액세스 포인트의 디폴트 WEP키 변경 방법론

이기성*, 서희석**

요약

무선 랜(WLAN : Wireless Local Area Network)으로 인터넷을 사용하기 위해서 단말기는 무선 공유기(AP : Access Point)와 접속해야 하며 접속하기 위해서는 인증절차가 필요하다. 인증절차 중 네트워크 키(WEP Key : Wireless Encryption Protocol Key)를 이용하는 방법이 있지만, 대부분의 AP 소유자는 WEP키를 변경 하지 않고 인터넷에 공개되어 있는 기본 WEP키를 사용함으로써 허가받지 않는 사용자가 접속하여 개인정보 유출의 취약점이 있다.

본 논문에서는 WEP키를 자동적으로 변경하는 방법으로 AP기기를 하드웨어 설계하는 방법을 제안한다. 따라서 정부가 추진하고 있는 무선 랜 보안 대책의 일환으로 무선 랜 보안 의무 법 설정에 접목시켜 인터넷 대란과 개인정보 유출을 막을 수 있는 효과가 있다.

The Methodology of Access Point Default WEP Key an Alteration

Ki-Sung Lee*, Hee-Suk Seo**

ABSTRACT

Using mobile device to access WLAN that use a Access Point to use mobile device to access WLAN that use a Access Point WEP key and authentication procedures that are needed.

Most owners of the AccessPoint in the AccessPoint device proportioned to create a company by using the default WEP key since default key are know by unauthorized users, there is vulnerability outflow of personal information.

In this treatise, automatic WEP key generation, in new hardware design in proposed. This can prevent personal information leakage.

Key Words : Access Point, OTP, WLAN, WEP Key, Default Password, Mobile Authentication

* 한국기술교육대학교 인터넷미디어공학부(✉ lgomdori@kut.ac.kr)
** 한국기술교육대학교 컴퓨터공학부
· 제1저자(First Author) : 이기성 · 교신저자(Correspondent Author) : 서희석
· 접수일(2010년 5월 29일), 수정일(1차 : 2010년 6월 30일), 게재확정일(2010년 7월 7일)

Ⅰ. 서 론

오늘날 노트북, 넷북, 스마트폰과 같은 휴대하기 간편한 이동형 디바이스들의 증가로 무선 네트워크, 즉 WLAN이 활성화 되었으며 WLAN은 AP(Access Point)에 접속함으로서 인터넷을 이용할 수 있다.

AP기기에 접속하기 위해서 사용자 인증방법인 WEP 키를 이용하지만 대부분의 WEP 키는 AP기기를 만든 업체에서 기본적으로 지정해준 WEP 키를 이용한다. 이로 인하여 기본 WEP키는 한정적인 값으로 저장되어 있으며 인터넷에 공개되어 있는 WEP키를 이용하여 허가받지 않은 사용자가 AP 무단 접속을 할 수 있으며 악의적으로 접속한 해커가 패킷을 분석을 한다면 AP기기에 접속되어 있는 사용자들의 개인정보 유출 위험성이 있고, 인터넷 전화 (VoIP : Voice over Internet Protocol)의 AP기기에 접속을 한다면 전화 도감청의 위협이 있다.

이런 현상으로 기본 WEP 키를 제 3자가 알지 못하도록 WEP키를 변경하는 방법을 권고하고 있지만 대부분의 AP 소유자는 기기의 조작방법 미숙과 안일한 보안 의식으로 인하여 기본 WEP 키로 사용자 인증을 하고 있다.

본 논문에서는 AP의 보안 정책의 일환으로 기본 WEP 키 값을 OTP 사용한 하드웨어 설계 제안과 휴대폰 인증 방식을 이용한 하드웨어 설계 제안을 한다.

Ⅱ. 기존 연구의 배경기술

2.1 무선랜 구성방법

무선 랜은 AP가 있는 경우인 Infrastructure모드와 없는 경우인 Ad-Hoc모드로 구분된다[1].

Ad-Hoc 모드는 Node PC끼리 데이터를 취급할 때 적합하며 무선랜 카드에서 전송한 데이터를 상대방의 무선랜 카드로 직접 송수신이 가능하다.

