 http://dx.doi.org/10.18807/jsrs.2016.6.3.079

무선 인터넷 서비스를 위한 해킹 대응 방안

국 중 각* · 김 희 완**

목 차

요약

무선 인터넷 서비스는 모든 산업을 지원하는 중요한 요소 중에 하나로 자리 잡게 되었다. 어디에서나 무선 인터넷 연결을 통해 노트북을 연결하거나 스마트폰 등을 연결해 사용하는 일이 잦아지면서 그에 따른 해킹 위험도 증가하고 있다. 인터넷 공유기의 DNS 주소 변조를 통한 정보유출 사고를 비롯하여 무선 공유기를 통한 해킹위협은 존재한다.

본 논문에서는 무선 랜에서의 전반적인 취약점을 이용한 해킹 기술들을 다룬다. WEP 암호화 알고리즘과 이를 개선한 암호화 알고리즘을 통하여 무선 랜 보안의 필요성에 대하여 분석하였다. 또한 무선 취약점을 이용한 해킹 기술인 WEP Crack, DoS 공격, DNS Spoofing에서 해킹 기술들을 다루며, 이러한 해킹에 대하여 대응 방안을 제시하였다.

표제어: 무선 인터넷, 서비스, 해킹 기술, 해킹 대응, 암호화 알고리즘

접수일(2016년 5월 16일), 수정일(1차: 2016년5월31일), 게재확정일(2016년 6월 5일)
* 제1저자, 삼육대학교 컴퓨터학부 교수, jkkook@syu.ac.kr
** 교신저자, 삼육대학교 컴퓨터학부 교수, hwkim@syu.ac.kr

1. 서론

현대 사회에서 무선 인터넷은 중요한 요소 중에 하나로 자리 잡게 되었다. 공공장소나 버스나 지하철 등에서도 무선 인터넷 연결을 통해 노트북을 연결하거나 스마트폰 등을 연결해 사용하는 일이 잦아지면서 그에 따른 해킹 위험도 증가하게 되었다. 인터넷 공유기의 DNS 주소 변조를 통한 정보유출 사고를 비롯하여 무선 공유기를 통한 해킹위협은 존재한다.

무선 공유기 보안을 위해서는 공유기 자체의 보안 설정을 하면 된다. 무엇보다 보안이 허술한 벤더의 공유기 제품을 사용하지 않은 것이 가장 좋은 방법이며, 무선 보안 문제는 공유기 뿐만 아니라 기업의 무선랜 사용에 있어서도 문제가 된다. 기업에서 내부자들의 무선 디바이스가 자신도 모르게 인가되지 않은 외부의 무선 AP(Access Point)에 접속해 무방비로 보안 위협에 노출된다. 기업 내부에 무선 AP가 없는 대부분의 기업에서는 무선 보안이 필요없다고 생각하는 경향이 있다. 하지만 내부 직원들의 업무용 스마트폰이나 태블릿PC, 노트북 등이 외부의 무선 AP에 연결되는 경우 보안의 홀이 생기게 된다. 특히, 요즘 통신사가 제공하는 무선 AP나 외부의 비밀번호 없이 사용 가능한 공공 무선 AP가 많은 상황에서 공격자가 외부에 만들어 놓은 무선 AP가 이들과 섞여있다고 가정할 때, 기업 내부에서 임직원들의 무선 디바이스들이 공격자의 무선 AP에 자동 접속된다면, 이를 통해 공격자가 내부로 들어오는 길을 열어주게 되는 것이다.

따라서, 본 논문에서는 무선 랜의 관한 개념과 전반적 취약점을 이용한 해킹 기술 그리고 다양한 해킹 기법에 관한 연구를 다루었으며, 그로 인한 보안의 필요성과 위험에 대한 대응 방안을 논하고자 한다.

2. 관련 연구

2.1 무선 랜 기술의 정의

무선 랜은 무선 신호 전달 방식을 이용하여 두 대 이상의 장치를 연결하는 기술이다. 이를 이용해 사용자는 근거리 저역에서 이동하면서도 지속적으로 네트워크에 접근할 수 있다. 오늘날 대부분의 무선 랜 기술은 IEEE 802.11 표준에 기반하고 있으며, 와이파이라는 마케팅 네임으로 잘 알려져 있다. 와이파이(Wi-Fi)는 와이파이 얼라이언스(Wi-Fi Alliance)의 상표명으로, IEEE 802.11 기반의 무선랜 연결과 장치 간 연결 등을 지원하는 일련의 기술을 뜻한다[1][2]. 처음의 와이파이는 사실상 IEEE 802.11과 동의어로 사용되었으나, 현재 와이파이는 802.11 기반의 많은 소프트웨어 기술을 포함하며, 802.11에서 지원되나 와이파이에서 쓰이지 않는 기술도 있으므로 둘을 혼동하지 않는 것이 좋다.

