화 알고리듬 및 동작 내용은 다음과 같다:

- RADIUS RFC 865, 2866, 2868, 2869
- IEEE802.1x EAP-MD5/TLS/TTLS/PEAP/SIM
- IEEE802.11i Dynamic WEP/WPAv1/WPAv2
- EAP-TLS기반 인증
- 인증 Demon 감시 Process

2.2 사용자 DB 및 인터페이스

사용자 DB는 MySQL 기반으로 생성된 DB 테이블을 포함하고, DB 연동 인터페이스를 통해 외부 DB와 연동된다. 그리고 이중화를 위해서 자체 DB 응답 모듈을 포함하고, 사용자 관리를 위하여 사용자 정보를 입출력한다.

2.3 웹 기반 관리화면

웹 기반 관리화면은 사용자의 접속위치, 사용량, 날짜 및 시간 등과 인증서버의 상태를 그래픽으로 표시함으로써 사용자 중심의 시각화를 제공한다. 이 관리화면은 JSP를 이용하여 구현되었으며, 웹 기반 GUI를 통하여 각종 통계 프로세스 조회 및 시스템 설정 기능을 제공한다.

2.4 DHCP 서버

DHCP(Dynamic Host Configuration Protocol) 서버는 클라이언트의 요청이 있을 때 자동적으로 IP 정보를 할당해주는 기능을 한다.

3. PC 에이전트 설계

그림 3은 PC에이전트의 구성도를 나타내며, 802.11i 모듈, 802.1x 모듈, 무선랜 핸들러 및 프로파일 생성모듈로 구성된다.

PC에이전트는 윈도우즈 운영체제의 사용 환경을 지원하고, 무선랜 검색, 검색된 무선랜의 보안 내용의 분석, EAP 인증 수행 및 무선구간의 암호화를 수행하여 무선 인증 접속을 수행한다.

- 사용환경: Win2K/XP/Vista/7/Win Mobile OS
- EAP 인증: EAP-MD5/TLS/TTLS/PEAP
- IEEE802.11i 데이터 암호화
- 무선 구간 암호화: WAPv2

그림 3. PC 에이전트의 구성도
Fig. 3 Configuration of PC agent

4. 인증 프로세스 설계

무선랜 인증 시스템의 인증 프로세스를 그림 4에 보였으며, RADIUS 무선랜 보안 시스템의 인증 절차는 다음과 같다.

● 단계 1: 먼저 인증 요청자(Supplicant, PC)가 무선으로 접속한다(S1).

● 단계 2: 인증자(Authenticator, 무선랜)는 인증 요청자에게 802.1x EAP 인증을 요청한다(S2).

● 단계 3: 인증자의 요청에 따라 인증요청자가 인증서 또는 계정을 입력한다(S3).

● 단계 4: 인증자는 인증요청자의 정보를 인증서버로 전송한다(S4).

● 단계 5: 인증서버는 수신된 인증서 또는 계정에 따라 허가된 인증자의 경우에 인증자에게 포트를 오픈명령 및 무선데이터 암호화 키를 전송한다(S5).

● 단계 6: 인증자는 네트워크 연결 및 무선데이터 암호화 키를 인증요청자에게 전송한다(S6).

따라서 802.1x EAP 인증을 사용하여 인증 절차가 끝난 후에 인증요청자와 인증자는 인증서버에서 할당받은 무선데이터 암호화 키 값으로써 암호화할 실제 키 값을 재생성하여 암호화를 수행한다.

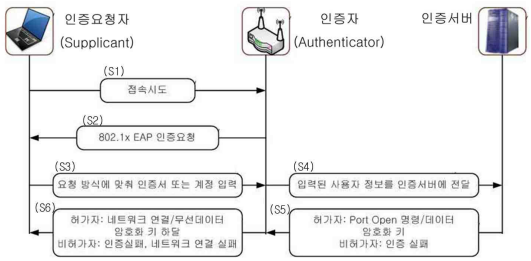

그림 4. 보안 시스템의 인증 프로세스
Fig. 4 Authentication process of security system

5. 결론

본 연구에서는 기업 무선 네트워크를 위한 웹 기반의 RADIUS 무선랜 보안 시스템을 개발하였다. 인증정보는 클라이언트와 서버 간에서 생성되도록 설계하여 타 기관의 인증관련 시스템과 연계되지 않도록 하였으며, IEEE 802.1x를 사용하여 클라이언트와 서버 간에 암호화된 인증정보를 인터넷망을 통하여 공유함으로써 보다 강화된 인증기법을 구현하였다. 그리고 본 연구에서 개발된 시스템은 별도의 인증 처리용 하드웨어를 구비하지 않고 소프트웨어만으로 인증 처리가 이루어지므로 저가의 시스템 구축이 가능하다. 국내 무선랜 보안 솔루션 시장은 매년 10% 이상 성장하고 있는 반면에 70~80%가 수입품임을 고려하면, 본 연구의 결과는 수입 제품의 독점적 점유를 방지하고 기업체 고유의 독자적 보안 시스템 구축에 기여할 것으로 예상된다.