따라서 무선랜 카드만 사용하면 데이터 취급은 물론 프린터나 주변기기를 공유하여 효율적으로 이용할 수 있다. 또한 각 PC의 네트워크 설정은 같게 해줌으로써 Peer-to-Peer 접속이 가능하다.

Infrastructure 모드는 AP 중계기를 이용하여 무선랜 카드와 데이터 통신을 하며 AP를 시야가 트인 곳에 설치하면 데이터를 송수신하는 PC 주변에 장애물이 있더라도 안정된 데이터 통신이 가능하다. 그 외에도 허브를 사용하여 유선 랜과 상호 접속이 가능하며 RG(Residential Gateway)를 사용하면 인터넷 접속이 가능하고 여러 대의 AP를 일정한 간격으로 설치하면 이동 중에도 네트워크 접속이 가능하여 로밍기능을 이용할 수 있다.

2.2 AP기기 보안 이슈

2009년 12월 한국인터넷 진흥원의 조사에 따르면 무선 인터넷 이용자는 54.9%로 전년도 대비 2.4%로 증가 하였고 서비스 별로 무선 랜 사용자는 9.2%로 전년 대비 1.5% 증가했으며 인터넷 전화 사용자 또한 증가하여 사설 AP의 수요가 증가하고 있으며 이로 인한 보안이슈도 나타났다[2]. 현재 인터넷의 공개되어 있는 사설 AP의 기본 WEP키는 <표 1>과 같다.

표 1. 사설 AP 기기의 기본 암호
Table 1. Default password of private AP device

사설 AP 기기	기본 암호
A사	SHOW3382
B사	2127393302
C사	16005252
D사	a123456789
E사	1234567890
F사	987654321b
G사	123456789
H사	534f4b4354
I사	123456789a
J사	1234

대부분의 사설AP 소유자는 WEP키를 기본으로 설정을 하기 때문에 인터넷에 공개가 되어있는 WEP키를 이용하여 무단으로 접속하는 사례가 많다. 이로 인해 기본 설정으로 되어있는 AP에 쉽게 접속하여 악의적인 해커가 패킷 스니핑 후 AP기기에 접속되어 있는 사용자들의 개인정보 유출을 하여 보안 사고의 우려가 있으며 해킹 사고 발생 시 해커를 찾기 어렵다.

2.3 무선 랜 취약점

Hacker's Challenge라는 책을 보면 2002년에 발생한 보안 사건들을 주로 다루고 있는데 20가지 에피소드 중 세 가지가 무선 랜 보안과 연관된 것이었다. 이러한 무선 랜 관련 이슈는 우리나라에도 점점 적용되어 가는 상황이다. 이 책에서 나온 세 가지 에피소드의 예를 살펴보면 다음과 같다[3].

- The Parking Lot

방화벽 등으로 AP를 분리하지 않았을 경우 무선 랜을 경유한 내부 망 침투가 이뤄지게 된다. 이 경우 침입자는 대상이 되는 건물 근처의 주차장에 차를 세워두고 노트북과 무선 랜 카드를 이용하여 네트워크에 침투했다면 해킹 사고가 발생한다면 침입자를 추적하기는 힘들다.

- Up in the Air

WEP이 실제로 크래킹이 되고, MAC 필터링도 MAC 주소 조작을 통해 깨질 수 있음을 보여준다. 그리고 이러한 크래킹과 조작에 필요한 기술들은 아주 높은 스킬을 필요로 하지 않는다.

- Accidental Tourist

우리나라에 현재 무선 랜을 통해 인터넷 액세스를 제공하는 카페나 패스트푸드점에서 인터넷을 사용하던 사용자가 우연히 같은 설정을 가진 같은 건물의 위층 사무실 네트워크에 접속하게 된 사건이다. 이 경우 사용자는 악의를 지니지 않아서 별다른 피해를 입히지 않았지만 이러한 종류의 문제조차도 원인을 발견하고 해결하는 데는 많이 시간이 필요한 작업이다.

2.4 무선 랜의 보안 프로토콜

- WEP(Wired Equivalent Privacy)

WEP는 무선 LAN 표준을 정의하는 IEEE 802.11 규약의 일부분으로 무선 LAN 운용간의 보안을 위해 사용되는 기술로서 무선 LAN에 연결된 어댑터와 AP가 서로 주고받는 데이터를 64(40+24)비트 혹은 128(104+24)비트로 암호화 하였지만 취약점이 발견 되어 전송 데이터에 대한 공격 툴들이 인터넷에 공개되었다[4].