와이파이 통신은 기본적으로 인터넷에 데이터를 전달하는 기능을 하는 AP(액세스 포인트)와 노트북이나 스마트폰과 같이 사용자가 서비스를 받는 단말간의 통신이다.

스마트폰이나 노트북 등 이동이 많이 이루어지는 단말에는 기본적으로 탑재되어 있어 사용자는 별다른 설정 없이 와이파이를 사용할 수 있으며,데스크톱 사용자도 쉽게 설치하여 사용할 수 있다. 게임기, 프린터, TV 등 다양한 주변 기기들에서도 와이파이를 지원하고 지원하는 단말들이 늘어나는 추세이다.

2.2 IEEE 표준

RFIEEE 802.11은 흔히 무선랜, 와이파이(Wi-Fi)라고 부르는 무선 근거리 통신망(Local Area Network)을 위한 컴퓨터 무선 네트워크에 사용되는 기술로, IEEE의 LAN/MAN 표준 위원회 (IEEE 802)의 11번째

워킹 그룹에서 개발된 표준 기술을 의미한다[3][4].

표 1. IEEE 표준

Tab.1 IEEE Standards

	802.11b	802.11b	802.11g	802.11n
Speed	11Mbps	54Mbs	54Mbps	300Mbps
Distance	450m	300m	450m	450m
Frequency	2.4GHz	5GHz	2.4GHz	2.4GHz/ 5GHz
Advantage	being used mostly	Less interference	Compatible with 802.11b	performance through a multi-antenna technique /a channel bonding
Disadvantage	Transfer speed is slow	No Compatibility	There may be interference from 2.4GHz devices	It requires a wireless

2.2.1 802.11 (초기 버전)

802.11은 2Mbps의 최고속도를 지원하는 무선 네트워크 기술로, 적외선 신호나 ISM 대역인 2.4GHz 대역 전파를 사용해 데이터를 주고받으며 여러 기기가 함께 네트워크에 참여할 수 있도록 CSMA/CA 기술을 사용한다. 하지만 규격이 엄격하게 정해지지 않아서 서로 다른 회사에서 만들어진 802.11 제품 사이에 호환성이 부족했고 속도가 느려서 널리 사용되지 않았다.

802.11b802.11b는 802.11 규격을 기반으로 더욱 발전시킨 기술로, 최고 전송속도는 11Mbps이나 실제로는 CSMA/CA 기술의 구현 과정에서 6-7Mbps 정도의 효율을 나타내는 것으로 알려져 있다[4].

표준이 확정되자마자 시장에 다양한 관련 제품이 등장했고, 이전 규격에 비해 현실적인 속도를 지원해 기업이나 가정 등에 유선 네트워크를 대체하기 위한 목적으로 폭넓게 보급되었으며, 공공장소 등에서 유, 무상 서비스를 제공하는 업체도 생겨났다[4].

2.2.2 802.11a

802.11a는 5GHz 대역의 전파를 사용하는 규격으로, OFDM 기술을 사용해 최고 54Mbps까지의 전송속도를 지원한다[4].

5GHz 대역은 2.4GHz 대역에 비해 다른 통신기기(무선 전화기, 블루투스 기기 등)와의 간섭이 적고, 더 넓은 전파 대역을 사용할 수 있다는 장점이 있지만, 신호의 특성상 장애물이나 도심 건물 등 주변 환경의 영향을 쉽게 받고, 2.4GHz 대역에서 54Mbps 속도를 지원하는 802.11g 규격이 등장하면서 현재는 널리 쓰이지 않고 있다[4].

802.11g는 a 규격과 전송 속도가 같지만 2.4GHz 대역 전파를 사용한다는 점만 다르다. 널리 사용되고 있는 802.11b 규격과 쉽게 호환되어 현재 널리 쓰이고 있다[4].

802.11n은 상용화된 전송규격이다. 2.4GHz 대역과 5GHz 대역을 사용하며 최고 600Mbps까지의 속도를 지원하고 있다[4]. 처음 Draft 1.0이 확정되었을 때, 대한민국의 경우 기술규격 내 주파수점유대역폭의 문제(2개의 채널점유)로 최대150Mbps이하로 속도가 제한되었으나 2007년 10월 17일 전파연구소의 기술기준고시로 300Mbps이상까지 사용할 수 있게 되었다[4]. 이 기술의 최종 표준안은 2008년 말 제정될 예정이었으나 2009년 9월 11일에서야 IEEE 802.11n-2009이 표준안으로 제정되었고[4] 대한민국에 현재 상용화되어 있다. 다른 규격보다 승인 규격이 엄격하고 출력 규제가 심하여, 일부 회사에서는 이 규제를 지키지 않고 있으나, 최대 600Mbps까지 전송속도를 높일 수 있다.

