The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 20, No. 3, pp.195-200, Jun. 30, 2020. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2020.20.3.195
JIIBC 2020-3-27

보안강화를 위한 무선 네트워크 관리 방안에 관한 연구

A Study on Wireless Network Management for Security Enhancement

이은섭*, 김영곤**

Eun-Sub Lee*, Young-Kon Kim**

요 약 무선랜은 사용의 편리함으로 인해 점차 많은 분야에 걸쳐 활용되고 있다. 무선랜의 가장 큰 장점은 무엇보다도 이동성에 있다고 할 수 있다. 국내 유선 인터넷 서비스는 '06년을 기점으로 포화상태에 있지만, 무선 인터넷 사용자는 꾸준한 증가세를 보이고 있다. 하지만 무선랜은 많은 장점과 동시에 무선 서비스의 특성 상 존재하게 되는 다수의 보안 취약점을 가지고 있으며, 이런 문제점을 해결하기 위해 다양한 보안관련 기술이 개발 및 적용되고 있다. 하지만 그에 반해 무선랜 사용자의 보안인식은 여전히 부족한 상태로, 매년 개인정보유출 등의 보안사고가 반복적으로 발생하고 있는 상황이다. 무선랜에서 발생할 수 있는 주요 취약점을 연구하고, 그에 대한 관리차원에서의 보안대책을 제시하고자 한다.

Abstract Wireless LANs are being used in many fields due to their ease of use. The biggest advantage of the WLAN can be said above all mobility. Domestic wired internet service has been saturated since 2006, but wireless internet users have been steadily increasing. However, WLAN has many advantages and characteristics of wireless service. It has a number of security vulnerabilities, and various security related technologies have been developed and applied to solve these problems. On the other hand, security awareness of WLAN users is still insufficient, and security accidents such as personal information leakage occur repeatedly every year. We will study the main weaknesses that can occur in WLAN and suggest security measures from the management level.

Key Words : wireless, weakness, Access control, Privacy, security

Ⅰ. 서 론

취약한 무선랜을 안전하게 보호하기 위해서는 각 사이트의 서비스 환경에 맞는 무선랜 보안 정책의 수립이 필수적이며, 보안 정책에 맞는 무선 보안 기술을 적용하여야만 한다. 이러한 상황에서 안전한 무선랜 서비스를 위해 도입해야할 무선 보안 기술에 대한 연구가 꼭 필요한 시점이다.

무선랜의 보안 취약점이 발생하는 근본적인 원인을 파악하고, 무선랜의 취약점을 이용한 공격에 대한 대비책을 마련해야만 한다. 우선 무선랜 운영자와 사용자에게 현행기술을 이용해 보안성을 제고할 수 있는 관리 및 운영 방안을 제안하고자 한다. 현재까지 제안된 기술만으로도 무선 상에서 보안의 3대 요소라 할 수 있는 인증, 기

*정회원, 한국산업기술대학교 컴퓨터공학과
**정회원, 한국산업기술대학교 컴퓨터공학과(교신저자)
접수일자 2020년 5월 6일, 수정완료 2020년 5월 30일
게재확정일자 2020년 6월 5일

Received: 6 May, 2020 / Revised: 30 May, 2020 /
Accepted: 5 June, 2020
**Corresponding Author: ykkim@kpu.ac.kr
Dept. of Computer Engineering, Korea Polytechnic University, korea

밀성, 무결성을 보장할 수 있다. 먼저 이러한 무선 보안 기술에 대해 분석하며, 해당 기술의 적용 방법을 파악해 나가야 한다.

하지만 현재까지 무선은 공유 매체라는 한계로 인해 사용자 권한별 접근 제어 정책을 펼 수가 없었다. 각 조직체에는 다양한 권한을 가진 다수의 사용자가 네트워크에 접근하는데, 유선 상에서는 사용자의 위치가 고정되어 있어 권한별 접근 제어가 용이하였다. 그렇지만 무선에서는 각 사용자의 위치가 언제든지 바뀔수 있고, 이동함에 따라 기존 유선과 같은 접근 제어 정책을 적용하기는 힘들다.

