이동통신 시스템에서의 WDA에 따른 보안 강화 기법

김영석*, 심 원**
e-mail:ganius84@snut.ac.kr*, wonshim@snut.ac.kr**

Security Reinforcement Technics against WDA in Mobile Communication System

Kim Young Seok*, Shim Won**
*Dept of Computer Science & Engineering
Seoul National University of Science and Technology

요 약

인터넷의 급격한 발전과 이용자의 증가로 인터넷은 이미 우리 사회에서 없어서는 안 될 중요한 요소가 되었다. 이러한 인터넷의 발달은 IT산업의 핵심요소가 되었으며 그 중요성이 점점 부각되고 있다. 특히 무선 네트워크는 다양한 단말기(노트북, PDA, 스마트폰)가 대중화되었고 이를 지원하는 표준이 만들어졌으며, 무선 네트워크 사용지역의 확대로 인하여 언제 어디에서나 정보환경에 가까이 접근할 수 있는 여건이 마련되었다. 그러나 이동성이 좋고 편리한 무선 네트워크의 장점의 이면에는 개인정보가 유출될 수 있는 치명적인 문제점들이 드러나기 시작했는데, 케이블을 사용하는 유선환경과는 달리 무선환경에서는 전파를 이용하여 통신하는 점을 악용하여 무선 AP를 도청하거나 패킷을 스니핑하여 개인정보를 유출하는 사례가 빈번하게 일어나고 있다. 본 논문에서는 현재 사용되고 있는 무선 네트워크의 기술표준을 분석해보고 실제 무선환경에서 개인정보가 얼마나 쉽게 노출될 수 있는가를 알아보기 위해 제작한 사설 안테나를 사용하여 무선 AP의 신호를 가로채 패킷을 분석하는 방법을 시연한다. 또한 안테나 각각의 지름을 달리하여 신호강도의 차이가 얼마나 있는지 분석하고, 개인정보를 보호하기 위한 방법을 제시한다.

1. 서론

1980년대 말 미국의 프록심, 심볼 등의 무선기기 업체에서 처음 사업화된 무선 네트워크 기법은 시행착오를 거치며 20여년이 흐른 2000년 후반에 무선 네트워크 기술의 발전과 이동통신 환경을 저해하던 각종 플랫폼들이 통합되었고, 특히 무선네트워크와 인터넷의 결합으로 등장한 무선 AP의 등장으로 인터넷 환경의 혁신을 이루게 되었다. 그러나 이러한 무선 네트워크의 필요성과 중요도에 비하여 보안 기법의 발전정도가 미약하고, 이에 대한 연구는 계속 이루어지고 있으나 무선 네트워크를 이용한 개인정보 유출사례가 점점 증가하는 추세이다. 2009년 방송통신위원회 국정감사 자료에 의하면 현재 국내에는 약 500만대의 무선 AP가 보급되어 사용 중 이지만 이중 74%인 370만대가 보안이 적용되지 않은 무선 AP로 파악되고 있다. 이렇게 보안이 취약한 무선 AP에 침입할 목적으로 차량이나 이동수단에 노트북과 크래킹에 필요한 다양한 무선통신기기를 적재한 상태에서 사무실이나 가정집 근처의 무선 AP에 접속하여 네트워크에 접근한 뒤에 중요한 정보를 엿볼 수 있는 패킷분석 프로그램으로 각종 개인정보를 엿보거나 가로채는 War Driving Attack 기법이 등장하였다. 이에 따라 이동통신 환경에서의 보안 기법에 대한 연구의 필요성이 증대되고 있다.

* 서울과학기술대학교 산업대학원 컴퓨터공학과 석사과정
** 서울과학기술대학교 컴퓨터공학과 교수

2. WDA의 정의

War Driving이란, 이동수단을 이용하여, 이동하며 무선 랜 지역을 찾고, Sniffing하는 행위를 말한다. 또한, 특정 지역의 무선 AP등 무선 랜 기기의 위치를 지도화 하는 것을 말하기도 한다.

War Driving이라는 용어는 워 다이어링(War Dialing)이라는 용어와 비슷한 점이 많다. 워 다이어링은 쓸만한 서버나 기계를 찾기 위해서 특정한 범위의 전화번호를 계속 다이어링 하는 일을 말한다. 이러한 방법을 통해서 경우에 따라 대학교의 보안이 허술한 서버나 비밀스러운 기계들에 접근하게 되는 경우가 있었다. 80년대에나 사용했던 이러한 방법이 다시 등장했는데, 바로 무선 랜에 대한 War Driving이다.

War Driving의 종류는 여러 가지가 있다. 이동수단에 따라서, 자전거로 무선 AP를 검색하고, Sniffing하는 행위는 War Cycling이라 하고, 이동 수단이 도보인 경우에는 War Warking, 비행기인 경우에는 War Flying이라고도 한다.

War Driving의 방법으로는 첫 번째로 운영체제에 따라 무선 AP를 검색해주는 다른 프로그램을 사용한다. 윈도우는 NetStembler, 리눅스는 Kismet과 airsnort, BSD는 dstumbler, PocketPC는 Ministumbler, Pocket Warrior는 PocketWinC를 사용한다. 먼저 기본적인 준비물로 <그림 1> 과 같은 무선랜 카드와 안테나, GPS 등이 필요하다. 무선랜 카드는 외장 안테나 장착 가능한 모델이 좋으며 USB로 된 외장 무선랜 카드도 이용되고 있다. 또한 각 운영

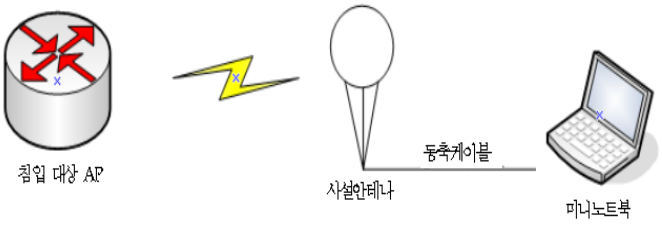
체제의 프로그램들이 지원하는지 여부도 중요하다. 특히 무선랜 카드는 제조사별로 특성이 많이 다르므로 선택에 유의하여야 한다.