* 5GHz 주파수 대역은 2.4GHz 주파수 대역에 비

해 높은 주파수가 갖는 전파 특성인 강한 직진성과, 신호감쇄에 의한 속도저하가 문제점으로 대두된다.

* 신호세기가 낮아지면 속도 역시 떨어진다.

* AP가 a/b/g 규격 자동설정이 되어있으면 a 규격 단말로 통신하고 있던 영역에 b규격이 한대라도 들어오면 속도가 낮은 b 규격으로 통신이 통일된다.

*AP에 접속하는 단말이 많으면 속도 성능이 떨어진다.

*IEEE 802.11 네트워크를 구성하는 장비들은 암호화되지 않은 상태로 통신할 수도 있고 64비트, 128비트의 WEP 암호화를 사용해 보안성을 높일 수도 있다. 하지만 WEP 자체의 구조적 취약점 때문에 WEP로 암호화된 데이터는 쉽게 해독될 수 있어서 현재 잘 쓰이지 않는다. 지금은 발전된 형태의 WPA, IEEE 802.11i(WPA2), IEEE 802.1x 등의 보안책을 사용한다.

2.2.3 RFID

RFID(Radio Frequency Identification)는 제품에 붙이는 태그(Tag)에 생산, 유통, 보관, 소비의 전 과정에 대한 정보를 담고, 리더(Reader)로 하여금 안테나를 통해서 이 정보를 읽고, 인공위성이나 이동통신망과 연계하여 정보시스템과 통합하여 사용된다[2]. RFID Tag는 무선 칩을 내장하고, 무선으로 데이터를 송수신하여 데이터 수집을 자동화한 Tag이다[3][4]. RFID는 자동인식 기술의 하나로써 데이터 입력 장치로 개발된 무선(RF: Radio Frequency)으로 인식하는 기술이다. Tag안에 물체의 ID를 담아 놓고, Reader와 안테나를 이용해 Tag를 부착한 사물, 동물, 사람 등을 인식하여 관리하고 추적할 수 있는 기술이다. RFID의 장점으로는 직접 접촉을 하지 않고 인식 방향에 관계없이 자료를 인식 할 수 있다. Tag에 붙은 Data를 받는데 인식되는 시간이 짧고, 유지보수가 간편하며, Barcode system처럼 유지비가 들지 않으며, 습도, 온도, 먼지 등에 제한을 받지 않고 data 전송이 가능하며, 많은 양의 data를 보내고, 받을 수 있으며 재사용이 가능한 장점을 가지고 있다.

3. 암호화 알고리즘

3.1 WEP

1999년의 IEEE 802.11무선 LAN 표준에 규정된 WEP(Wired Equivalent Privacy) 암호 방식을 무선 구간에서 전송되는 MAC 프레임들을 40비트 길이의 WEP 공유 비밀 키와 임의로 선택되는 24비트의 Initialization Vector(IV)로 조합된 총 64비트의 키를 이용한 RC4 스트림 암호 방식이다[5]. 이러한 WEP에 의한 단말과 AP간 암호를 위하여 먼저 쌍방은 동일한 패스워드 문장으로부터 생성되는 4종류의 장기 공유 키를 자동 생성한다. 이 4개의 고유 키는 2비트의 KeyID로 각각 구분된다. 이후, 4개의 공유 키 중 하나를 선택하여 MAC 프레임에 대한 WEP 암호시 사용한다.

전송되는 MAC 프레임을 보면 암호화된 데이터뿐만 아니라 암호화시 사용된 IV(Initialization Vector : 3byte 길이의 RC4 암호용 IV값으로써 매 프레임마다 임의로 선택되거나 1씩 단순 증가 됨), KeyID(2bit의 길이를 가지며 송신측이 선택한 4가지의 WEP 비밀 키 중 하나의 KeyID 값을 명시하며, 이 키 ID는 세션 연결 후 변경되지 않음, ICV(Integrity Check Value : 평문 데이터 영역에 대한 무결성 보호를 위한 값으로 WEP에서는 CRC-32가 쓰임)값도 함께 수납된다. 그 결과 원래 MAC 프레임에 8byte가 더해진다.