REFERENCES

[1] J.W. Lim, J.D. Jang, C.P. Yoon, H.B. Ryu, “Mobile Malicious AP Detection and Cut-off Mechanism based in Authentication Network”, *Journal of Information and Security*, Vol. 12, No. 1, pp 55-61, 2012.

[2] S.K. Hwang, S.J. Han, “A Study on efficient transmission performance improvement Considering the security in the wireless LAN environment”, *Journal of The Korea Institute of Information and Communication Engineering,* Vol. 17, No. 4, pp. 837-846, 2013.

[3] J.H. Park, Y.J. Kim, Y.J. Lee, J.M. Yang, “PPP CHAP Modification for Wireless Internet Access of Remote Mobile Subscriber on GPRS Network”, *The KIPS transactions*, Part C, Vol. 9C No. 4, pp. 551-562, 2002.

[4] Y.H. Ham, B.H. Chung, K. Chung, “A Study on DIAMETER IAPP Server Supporting Wireless LAN Terminal Handoff”, *The Journal of Korea Information and Communications Society*, Vol. 28, No. 12C , pp. 1258-1267, 2003.

[5] Y.H. Ham, B.H. Chung, K. Chung, “The Implementation of RADIUS Client for 802.1aa Authentication and 802.11i Key Exchange”, *Proceedings of The 30th*

KISS Spring Conference, pp. 371-373, 2003.

[6] D.P. Kim, C.B. Kang, S.W. Kim, "Rogue AP Protection System Based on Radius *Authentication Server*", *Proceedings of The 31th KISS Spring Conference*, pp. 316-318, 2004.

[7] Y.M. Kim, S.Y. Lim, M.C. Kang, J.B. Lee, J.H. Lim, E.Y. Ban, J.I. Han, "Design of Multi-Authentication Server for user authentication in SaaS platform", *Proceedings of The 35th KISS Spring Conference*, pp. 897-900, 2011.

[8] R.N. Akram, K. Markantonakis, K. Mayers, "Trusted Platform Module for Smart Cards", New Technologies, Mobility and Security, *Proceedings of 6th International Conference,* pp. 1-5, 2014.

저자약력

정 연 우(Yeon-Woo Jeong) [정회원]

- 1986년 2월: 경상대학교 경영학과 (경영학사)
- 1995년 3월: 벽산정보산업
- 1999년 5월: S&T중공업(주)
- 2006년 4월: 아이엠소프트(주)

<관심분야>

스마트공장 시스템, IoT, EMS, MES, ERP, SCM

손 종 윤(Jong-Yoon Sohn) [정회원]

- 1989년 2월: 경남대학교 물리학과 (이학사)
- 1993년 8월: 경남대학교 물리학과 (이학석사)
- 2001년 2월: 경남대학교 물리학과 (이학박사)
- 2002년 9월 ~ 2005년 9월 : 동의대학교 기초과학연구소 연구원(광학담당)
- 2006년 3월 ~ 현재: 경상대학교 물리학과 시간강사
- ㈜동서기전, ㈜플러스빅, 로보테크 연구소장 역임

<관심분야>

신호처리 및 시스템, 무선통신, 마이크로파 및 전파전파, 컴퓨터 시뮬레이션, 제어 시스템 설계

전 중 창(Joong-Chang Chun) [종신회원]

- 1983년 2월 : 경북대학교 전자공학과 (공학사)
- 1991년 2월 : 포항공과대학교 전자전기공학과 (공학석사)
- 1995년 2월 : 포항공과대학교 전자전기공학과 (공학박사)
- 2003년 2월~현재 : 경남과학기술대학교 전자공학과 교수

<관심분야>

안테나 및 전자장 이론, 이미지 처리, 무선 네트워크

최 경 선(Kyung-Sun Choi) [정회원]

- 1988년 2월: 영남대학교 전기공학과 (공학사)
- 1990년 2월: 경북대학교 공대 전기공학과 (공학석사)
- 1998년 2월: 영남대학교 전기공학과 (공학박사)
- 1990년 3월~1998년 12월: 한국전기연구원, 선임연구원
- 1999년 3월~2002년 9월: 창신대학 정보통신과, 교수
- 2002년 10월~현재: 경남테크노파크, 신재생에너지팀장

<관심분야>

스마트공장구축, 최적제어, 스마트홈 시스템, 스마트 그리드