이를 해결하기 위해 무선 상에서 적용할 수 있는 사용자 권한별 접근 제어 방법에 대한 연구가 필요하다.

결론적으로 안전한 무선사용을 위해 인증, 기밀성, 무결성을 보장할 수 있는 무선 보안 기술을 분석하여 적용할 수 있도록 하며, 여기에 무선 사용자의 권한에 맞게 접근 제어 정책을 펼 수 있는 기술을 추가하여 완벽한 무선 보안 환경을 구축할 수 있는 기술을 제시하고자 한다.

II. 무선 네트워크 취약점 분석

1. 무선 네트워크 물리적 취약점

유선 네트워크 환경의 네트워크 장비인 라우터와 허브가 일반 사용자가 접근하기 어려운 곳에 설치되고 보이지 않게 관리되는 것에 비하여, 무선 환경의 네트워크 장비인 AP는 외부에 설치되어 일반인에게 노출되어 있다.

이렇게 무선 네트워크 장비인 AP가 외부에 노출되어 있는 것은 AP와 단말기사이에 무선 전파의 원활한 송수신을 위해서 AP가 사용자와 근접한 곳에 설치되어야 하기 때문이다.[1]

그림 1은 무선 장비인 AP가 외부에 노출되어 발생하는 취약성들을 나타내고 있다. 외부에 설치된 AP에 비인가자의 물리적인 접근이 가능하게 되어, AP의 도난 및 파손, 구성설정 값의 초기화, 전원 차단, 전력선 절단, AP와 연결된 LAN 선 절단, 물리적인 설정 값 변경 등의 취약성에 노출된다.

AP 이외의 무선랜 장비인 인증서버와 유선 네트워크로 연결되는 라우터 등은 모두 전산실 등에 설치 운영하여, 비인가자의 접근을 차단하여야 함은 물론이고, Telnet이나 웹브라우저를 통한 장비 구성 정보를 변경하지 못하도록 구성 시에 반드시 암호를 설정하여 보호하여야 한다.

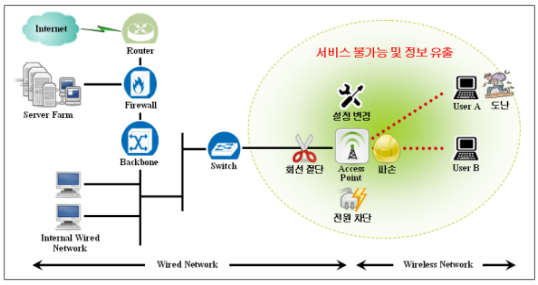

그림 1. 무선 네트워크 물리적 취약점
Fig. 1. Wireless Network Physical Vulnerabilities

2. 무선 네트워크 기술적 취약점

가. 무선랜 구성 정보 노출

제공을 위해서 대부분의 기관에서는 SSID를 기본적으로 브로드캐스트하고 있다. 이 경우, AP의 전파송수신 영역 안에 있는 모든 무선랜 단말기에서 SSID 값을 전송받을 수 있다. 즉, AP의 전파송수신 영역 안에 있는 모든 사용자는 자신이 현재 특정 무선랜 서비스를 사용할 수 있는 영역에 있고, 그 서비스를 제공하는 기관이 어디일 것이라는 것을 인식하게 된다.

무선랜 환경에서 접근제어를 위해서 MAC 주소 필터링을 적용하기도 한다. 즉, 무선 전파를 송수신하는 무선랜 카드에 부여된 MAC 주소 값을 이용하여 무선랜 서비스의 접속을 제한하는데 활용하는 것이다. 이러한 MAC 주소 필터링은 간단한 접근 제어 방식이면서 공격의 위험을 줄이는데 효과적이다. 또한, 네트워크 규모와 관계없이 적용될 수 있는 보안 메커니즘으로 무선랜 뿐만 아니라, 유선 네트워크에서도 많이 활용되는 방법이다. 하지만 MAC 주소 필터링은 공격자가 정상사용자의 MAC 주소를 도용함으로써 쉽게 무력화되고 있는 실정이다.