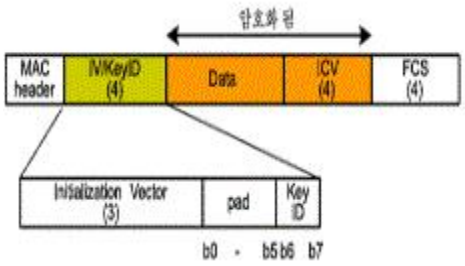

그림 1. WEP 암호

Fig. 1. WEP Cryptograph

WEP 암호화 방식은 64bit 암호화 방식인 40bit WEP와 WEP2인 128bit 암호화 방식인 104bit WEP가 있다.

3.2 WPA/WPA2-PSK

WEP의 보안 취약점이 드러난 이후 그 대안으로 나오게 되었으며, 와이파이 보호접속 (Wi-Fi Protected Access) 라고도 한다.

WEP 보안 취약점이 드러난 후 그 대안으로 802.11i 라는 보안 표준 프로토콜이 등장했다. 802.11i 가 완성되기 전에, WEP 의 대안으로 일시적으로 사용되던 것이 WPA 다. 이 WPA 에서 사용한 암호화 알고리즘은 TKIP 로서, WPA2 에서는 이를 대체하기 위해서 AES 암호화 알고리즘을 사용하여 더 강한 보안 제공한다.

WEP 와 다른 점

- TKIP (임시 키 무결성 프로토콜) 을 통해 데이터 암호화를 향상시켰다.
- WPA2 는 2세대 WPA로서 보안 기능이 개선되었으며 고급 암호 표준화(AES), 사전 인증으로 구성된다.
- WPA 는 Infrastructure 모드만 지원. WPA2는 Infra, Adhoc 모두 지원한다.

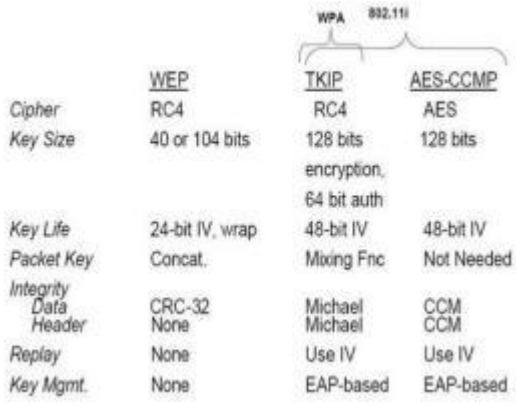

그림 2. WPA/WPA2-PSK 암호화

Fig. 2. WPA/WPA2-PSK Encryption

3.3 WPA Enterprise(WPA-EAP) 방식

WPA-PSK가 기존 WEP의 암·복호화 키 관리 방식을 중점적으로 보완한 방식인데 비해서 WPA-Enterprise는 사용자 인증영역까지 보완한 방식이다. 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 메카니즘을 수용할 수 있도록 IETF의 EAP 인증 프로토콜을 채택한 것이다[6].

규모가 큰 무선 랜 환경에서 WPA-EAP 방식을 구현하기 위해서는 클라이언트와 AP뿐만 아니라 사용자 인증을 수행할 인증서버(Authentication Server)가 별도로 추가되는데 이는 WPA-EAP 구현을 위한 802.1X 표준에서 요구하는 사항을 수용하기 때문이다.

포트기반의 네트워크 접근제어(Port-Based Network Access Control)[7] 표준인 802.1x이 등장하게 된 배경에는 전화접속을 이용한 통신이나 가정의

인터넷 접속 수단으로 사용되는 ADSL/VDSL 환경에서 네트워크 접속 허용을 위한 장치 및 사용자에 대한 인증절차가 요구되었기 때문이다. 802.1X 표준을 구현하기 위해서는 요청자, 인증자, 인증서버로 구성된다.

3.4 무선 랜 보안의 필요성

무선 랜이 보급됨에 따라 편리한 인터넷 환경이 제공되었지만 이로 인해 생기는 위험 또한 크게 증가하고 있다. Firewall이나 VPN등을 구축하고 있는 기관들은 무선 랜의 위협에서 안전하다고 생각하고 있지만 무선 랜 신호가 모든 유선 네트워크의 보안 시설을 뚫고 지나가 침입자들에게 뒷문을 열어주고 있다는 사실은 잘 모르고 있다. 보안이 완벽하지 않은 무선 랜을 이용하면 회사나 단체들의 기업 백본 네트워크에 침입해 다양한 정보를 탈취하고 오염시킬 수 있기 때문에 무선 네트워크 보안문제는 더 이상 주변 문제가 아니다.