- WPA Personal(WPA-PSK)

기존의 WEP 보다 한층 보안이 강화된 무선 랜을 구성할 수 있는 방법으로 사용자 별, 네트워크 세션 별, 전송되는 프레임 별로 키를 달리하는 TKIP(Temporal Key Intergrity Protocol) 암호 알고리즘과 AES(Advanced Encryption Standard) 암호 알고리즘을 채택하여 외부의 공격자가 네트워크 도청을 수행하여 수집한 데이터를 기초로 WEP 키를 추출하는 공격에 대한 저항력을 가지도록 하였다.

- WPA Enterprise(WPA-EAP)방식

WPA-EAP로 불리는 WPA Enterprise 방식은 인증/암호화를 강화하기 위해서 다양한 보안 표준 및 알고리즘을 채택하였는데, 가장 중요하며 핵심이 되는 사항은 유선 랜 환경에서 포트 기반 인증 표준으로 사용되는 IEEE 802.1X 표준과 이와 함께 다양한 인증 메커니즘을 수용할 수 있도록 IETF의 EAP 인증 프로토콜을 채택했으며 기업에서 별도의 인증 서버인 RADIS(Remote Authentication Dial-In User Service)가 구축되어야 한다.

2.5 OTP 암호 방식

- 시간 동기화 방식

시간 동기화(Time Synchronous) 방식은 시간을 일회용 비밀번호의 입력 값으로 사용하며 PIN(사용자 비밀번호, 비밀키)과 함께 인증 서버에 전달하면, 서버는 PIN을 인덱스로 하여 해당 비밀키를 찾고, 생성된 일회용 패스워드가 수신한 것과 일치하는 지를 확인한다. 또한 인증 서버와 사용자 모두 같은 시간을 일회용 비밀번호의 입력 값으로 넣어야 하기 때문에 인증 서버와 사용자 토큰 사이에 시간이 일치하지 않으면 사용자 인증에 실패할 수밖에 없다.

- 이벤트 동기화 방식

이벤트 동기화 방식은 시간 정보 대신에 인증서버와 인증 횟수(Counter) 기록을 공유하고 인증 횟수를 일회용 패스워드 생성 시 입력 값으로 활용하며 카운터를 인증 서버와 OTP 토큰 사이에 일치시켜야 정상적으로 인증이 수행된다[5].

III. OTP 인증방식 설계

본 논문의 서두 중 사설 AP의 경우 개인 소유물이기 때문에 기본 WEP 키를 필수적으로 변경할 의무가 없어 현재는 권고사항이라고 언급하였다. 기본 WEP 키를 변경하지 않으면 무단 사용자로 인하여 AP 소유자의 인터넷 속도 저하와 악의적으로 AP에 접근하여 개인 정보를 유출시킬 우려가 있으므로 본 논문에서는 기본 WEP 키를 자동적으로 변경할 수 있는 AP기기의 하드웨어 시스템을 제안한다.

3.1 하드웨어 설계

(그림 1)은 본 논문에서 제안하고자 하는 사설 AP기기의 하드웨어 구조도이며 기존 AP에서 OTP 생성모듈과 액정디스플레이를 추가한다.

기존 AP의 모듈 중 DRAM은 스토링 테이블과 코드 등 애플리케이션을 실행하는데 필요한 메모리를 지원하며, CPU는 ISA 버스를 통해 PCMCIA 인터페이스와 LAN 조절기를 연동시키고 임베디드 운영체제 구동을 총괄한다. 리모트 스위치는 AP관리 소프트웨어와 하드웨어 측면에서 시스템 포맷과 같은 정비와 수정 기능을 한다. 100-BASE-TX 제어 프로세서는 UTP 케이블과 연결해 LAN 조절기 파라미터 저항 등의 역할을 한다[6].