무선랜 분석 도구를 이용하여 공격자들은 필요한 정보를 수집한다. 무선랜 분석도구는 무선랜 서비스를 제공하는 AP의 전파를 수집하고 분석하여 AP가 사용하는 전파 채널 정보, 설정된 SSID 값, WEP 사용 여부 등의 정보를 제공하고, AP와 사용자 단말기간의 신호 또는 무선 데이터를 분석하여 무선랜 단말기의 MAC 주소 값, 무선랜이 이용하는 IP 대역, WEP를 적용한 무선 패킷이 사용하는 초기 벡터(Initial Vector) 값 등의 정보를 분석해 낼 수 있다. 뿐만 아니라, 무선 패킷을 수집할 수 있어, 수집된 패킷을 이용한 암호키 복구 및 MAC 주소 공격 등에 악용될 수 있다.

나. 무선랜 보안 프로토콜 취약성

무선 네트워크를 Open mode로 운영할 경우, 네트워크의 성능(전송률)은 가장 우수하다. 또한 관리자 입장에서는 구성이 용이하며, 사용자 입장에서는 사용하기가 편리하다. 하지만 무선 상에서 전송되는 데이터가 공격자에게 그대로 노출되기 때문에 공격자는 손쉽게 네트워크에 침입할 수 있으며, 침입 후 Packet Sniffing을 통해 사용자의 모든 데이터를 수집할 수 있게 된다.

IEEE 802.11b 표준에서 사용자 인증과 데이터 암호화를 위해 제정한 WEP는 다른 암호 프로토콜에 비해서 구현이 간단하고 사용도 편리하여, 무선랜에서 사용자 인증과 데이터 암호화를 위하여 많이 사용되고 있었다. 하지만, WEP는 RC4 암호 메커니즘을 적용하고 있고, 짧은 길이의 암호키를 사용하는 등 설계상의 오류로 인해 아래와 같은 보안 취약성을 갖고 있다. 뿐만 아니라,무선랜 운영시 WEP의 적용은 옵션 사항이다.

다. 유선 네트워크와의 연동 시 발생하는 취약점

네트워크를 운영하는 많은 곳에서는 유선 네트워크를 통해서 내부망에 접속하는 접점에 보안장비인 Firewall, IDS(Intrusion Detection System), 네트워크 모니터링 장비 등과 통합 보안 솔루션을 설치하여 해킹과 컴퓨터 바이러스 유입을 막고 있다. 하지만 무선랜을 위한 보안 솔루션을 거의 운영되고 있지 않고 있다. 무선랜을 사용하는 많은 곳에서는 AP를 내부망에 설치하여 운영하고 있고, 이때 AP의 전파가 외부까지 전송되는 경우가 많다. 이와 같이 AP 전파가 외부까지 전송될 경우, 이를 이용한 해킹과 바이러스 유입 등의 침해사고가 발생할 수 있다.

무선랜이 갖는 또 하나의 취약성으로는 비인가 AP의 설치 운영으로 인한 데이터 유출 가능성이다. 기관의 내부망에 설치된 비인가 AP를 통하여 공격자가 내부망을 공격하거나, 기관 외부망에 설치된 AP의 전파 출력을 높여 내부 사용자의 접속을 유도하여 주요 데이터를 모니터링하는 경우를 말한다.[3]