무선 랜의 위험성을 이해하려면 먼저 모든 보안 취약점에 대해 이해할 필요가 있다. 무선 랜들은 유선 네트워크의 모든 보안문제를 그대로 갖고 있다. 게다가 무선이라는 점 때문에 더욱 위험하다. 게다가 무선랜 기능이 장착된 노트북 컴퓨터가 늘어나고 운영체제가 점점 더 무선 친화적으로 변함에 따라 대다수 노트북들은 이제 연결 가능한 액세스 포인트(AP)를 자동으로 차는 기능을 기본 사항으로 장착하고 있다.

마지막으로 무선 네트워크 기기들은 연결 방식이 매우 변화무쌍하다. 무선 기기가 만약 매우 강한 신호를 포착한다면 그 새로운 AP에 접속하는 경우도 발생할 수 있다. 이 AP는 바로 그 빌딩 주차장에서 해커가 사용하는 노트북 컴퓨터가 될 수도 있다.

요즘은 무선 랜 액세스 카드가 내장되지 않은 노트북 컴퓨터를 찾기가 점점 더 어려워지고 있다. 그리고 어떤 직원이든지 약간의 돈만 투자하면 무선랜 AP를 구입해 무선 네트워크로 연결되는 게이트웨이를 제공하는 이더넷 잭에 연결시킬 수 있다.

유선네트워크에 점점 더 많은 무선네트워크가 추가되면서 침입자들이 들어올 수 있는 위험성도 점점 더 커지고 있다. 기관이나 회사들은 자기네 회사 내의 AP만 생각하지 말고 기업 전체적으로, 그리고 전 세계에 걸쳐 구축되고 있는 공중보안에 대해 생각해야 할 것이다.

4. 무선 취약점을 이용한 해킹 기술

4.1 WEP Crack

WEP Crack은 동일한 키로 암호화된 다량의 패킷이 필요하기 때문에 공격자가 네트워크에 강제로 데이터 패킷(패킷 인젝션)을 유발해야 한다. 따라서 대상 AP에 aireplay-ng 툴로 ARP Replay를 전송하여 네트워크에 많은 데이터 트래픽이 생기도록 유도한다. 이렇게 발생된 다량의 데이터 패킷으로 WEP Crack에 필요한 동일한 키로 암호화 된 패킷을 수집하는데 데이터가 WEP로 암호화 되어있어도 패킷의 크기를 조사하는 방법으로 ARP 패킷을 식별할 수 있다. 이렇게 발생된 패킷은 airodump 툴로 확인이 가능한데 자동적으로 저장이 된다. 이를 토대로 aircrack-ng 툴을 이용하여 WEP Crack을 수행한다. 값이 ASCII값으로 나타나면 해킹 된 것이다.

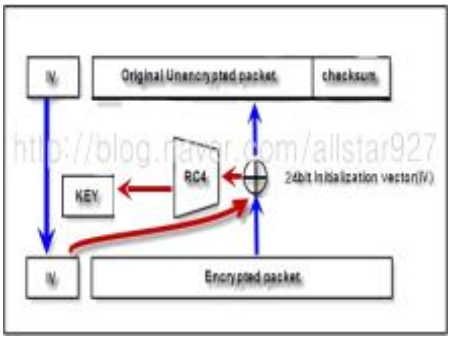

그림 3. WEP크랙 방식
Fig. 3. WEP Crack Method

4.2 DoS(Denial of Service) Attack

서비스 거부 공격(DoS)은 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격이다[8][9]. 무선에서는 AP와 Station간의 연결을 강제적으로 끊는 공격으로 주로 WPA Crack의 과정에서 DoS공격이 감행된다.

공격자는 자신의 AP로 속여 Station에게 802.11 결합과정 중 인증과 결합(Association)을 거부하는 DeAuthentication 패킷과 DeAssociantion패킷을 보내 강제적으로 AP와의 연결을 끊는다.

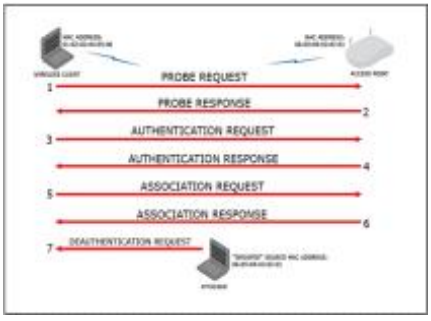

그림 4. Dos공격 원리
Fig. 4. Dos Attack Principle

4.3 DNS Spoofing

정상적인 사용자와 DNS서버 통신 사이에 공격자가 개입하여 비정상적인 DNS답변 송신으로 정보를 취득하는 기법으로 우선 사용자에게 해커의 IP가 GateWay라고 속인다. 그럼 희생자 쪽 컴퓨터는 해커가 GateWay인줄 알고 해커에게 패킷을 보낸다. 희생자가 네이버의 홈페이지를 요청할 시 미리 만들어둔 가짜 네이버 홈페이지를 답신해준다. 그럼 희생자는 그곳이 진짜 네이버인줄 알고 아이디와 패스워드를 입력하면 해커에게 네이버의 아이디와 비밀번호가 고스란히 남게 된다.