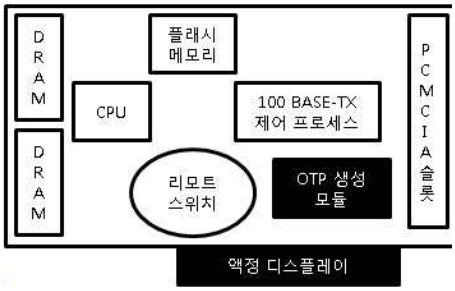

그림 1. 제안하는 AP의 구조
Fig 1. Structure of AP

본 논문에서 제안하는 모듈 중 OTP 생성 모듈은 이벤트 동기화 방식으로 WEP 키를 생성하며 액정 디스플레이에는 AP 소유자에게 WEP 키를 보여주는 장치로써 항상 디스플레이가 되고 AP 기기의 전원이 리셋되면 최초 AP에 접속되는 단말기의 MAC(Media Access Control) 주소와 인증횟수를 이용하여 새로운 WEP 키가 자동적으로 생성이 되어 액정 디스플레이에 표시가 된다.

이런 이유는 사용자 측면에서 AP기기에 접속을 할 경우 계속 암호를 변경하면서 접속하는 불편한 점을 줄이고자 AP 기기의 전원이 리셋 될 경우만 암호가 변경되는 시스템을 제안한다.

3.2 AP 접속 절차

이동형 단말기에서 무선 랜으로 접속할 경우 인증 절차는 (그림 2)와 같다.

이동형 단말기 무선랜카드의 MAC주소를 AP에 전송하며 AP기기의 플래시 메모리는 단말기의 MAC주소와 현재까지 인증 요청 횟수를 저장한다.

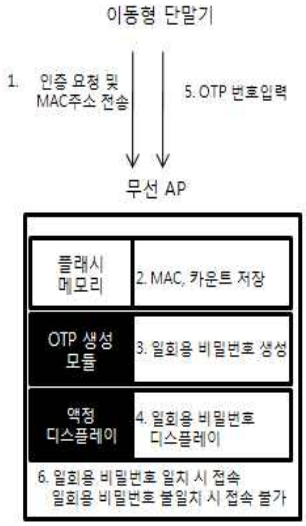

그림 2.. AP의 인증절차
Fig 2. Certification procedures of AP

OTP 생성 모듈은 이벤트 동기화 방식으로 플래시 메모리에 인증 요청 횟수와 MAC 주소 토큰을 조합하여 WEP 키의 자리 수는 최소 6자리에서 최대 8자리로 문자와 숫자를 이용하여 생성하며 이 비밀번호를 AP 기기의 액정 디스플레이에 표시를 한다.

WEP키 저장 방식은 WPA-PSK(AES)로 저장되어 제 3자가 암호화된 키를 가지고 있어도 WEP 키를 유추할 수가 없다. 가정에서 사용하는 사설 AP는 거실 또는 방에 설치가 되어 있기 때문에 사용자는 AP의 액정 디스플레이로 확인 후 WEP 키를 입력한다. WEP 키는 이벤트 기반의 OTP를 사용하여 인증횟수로 비밀번호를 생성하는데 OTP를 잘못 입력 시 이벤트를 동기화 하지 못하는 문제점이 발생한다.

따라서 만약 AP 사용자가 실수 또는 호기심에 의해 잘못 입력했을 경우 플래시 메모리에 저장되어 있는 카운터의 오차 범위(카운터~카운터 +16 범위를 일반적인 오차 범위로 허용함)를 정해 범위 내에 들어올 경우에 사용자 인증을 허용하는 방법으로 사용자 인증을 허용하는 방식으로 문제점을 극복한다[7].

3.3 암호 설정 범위

현재 AP에서 사용하는 WEP 키는 인터넷에 공개되어 있는 WEP 키를 이용하여 접속을 할 수 있다. 이런 WEP 키를 이용하여 AP에 접속 후 AP의 설정을 웹페이지에서 변경할 수 있는 임베디드 소프트웨어 암호도 인터넷에 공개되어 있다[8].

웹페이지에서 웹브라우저의 URL창에서 게이트웨이를 입력을 하면 AP설정을 변경 할 수 있다. 이런 방법을 이용하여 WEP 키를 변경할 수 있을 뿐만 아니라 AP 기기의 중요 설정을 변경 할 수 있다.