3. 무선 네트워크 관리적 취약점

무선랜을 운영하는 대부분의 기관에서는 사용하는 AP의 갯수 정도만 파악하고 있어 실제로 장비가 파손되거나 도난당하여 무선랜 서비스를 제공하지 못하고 있어도 이를 파악하지 못하는 경우가 발생할 수도 있다. 이를 방지하기 위해, 기관에서 사용하는 무선랜 장비인 AP와 무선랜 카드 등에 대한 장비 운영현황과 사용자 현황 등을 파악하여야 한다. 뿐만 아니라, 무선랜 장비에서 제공하는 기본값 혹은 초기값을 사용하고 있는 곳이 많아, 공격자의 표적이 되고 있다. 특히, 보안설정을 위해 사용하는 WEP 등도 장비에서 제공하는 초기값을 사용하고 있어 보안에 매우 취약한 것으로 드러나고 있다.

무선랜 운영 기관에서 마련한 보안정책에 보안기능을 사용하지 않는 사용자가 있으면, 전체 기관의 정보보호에 허점이 발생하기 마련이다. 사용자의 정보보호 무관심으로 인해 무선랜 단말기에 보안기능을 미설정하거나, 무선랜 정보보호를 위해 사용하기로 정한 보안기능을 사용하지 않는 경우가 많은데, 이렇게 무선랜 보안기능을 설정하지 않는 사용자는 공격자의 표적이 될 수 있다. 또한, 사용자들이 정보보호에 대한 인식 부족으로 기관에서 설정한 보안설정 값이나 암호키 값을 외부 방문객들에게 노출시키는 경우도 발생한다. 이러한 경우가 발생하면 보안 관리자가 설정해 놓은 정보보호에 관한 노력이 한순간에 무너질 수 있고, 이로 인해 외부인의 침해가 발생할 수 있다. 사용자의 부주의로 인한 비인가 AP의 설치 및 운영 등은 앞에서 설명한 것처럼 공격자가 내부망 침투를 위한 통로로 악용될 소지가 있으며 이로 인해 많은 피해가 발생할 수 있게 된다.

무선랜을 설치하여 운영하는 기관의 대부분은 유선 네트워크 관리자가 무선랜도 관리하는 경우가 많다. 이러한 경우에, 유선 네트워크 관리자가 무선랜에서 사용하는 전파 특성을 파악하지 못하는 경우가 많다. 즉, 전파 자원의 관리 미흡으로 인해 무선랜 환경에 취약성이 발생한다. 이러한 취약성에는 다음과 같은 것들이 있다.

우선, AP의 전파 출력 조정을 하지 않아 기고나 외부로 무선랜 전파가 유출되는 경우이다. 기관 외부로 전파가 도달되면, 기관외부에서 공격자에 의한 공격이 발생할 수 있다. 이러한 경우에는 반드시 기관 내부와 기관 외부에서 전파 출력을 측정하여, 적절한 무선랜 서비스 영역을 제공할 수 있도록 노력하여야 한다.

Ⅲ. 무선 네트워크 보안강화 방안

물리적 취약점, 기술적 취약점, 관리적 취약점을 보완하고 보안을 강화하기 위해 실시간 사용자 인증, 그룹별 보안정책 구성, 보안솔루션 설치 및 배포를 통한 보안강화 방안을 제시한다.

1. 실시간 사용자 인증

가. 인증프로세스

실시간 사용자를 위해 크게 두 가지로 클라이언트 PC(Supplicant), 액세스 포인트(Authenticator), RADIUS 서버(Authe- ntication server)를 통해 사용자 인증 프로세스를 제시한다.