그림 5와 같이 정상적인 DNS과정에서는 클라이언트가 naver에 접속을 하면 게이트웨이를 거쳐 DNS서버에 특정회사의 IP를 물어보기 위해 DNS Query를 보낸다. Query를 받은 DNS서버는 회사의 IP를 찾아 다시 전송한다. 전달받은 IP로 접속을 하면 회사의 웹 서버에 접속이 된다.

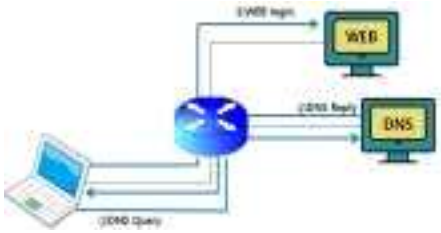

그림 5. DNS 과정
Fig. 5. DNS Process

DNS Spoofing 원리는 그림 6과 같이 사용자가 DNS Query 패킷 전송시 DNS서버와 공격자 모두에서 DNS Query 패킷을 전송한다. 사용자는 공격자가 전송하는 DNS Reply패킷을 받아 해당 주소로 접근한다. DNS서버가 전송하는 DNS Reply패킷은 버려지게 된다.

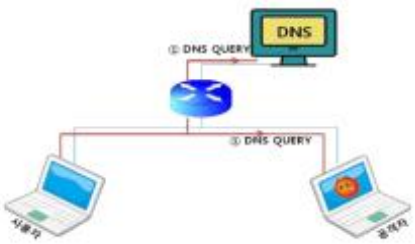

그림 6. DNS Spoofing
Fig. 6. DNS Spoofing

4.4 해킹 대응 방안

해킹에 무방비인 AP들은 보통 별도의 인증 없이 누구나 바로 접속해서 사용할 수 있는 오픈시스템인 경우가 대부분이다. 이런 AP는 AP 사용자그룹에 부여되는 고유 ID인 SSID(Service Set IDentifier)를 지속적으로 브로드캐스팅하기 때문에 '넷스텀블러'(Netstumbler)와 같은 스캐닝 프로그램을 통해 금방 위치를 찾아 접속할 수 있다.

일반적으로 가장 많이 쓰이는 무선랜 규격인 IEEE 802.11b를 지원하는 AP를 찾으려면 보통 근방 100m 안으로 들어가야 하지만, 최대 4㎞ 범위에 있는 AP를 모두 찾을 수 있다. 해커들은 보통 넷스텀블러와 이같은 안테나를 장착한 노트북PC나 PDA를 차에 싣고 찾아내는 소위 '워 드라이빙'(War Driving) 방식으로 보안기능이 없는 AP를 찾아낸다. 개인 사용자들은 ADSL 공유기 가운데 무선랜 AP기능을 제공하는 제품을 구매해서 사용하는 경우도 상당수에 이르는데, 이런 제품의 경우 특별한 보안설정 기능이 없는 경우가 많다. 일단 AP에 접속한 뒤 해커들은 이더리얼(Ethereal) 키스멧와이어리스(Kismet Wireless) 등 패킷 스니핑 프로그램을 사용해 해당 기업이나 기관이 사용하는 IP대역을 찾아내 바로 인트라넷에 들어간다. 이후 에어로피크(Airopeek) 스니퍼 와이어리스(Sniffer Wireless) 등의 툴을 통해 내부 사용자의 ID와 패스워드를 찾아내 모든 내부 정보를 빼낼 수 있다. 일부 AP들은 SSID를 사용자가 요구할 때만 브로드캐스팅하는 기능을 갖추고 있지만, 이 경우에도 에어로피크 키스멧 와이어리스 스니퍼 와이어리스 등을 이용하면 SSID를 쉽게 알아낼 수 있다.

클라이언트 무선랜 어댑터와 AP간 데이터를 암호화하는 웹(WEP) 비밀키 기능을 지닌 AP의 경우에도 에어스노트(Airsnort) 웹크랙(WEP Crack) 등의 웹키 크랙 프로그램을 통해 비밀키를 쉽게 알아낼 수 있다.