이런 중요한 정보를 설정하는 AP기기 암호는 대부분 'admin'으로 통용되거나 없는 경우가 있어 제 3자가 인터넷에 공개 되어 있는 WEP 키를 이용하여 AP에 접속하여 설정을 변경 시킬 우려가 있다. 따라서 이런 암호 또한 본 논문에서 제안한 OTP를 이용하여 액정 디스플레이에 표시해 줌으로써 AP의 설정 값을 변경 하지 못하도록 해야 한다.

3.4 안정성 분석

- 인증 공격 시도

MAC 주소는 LAN카드의 고유번호이지만 운영체제(OS : Operation System)에서 MAC주소를 변경 할 수 있어 이동형 단말기의 WLAN이 AP에 접속할 때 인증된 MAC주소로 변경 후 접속을 시도할 수 있다. 하지만 물리적으로 AP기기의 액정 디스플레이에 표시된 WEP 키를 입력해야지만 접속이 가능하므로 공격이 불가능 하다.

- 암호키 공격 시도

WPA-PSK(AES) 방식은 128,192,256 비트 등의 가변 키 크기를 가지는 수학적 암호화 알고리즘을 사용하

기 때문에 WEP 키를 공격자가 알고 있다고 해도 키 값이 특정 시간이나 일정 크기의 패킷 전송 후에 자동적로 변경됨으로써 현재 기술로는 아직 암호를 해독할 수 없다.

따라서 안전하게 사용할 수 있으며, 현재 인터넷에 공개된 WEP 키로 인증을 시도를 한다면 OTP를 이용하여 WEP 키를 생성하기 때문에 유추할 수 없다[9].

3.5 펌웨어 업그레이드

현재 대부분의 AP 외형 모형은 위의 (그림 3)과 같다고 한다면 펌웨어 업그레이드로 기존 AP들도 본 논문에서 제안하는 시스템의 비슷한 효과를 낼 수 있다.

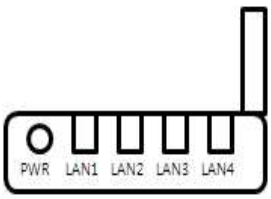

그림 3. 현재 AP 외형
Fig 3. Shape of AP

예를 들면 이동형 단말기에서 AP를 접속할 경우 각 포트의 LED에 불빛이 2~3초간 전부 꺼진 후 AP의 리모트 스위치에서 OTP를 생성하여 한 개씩 LED에서 6번 몇 초간 불빛이 들어왔다 꺼진다. LAN1 포트 기준으로 1,2,3,4의 숫자를 매칭 시켜 기본 인증키의 값을 입력하고 이 인증키 값을 변경하도록 펌웨어를 업그레이드를 한다.

하지만 기존 AP의 하드웨어 설계상 WEP 키를 표시해줄 LED의 개수가 적어 암호화가 숫자로만 국한되며 AP 기기 조작 미숙자는 사용법이 어려움이 있고, 액정 디스플레이가 미설치된 관계로 WEP키를 잊어버릴 가능성이 있는 문제점이 있어 향후 보완해야 될 과제이다.

Ⅳ. 휴대폰 인증 액세스 포인트 설계

현재 웹사이트에서 주민등록번호나 신용카드, 휴대폰 번호, 공인인증서와 같은 매개체를 이용하여 본인인증을 한다. 본 논문에서는 이러한 인증체계 중 개인정보 중요도가 낮은 휴대폰 번호를 이용하여 인증하는 방식을 제안한다[10].

4.1 하드웨어 설계

아래 (그림 4)는 휴대폰으로 인증을 하기 위한 AP기기의 외부 구조도 이다. 기존 AP에서 액정 디스플레이와 숫자를 입력할 수 있는 키패드와 인증을 하기 위해 문자메시지를 보낼 수 있는 SMS 모듈을 추가하였다.

그림 4. 휴대폰 인증 AP
Fig 4. Cell phone certification of AP

SMS 모듈은 휴대폰의 CDMA 방식의 SMS모듈로서 문자메시지를 수신할 수 있다. 현재 인터넷 전화 AP기기의 경우 이동통신사와 AP를 생산하는 업체와 협약을 맺어 출시하는 제품들이 있다. 이런 AP 기기에 SMS모듈을 추가하고 전화번호를 입력할 수 있는 키패드와 액정 디스플레이를 추가를 하여 AP소유자는 기본 WEP 키를 입력하기 위해 AP기기에 문자메시지를 받을 수 있는 휴대폰 번호를 입력한다. AP기기는 난수(WEP 키)를 발생하여 AP 기기에서 사용자가 입력한 번호로 문자메시지를 보낸다.