클라이언트 PC는 망에 접근하려는 PC 등의 단말 사용자가 무선인 경우에는 무선 단말기를 말한다. 액세스 포인트는 클라이언트 PC와 RADIUS 서버 간의 통신을 돕는 경유 장치 역할을 한다. AP와 클라이언트는 EAP-OL(EAP Over LAN) 프로토콜을 사용하여802.1x 메시지를 교환해서 클라이언트 스테이션에서 송신한 메시지가 AP를 거치면서 암호화된 뒤 EAP 확장자를 달아 RADIUS 서버로 전송된다. 이 메시지는 대개 RADIUS 서버로부터 응답 EAP 패킷을 받는 즉시 EAPOL 형식으로 해석되어 클라이언트에게로 전송된다. 이제 클라이언트와 RADIUS 서버 사이에 의견 교환이 이루어진다. 인증 과정을 통과한 클라이언트는 자동키 배포 기능이 있는 EAP 유형인 경우에는 AP로부터 암호화키를 받는다. 인증된 클라이언트는 이후로 이 키를 사용하여 데이터를 암호화한다.[3]

나. 사용자 인증 내역

사용자 인증을 위해서는 802.1x EAP 기반 사용자 인증을 제시한다. EAP 사용자 인증 방식에는 인증서를 사용하거나 마이크로소프트 윈도 운영체제에서 지원하는 기술을 이용해 아이디/비밀번호로 인증을 처리할 수 있는 TLS(Transprot Layer security), TTLS(Tunneled Transport Layer Security), PEAP(Protected Extensible Authentication Protocol)이 있다. 모두 무선랜 장비에서 지원하고 있음에 따라 사용자 환경과 보안정책에 맞게 적절한 인증 방식을 선택할 수 있는 장점과 강력한 보안 능력을 갖추고 있다.[4]

2. 사용자 그룹별 보안 정책

가. 그룹별 보안정책 구성

사용자 그룹별로 인터넷 이용에 대한 접근권한을 제어함으로서 조직 내 무선 네트워크 보안성을 강화 할 수 있는 방안을 제시한다.

무선네트워크 환경에서 인증과 암호화를 함으로서 보안이 강화되는 효과가 있으나 무선네트워크를 이용하는 이용자들에 대한 권한이 동일하게 부여되면 접근성에 문제점이 대두됨에 따라 이용자 그룹별로 인터넷 이용에 대한 접근권한을 제어함으로서 다양한 학내 구성원, 계약직, 방문자, 시민 등 에게 보안측면과 운영상에 편리성을 가져올 수 있다. 그림 2는 그룹별 보안정책 구성도이다.

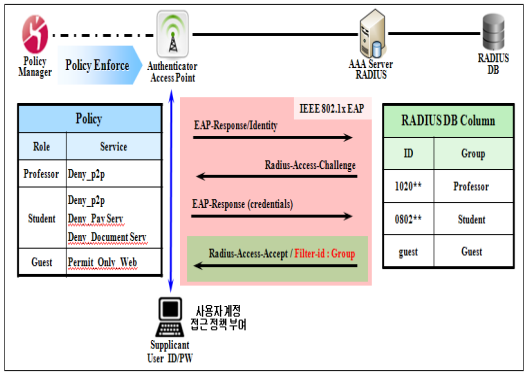

그림 2. 그룹별 보안정책 구성도
Fig. 2. Wireless Network Physical Vulnerabilities

나. 사용자 그룹별 보안정책 적용

◦ 조직내 구성원 그룹

조직내 구성원 그룹 조직에 따라 등급을 나누어 구성할 수 있으며, 일반적인 서비스는 모두 허용되고, P2P서비스에 대하여 정책을 상이하게 적용할 수 있다.

◦ 일반사용자 그룹

일반사용자 그룹은 조직내 구성원이 구성원에 준하여 업무를 처리하는 사용자들로서 조직내 아이디가 없는 사용자들로 구성됨에 따라 조직 내 데이터베이스, 전산시스템 등 서비스는 차단하고 일반적인 서비스만 허용되는 정책이 적용된다.

◦ 제한사용자 그룹

제한사용자 그룹은 아이디가 없고, 조직을 방문하는 외부인 또는 시민들에게 별도의 사용자등록 절차 없이 무선인터넷 서비스를 이용하고자하는 사용자들로서 기본적으로 모든 서비스는 차단되며 관리자가 허용해주는 서비스에 한하여 이용이 가능하다.