이와 같이 크랙 프로그램들은 일부 상용제품도 있지만, 대부분 오픈소스 기반의 무료 SW로 웹사이트나 P2P프로그램을 통해 구할 수 있다.

이밖에 애드혹(Adhoc)이라는 프로그램을 사용해 노트북PC가 AP 기능을 하도록 설정, 외부에서 이 AP로 접속해 해킹하는 경우도 있다. 이 방법은 주로 기업 내부자가 이용할 소지가 높은데, 무선랜 어댑터 하나만 있으면 모든 기업 정보를 외부로 유출할 수 있다.

그러므로 해킹에 대응하기 위해서는 우선 AP의 위치를 지속적으로 알려주는 SSID 브로드캐스팅 기능을 사용하지 말고, 추측이 가능한 SSID 이름을 사용하지 말아야 한다. 예를 들어 특정회사에서 사용하는 AP에 SSID 이름을 회사이름으로 해놓으면 누구나 접속할 수 있도록 대문을 활짝 열어놓은 것과 마찬가지이다. AP에 무선랜 어댑터의 고유번호(MAC주소)를 통해 인증 기능을 수행할 수 있는 경우에는 이 기능을 활성화하고, 웹키 설정 기능도 역시 활성화시켜야 한다. 이 정도의 보안기능 설정만으로도 해킹은 막을 수 있다.

또한, 웹 요청에 대한 잘못된 예외 규칙을 정하여 소스 코드에서 철저하게 검증하여야 한다. 데이터 형식, 허용되는 문자셋, 최소, 최대 허용 길이, NULL 값의 허용 여부를 검사하고 인증되지 않은 사용자가 시스템에 접근할 수 없도록 웹 컨텐츠의 퍼미션을 점검하고 클라이언트 측의 캐싱 점검, Path

Traversal 가능을 점검한다. 또한 패킷 필터링 접근제어와 IP 인증 기반 접근제어, 취약점 서비스 사용의 제거, 암호화 프로토콜의 사용을 통해서 방어 할 수 있다.

5. 결론

무선 인터넷 환경의 발전으로 다양한 서비스가 제공되지만, 그로 인한 해킹 위험도 늘어나고 있다. 무료 와이파이 접속시 스마트폰이나 노트북·태블릿 PC의 중요한 개인정보 및 회사정보가 유출되지 않도록 사용자들의 각별한 주의가 필요하다. 무선랜의 전송 특성상 보안의 고려는 필수적이지만 무선랜 이용환경의 다양화로 인해 일관된 보안정책 적용에 어려움이 있기에 다방면으로 보안강화를 위한 노력을 추진해야 한다.

IEEE에서 제공한 WEP, WPA와 같은 보안 메카니즘들에서 취약성이 발견됨에 따라 다양한 공격 기법들이 제안되었다. 무선 취약점을 이용한 해킹 기술들에 대한 대응방안을 제시하였다. 해킹에 대응하기 위해서는 우선 AP의 위치를 지속적으로 알려주는 SSID 브로드캐스팅 기능을 사용하지 말고, 추측이 가능한 SSID 이름을 사용하지 말아야 한다. 또한, 웹 요청에 대한 잘못된 예외 규칙을 정하여 소스 코드에서 철저하게 검증하여야 한다.

우리가 아무 생각 없이 쓰고 있는 무선 네트워크나 인터넷도 누군가가 지켜보고 있을 수도 있고 마음먹으면 개인정보를 빼서 악용도 가능하다. 그런 면에서 대응방법 등을 항상 숙지하고 부적절한 사이트나 광고 등에 함부로 접속하지 않으며 해킹에 대하여 항상 조심해야 할 것이다.

Reference

[1] S.M. Park, H.J. Kim, J.G. Kim, T.G. Hwang, and S.J. Lee(2013), “Design and Implementation of Multiple Access Game Control System using Bluetooth”, Journal of IKEEE, Vol.17, No.4, 492-498
(박상면, 김호진, 김정길, 황태규, 이상준(2013), “블루투스를 이용한 다중접속 게임 제어 시스템의 설계 및 구현,” 전기전자학회논문지,)

[2] J.A. Son, and K.M. Heo(2013), “Fear and Measures of Motor Vehicles Communication Network Hacking”, Korean Police Studies Review, Vol.12, No.1, 113-142
(손정아, 허경미(2013), “자동차 통신 네트워크 해킹의 위험 및 대책,” 한국경찰연구 12(1), 113-142)

[3] S.H. Hong(2013), “Disconnection of Wireless LAN Attack and Countermeasure”, Journal of Digital Convergence, Vol.11, No.12, 453-458
(홍성혁(2013), “무선 LAN 연결 해제 공격과 보안,” 디지털융복합연구 11(12), 453-458)