WEP 키의 길이는 최소 6자리에서 8자리까지 발생

하며 숫자와 문자의 조합으로 생성된다. 생성방법은 AP 기기의 시간을 이용하여 생성하며 입력범위는 아스키 코드를 이용하여 숫자와 영문자의 소문자, 대문자까지이다.

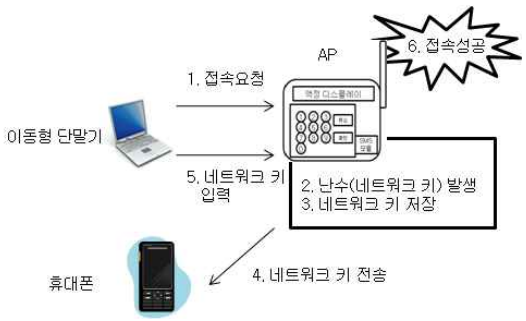

그림 5. 인증 절차
Fig 5. Certification procedures

문자메시지를 받는 사용자는 이동형 단말기를 이용하여 네트워크 키 값을 입력을 한다.

위의 방법으로 접속을 하면 권한이 없는 사용자가 AP에 접속 할 수 없을 뿐만 아니라 WEP 키를 유추하기가 어렵다. 또한 본 논문에서 제안한 OTP 인증 방식의 저장방법인 WPA-PSK(AES)으로 저장되어 액정 디스플레이에 WEP 키를 표시한다.

허가된 다른 단말기가 AP에 접속 시 이 암호를 사용하여 접속하며 암호의 변경 시점은 AP기기의 전원이 리셋 되었을 경우 새로운 WEP 키가 생성되어 문자메시지를 보내는 방식이다[11].

4.2 안정성 분석

- WEP 키 유출

웹사이트 상에서 휴대폰 인증방식은 휴대폰 가입 시 등록한 개인정보와 통신사에 등록된 DB를 대조하여 일치할 경우 인증번호를 보내주는 방식이지만 본 논문의 휴대폰 인증 방식은 AP기기에서만 휴대폰 번호가 저장되어 개인 정보 유출을 최소화 하며 제 3자가 네트워크 키를 요청하여도 AP기기에 입력된 휴대폰에만 WEP 키 문자 메시지가 수신되기 때문에 AP 무단 접속을 하기가 어렵다.

V. 결론 OTP 인증과 휴대폰 인증분석

아래 <표 2>는 기존 AP, 펌웨어 업그레이드, OTP인증방식, 휴대폰 인증방식을 비교하였다.

표 2. AP 비교
Table 2. Comparative AP device

	기존 AP	펌웨어 업그레이드	OTP 인증	휴대폰 인증
사용자 편의성	O	X	△	O
WEP키 유추	O	X	X	X
강력한 암호저장	△	△	O	O
비용 발생	X	X	O	O

기존 AP는 사용자의 편의성은 높지만 인터넷에 공개된 기본 WEP 키를 이용하여 AP를 무단으로 사용할 수 있으며, 펌웨어 업그레이드 방식은 사용자의 편의성은 낮지만 인터넷에 공개된 WEP 키를 사용할 수가 없고 새로운 하드웨어를 설계하지 않기 때문에 비용이 발생하지 않는다. 또한 OTP 인증방식은 액정 디스플레이를 설치하기 때문에 약간의 비용은 발생하지만 일회용 비밀번호를 사용하여 제 3자가 AP를 사용할 수 없고 휴대폰 인증방식은 액정디스플레이, 키패드, SMS모듈을 설치함으로써 비용이 많이 발생하지만 사용자의 편의성 및 강력한 암호저장과 기본 WEP 키를 사용하지 않고 휴대폰으로 인증하는 방식을 사용함으로써 AP를 무단으로 사용할 수 없다.