3. 사용자 접근 제어

강력한 보안 기능을 사용함으로서 일반 사용자가 무선네트워크에 접근하는 것이 어렵게 구성 방안을 제시 한다. 비 인증 사용자가 인터넷 사용을 시도하면 방화벽 정책에 의하여 차단이 되고, 자동적으로 매뉴얼 페이지(Manual Page)로 포워딩(Forwarding) 된다. 비인증 사

용자는 Manual Page에서 접속방법을 숙지하고, 필요에 따라 연결프로그램을 다운로드 받아 컴퓨터에 설치한 다음 재접속 하도록 유도 한다. 인증을 받지 않은 사용자가 인터넷을 시도 하였을 경우 사용자 PC는 무인증 IP 주소를 할당을 받아 외부 인터넷에 집근한다.

인증된 사용자는 CM(Connection Manager)을 이용하여 사용자의 편리성을 제공하며, 비인증 사용자가 인증요청을 하여 데이터베이스에 등록되어 있는 사용자로 확인이 되었을 경우 사용자 PC는 Radius서버에서 같이 운영되고 있는 DHCP서비스에서 IP주소를 할당을 받고 PMS(Patch Management System) Active_X 설치를 한 후 인터넷 서비스 이용이 가능하게 된다.[5]

4. 보안 솔루션 설치 및 배포

가. PMS 솔루션을 이용한 보안 패치 적용

PMS(Patch Management System) 솔루션을 이용하여 인증 받은 사용자가 인터넷 서비스를 이용 하려고 할 때 외부로 나가는 백본장비에서 모니터링을 하고 있다가 사용자의 PC에 PMS(Patch Management System) ActiveX가 설치되어 있지 않으면 특정 Page로 유도함으로서 반드시 ActiveX를 설치하게 한다. 결과적으로 백신 에이전트를 사용자들에게 배포하고, 에이전트에 의해 백신프로그램을 설치하게 된다. 또한 윈도우즈 업데이트를 다운 받을 수 있게 한다.[6]

나. APC 솔루션을 이용한 백신 설치

PMS(Patch Management System)를 통해 배포된 백신 에이전트가 사용자 PC에 설치가 되면 이 에이전트와 APC(Ahnlab Policy Center) Management 사이에 통신이 일어나 백신 프로그램인 V3 Security 프로그램이 설치가 된다. 설치된 백신 프로그램은 사용자 PC가 부팅 되면서 활성화 되어 실시간으로 인터넷 및 시스템을 감시하고 있다가 악성 바이러스나 스파이웨어가 감지되면 사용자에게 메시지를 보여주고 자동으로 치료를 하게 된다.

V. 결 론

무선랜은 이미 현대사회의 여러 분야에서 사용되고 있고, 이는 향상된 전송속도를 제공하는 새로운 무선 표준의 상용화와 더불어 더욱 다양한 분야에서 활용되어 유선랜의 상당부분을 대체할 것으로 예상되고 있다.

이에 따라 무선랜의 보안은 더욱 중요한 부분을 차지하게 될 것으로 예상되지만, 무선랜의 사용자나 관리자의 인식은 여전히 부족한 상태로, 여러 조사 자료나 반복되는 사고의 발생에서도 그러한 사실을 확인할 수 있다. 안전한 무선랜의 사용을 위해서는 무선랜의 구축에서부터 보안이 고려되어야 하며, 항상 새로운 취약점이 나오는 현실에 맞춰 꾸준히 보완되고 관리되어야 한다.

이에 따라, 본 논문에서는 안전한 무선랜 환경 구축을 위해서 무선랜 운영자가 무선랜 환경이 갖는 물리적, 논리적, 관리적 취약성을 점검하여, 무선랜 장비인 AP에 대한 비인가자의 접근 제한 등을 고려 무선랜 장비에서 제공하는 보안 기능을 활용하여, WEP 설정, MAC 주소 필터링, 무선 전파 출력 조절, 장비 초기값 사용 금지 등의 보안 정책을 제시하고 운영 지침을 제공하여, 무선랜을 통한 침해 사고의 가능성을 줄이고자 하였다.