[4] H.B. Shim(2012), “Comparative analysis for advanced technologies of the location based service”, Journal of the Korea Institute of Information and Communication Sciences, Vol.16, No.4, 853-871

(심현보(2012), “위치기반 서비스 고도화 기술 비교 분석,” 한국정보통신학회논문지 16(4), 853-871)

[5] J.H. Choi, and S.H. Oh(2012), “Study on Vulnerability and Countermeasures of Authentication Mechanism in Wireless LAN”, Journal of the Korea Institute of Information Security & Cryptology, Vol.22, No.6, 1219-1230
(최진호, 오수현(2012), “무선 랜 환경 인증 메커니즘의 취약성 분석 및 대응방안 연구,” 정보보호학회논문지 22(6), 1219-1230)

[6] K.S. Lee, and H.S. Seo(2010), “The Methodology of Access Point Default WEP Key an Alteration”, Journal of Knowledge Information Technology and Systems, Vol.15, No.4, 1-8
(이기성, 서희석(2010), “액세스 포인트의 디폴트 WEP키 변경 방법론,” 한국지식정보기술학회논문지 5(4), 1-8)

[7] S.R. Lee, and Y.J. Park(2004), “Design of PKI Cryptosystem enabling Efficient Mutual Authentication on Wireless LAN”, The institute of Electronics Engineers of korea, Vol.41, No.3, 69-78
(이상렬, 박용진(2004), “무선랜에서 효율적인 상호인증이 가능한 PKI 보안시스템 설계, 전자공학학회눈문지 41(3), 69-78)

[8] S.W. Jang, and K.Y. Kim(2013), “Detection of Network Attacks Based on an Improved Clustering Algorithm”, Journal of Korean Institute of Information Technology, Vol.11, No.3, 141-150
(장석우, 김계영(2013), “개선된 클러스터링 알고리즘 기반의 네트워크 공격 탐지,” 한국정보기술학회논문지 11(3), 141-150)

[9] J.S. Hong, N.O. Park and W.H. Park(2012), “Detection System Model of Zombie PC using Live Forensics Techniques”, The Journal of Society for e-Business Studies, Vol.17, No.3, 117-128
(홍준석, 니오박, 박원형(2012), “활성 포렌식 기술을 이용한 좀비 PC 탐지시스템 모델,” 한국전자거래학회지 17(3), 117-128)

Joong Kak Kook

Joong Kak Kook is a professor in the Department of Computer Engineering at Sahmyook University. His main research interest is software engineering, mobile learning, object-oriented programming, and App developments. He earned his bachelor's degree from Kookmin University in 1978, and a master degree from McGill University (Montreal, Canada) in 1985, respectively, and received a Ph.D in Computer Information from University of Oregon (Eugene, OR, U.S.A.) in 1988. Before joining Sahmyook University, he had experience as a researcher for four years at the Korea Institute of Science and Technology (KIST) and as a researcher for two year and half years in the Houston University, Texas, U.S.A.

Hee Wan, Kim

Hee Wan Kim is a professor in the Department of Computer Engineering at Shamyook University. He received the MS degree and the Ph.D. degree in the Department of Computer Engineering from Sungkyunkwan University in 1995 and 2002, respectively. He has two Certificate as a Professional Engineer(P.E.) in Information Systems Management and Chief Information System Auditor from Korean Ministry of Science and Technology. He worked as a computer programmer for 4 years at Korea Electric Power Cooperation(KEPCO). His current research interests include database, information system audit, database security, software engineering.

Hacking Countermeasures for Wireless Internet Service

Jung Gak Kook* · Hee Wan Kim**

ABSTRACT

Wireless internet service is an important factor to support all industries. In order to connect and use the smart phones or the laptop via a wireless Internet connection, it has been increasing the hacking risks associated with it. As information spills through the DNS address modulation of the Internet router, hacking threats through a wireless router is present.

In this paper, we are dealing with the hacking technique utilizing the overall vulnerability of a wireless LAN. We analyzed the need for the wireless LAN security through WEP encryption algorithm and the improved encryption algorithm. In addition, we presented a countermeasure against these hacking technologies which is WEP Crack using wireless vulnerability hacking technology, DDoS attacks, DNS Spoofing.

Keywords: Wireless Internet, Service, Hacking Technology, Hacking Countermeasures, Encryption Algorithm

* Professor, Sahmyook University, Division of Computer Engineering, jkkook@syu.ac.kr
** Professor, Sahmyook University, Division of Computer Engineering, hwkim@syu.ac.kr