Ⅵ. 결 론

현재 상용화된 사설 AP의 경우 관리자가 보안적인 측면에서 AP 기기의 로그인 암호와 WEP 키 값을 안전한 암호로 변경함으로서 무선 랜의 보안이 한층 강화되지만 대부분 사용자는 AP 기기의 조작방법 미숙과 안일한 보안 의식으로 인하여 WEP 키를 기본 값으로 사용함으로서 무선 랜의 보안정책에 문제가 있다. 본 논문에서 기본 WEP 키는 사용자가 필수로 변경하지 않아도 공개된 암호를 이용하여 AP 관리자에게 허가받지 않은 제 3자가 AP에 접속 불가능한 방법인 OTP인증방식을 이용한 하드웨어 설계와 휴대폰 인증방식을 이용한 하드웨어 설계 2가지를 제안하였다.

OTP 인증방식은 현재 사용하고 있는 AP를 본 논문에서 언급한 펌웨어 업그레이드를 이용하여 인증을 한다면 몇몇의 문제점이 있기는 하지만 새로운 AP를 구입 하지 않고 기존의 AP를 사용할 수 있어 재사용성이 용이하며 휴대폰 인증 방식은 새로운 하드웨어 설계에 의해 비용이 발생하지만 안전한 인증방식을 사용할 수 있다.

따라서 개인적 측면에서 무단 사용자를 차단함으로써 개인정보 유출 감소할 수 있으며 국가적인 측면에서는 현재 추진하고 있는 무선 랜 보안 대책의 일환으로 AP의 암호화를 의무화하는 법안에 접목시켜 인터넷 대란과 개인정보 유출을 막을 수 있는 효과가 있다.

참고문헌

[1] 신택수,조성민,민상원, “무선 LAN에서 Ad-Hoc과 Infrastructure 모드의 자동전환 기술 설계 및 구현”, *한국통신학회논문지*,제31권 제9A호,pp.837-934,2006

[2] 김희정, "2009년 무선인터넷이용실태조사", *한국인터넷진흥원*, 2009

[3] MIKE SCHIFFMAN, “*HACKER'S CHALLENGE : TEST YOUR INCIDENT RESPONSE SKILLS USING 20 SCENARIOS*”, McGraw-Hill,2002

[4] 김상철, "무선랜 보안(Wireless LAN Security)", *한국정보보호진흥원*, pp.1-6,2002

[5] 송유진,이동혁, “OTP 기반의 웹서비스 인증 메커니즘 설계 및 구현”, *한국전자거래학회지*, 제10권 제2호,pp.1-161,2005

[6] 권동혁,이병관, "무선 액세스 포인터의 디바이스 인증과 데이터 암호화 설계", 한*국인터넷정보학회 춘계학술발표대회*, pp.183-188 ,2009

[7] 김종진,조은영,손현진, “홈네트워크에서의 기기 위치 정보와 OTP 알고리즘을 활용한 인증 보안 메커니즘”, *한국정보과학회 가을 학술발표논문집*, 2007

[8] 김종진,조은영,손진현, "홈네트워크에서의 기기 위치 정보와 OTP 알고리즘을 활용한 인증 보안 메커니즘", *한국정보과학회 가을 학술발표 논문집*,제34권 제2호(D),pp.12-17,2007

[9] 정은희,조인석,이병관“무선 랜 환경에서 OTP를 이용해 사용자 인증을 강화시킨 보안 시스템 설계”, *한국인터넷정보학회*, 제9권 제2호,pp.141-144,2008

[10] 인텐스테크놀로지, “모바일 환경에서의 본인확인 서비스 모델 연구”, *한국인터넷진흥원*,pp.14-16,2009

[11] 김우경,서선희,이경현,"SMS와 OTP에 기반한 사용자 인증 시스템 설계 및 구현", *한국정보처리학회*,제31권 제2호(I),pp.433-435,2005

이기성(Ki-Sung Lee)

2010년 한국기술교육대학교 인터넷미디어공학부 재학

※ 관심분야 : 암호 알고리즘, 무선 인터넷 보안

서희석(Hee-Suk Seo)

2000년 성균관대학교 공학사
2002년 성균관대학교 공학석사
2005년 성균관대학교 공학박사
2005년 한국시뮬레이션학회 편집위원
2005년~현재 한국기술교육대학교 교수

※ 관심분야 : 네트워크보안, 모델링 방법론