또한, 사용자 인증의 강화와 무선 데이터의 암호화 설정을 통한 보안성 증대 필요성에 따라 무선랜 관리자 및 사용자의 보안 정책 수립 절차를 제시하여 기관에서 수립된 정보보호정책의 원활한 적용과 사용자의 참여의식 고취를 통해 개인정보의 유출 사고를 현저히 줄일수 있도록 하였다.

마지막으로 무선랜를 통한 침해사고가 발생할 경우에 효과적으로 대응하기 위한 대응 방안을 마련하고, 이와 관련된 정보교류 및 기술지원 등을 활성화하여 침해 사고의 피해를 줄이기 위한 방안을 마련해 두고자 하였다. 무선랜 운영 시 필요한 고려사항과 유의사항들을 모두 하나의 운영정책을 통해 일괄적인 기준을 가지고 관리하도록 하였으며, 무선랜의 보안정책, 취약점과 대응방안에 대해 다뤄, 사용자와 관리자의 무선랜 관리에 대한 방안을 제시하고자 하였다.

References

[1] Seung-Cheol Lim, “A Study on Improvement of Call Admission Control using Wireless Access Point Sharing”, The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 18, No. 4, pp. 91-96. 2018.
DOI: https://doi.org/10.7236/JIIBC.2018.18.4.91

[2] Ahmed Mateen, Qingsheng Zhu, Salman Afsar, Muhammad Usman, “IoT and Wireless Sensor Network Monitoring for Campus Security”, The Journal of The Institute of Internet, Broadcasting and Communication,

Vol. 18, No. 6, pp. 33-41, 2018.
DOI: https://doi.org/10.7236/JIIBC.2018.18.6.33

[3] Shin Hyo Kim, Seok Joon Lee, Hyeokchan Kwon, Fog Il, Jo Hyunsook, "Next-generation wireless LAN security technology trends", Journal of KIISE, 30(1C), 433-435.

[4] Young-Do Joo, "Analysis on Security Vulnerabilities of a Password-based User Authentication Scheme for Hierarchical Wireless Sensor Networks", The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 15, No. 4, pp. 63-70, 2015
DOI: http://dx.doi.org/10.7236/JIIBC.2015.15.4.63

[5] Yeon-Woo Jeong, Jong-Yoon Sohn, Joong-Chang Chun, Kyung-Sun Choi, "Development of a RADIUS WLAN Security System for Industrial Applications Based on WEB", Journal of Korea Institute of Information, Electronics, and Communication Technology, 9(6), pp. 599-603. 2016

[6] Ji-Hyun Nam, Ju-yeop Lee, Song-hui Kwon, Hyoung-Kee Choi, "Comparative Analysis on Security Protocols of WPA3 Standard for Secure Wireless LAN Environments", The Journal of Korean Institute of Communications and Information Science, 44(10), pp. 1878-1887. 2019

저 자 소 개

이 은 섭(준회원)

- 2003년 2월 : 한국산업기술대학교 컴퓨터공학과(공학사)
- 2017년 2월 : 한국산업기술대학교 컴퓨터공학과(공학석 사)
- 2020년 2월 : 한국산업기술대학교 컴퓨터공학과(공학박사)

- 관심분야 : 보안, 정보보호, DB, 네트워크, 서버

김 영 곤(정회원)

- 1983.2:경북대학교 전자공학과(공학사)
- 1985.2:연세대학교 본대학원 전자공학과(공학석사)
- 2000.2:한국과학기술원 전산학과(공학박사)
- 1985~2007:KT 수석연구원

- 2007 ~ : 한국산업기술대학교 컴퓨터공학과 교수
- 전문분야 : 소프트웨어공학, 정보통신시스템 통합, 보안