<그림 1> 무선랜카드

<그림 1>의 무선랜카드와 별도로 여기에 먼 곳의 신호를 수신하여 전파수용범위를 넓히기 위한 안테나가 필요하다. 우선 무선 랜 카드가 <그림 1>과 같이 외장 안테나 포트를 지원해야 안테나를 사용할 수 있다. 안테나의 사용여부는 옵션이지만, 전파를 잘 받는 좋은 위치가 아니라면 안테나는 필수적으로 사용되어야 한다. 그리고, 각 무선 AP의 위치를 찾아내 기록하기 위한 GPS가 있다면 지도상의 무선 AP지도를 작성할 수 있다.

3. 사설 안테나를 이용한 WDA 실험

2장에서 언급한 내용을 바탕으로 본 논문에서는 War Driving Attack 에서의 침입 유형 중 <그림 2>와 같이 직접 제작한 안테나를 이용하여 보안설정이 적용되지 않은 실제 무선랜에 접속, 해당 네트워크의 패킷을 분석해보았다. 또한 무선랜 접속에 이용하는 안테나의 크기를 4개로 달리하여 접속대상 AP의 신호강도를 서로 비교, 분석하였다.



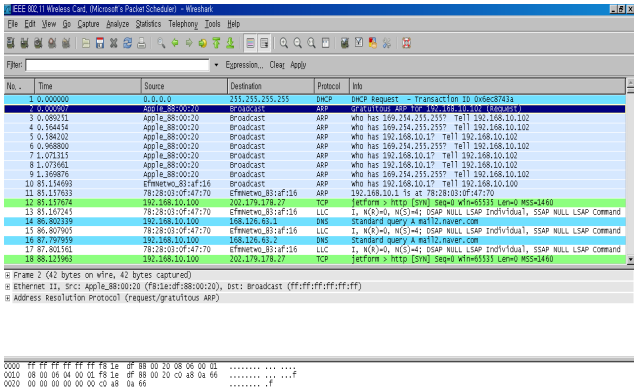
<그림 2> 무선 네트워크 침입 개요

<그림 3>과 같은 안테나와 무선랜카드 제조사에서 제공되는 신호강도 측정 프로그램을 이용하여 주변 AP를 검색한 뒤 신호강도가 비교적 강하고 보안설정이 되어 있지 않은 AP에 접속한 뒤 와이어샤크 프로그램을 이용하여 패킷을 분석해 보았을 때 다음과 같은 결과를 얻을 수 있었다.

<그림 3> 신호수신용 안테나

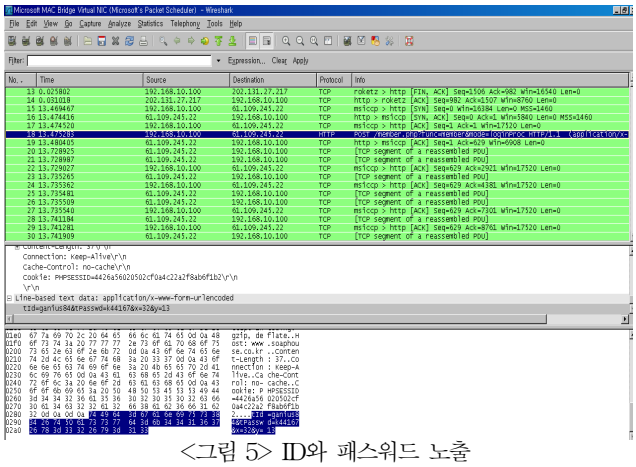
1. 인터넷 사용 경향(웹 사이트 탐색 주소)
2. MSN 대화내용
3. 패킷을 암호화하여 전송하지 않는 사이트에서의 ID와 패스워드
4. 스마트폰과 같은 무선기기의 Mac Address
5. ftp서버에서 주고받는 파일정보

위의 패킷분석 결과에서 나타난 개인정보 유출은 심각한 보안 위협이 될 수 있으며, 특히 개인정보인 ID와 패스워드가 노출되는 것이 확인되었다. 인터넷을 사용하는 대다수의 사람들이 하나의 ID와 패스워드로 여러 사이트에 가입하여 사용하는 경향이 있기 때문에 한번 노출될 경우 다른 사이트에서도 개인정보 유출이 있을 수 있다.



<그림 4> 와이어샤크에서 스마트폰의 Mac Address 추출

보안이 적용되지 않은 무선 AP에 원격으로 접속하여 패킷을 수집해보면 IP주소와 목적지를 쉽게 알 수 있고 AP에 접속되어 있는 각종 무선기기의 MAC Address도 쉽게 파악이 가능하다. <그림 4>에서 스마트폰으로 무선 AP에 접속한 상태(Apple_88:00:20)와 화면 중간 부분에 MAC Address(f8:1e:df:88:00:20)까지 표기되는 것을 알 수 있으며 FTP 서버에 접속하여 주고받은 파일명과 송신지 IP 까지도 쉽게 파악가능하다. 무선 AP에 접속하여 패킷분석을 해 본다면 누구나 쉽게 개인이 사용하는 무선기기의 종류나 자주 이용하는 사이트와 같은 인터넷 이용 성향 파악이 가능하다. 또한 네이버나 다음과 같은 대형 포털사이트가 아닌 쇼핑몰이나 개인이 만든 홈페이지와 같이 패킷을 암호화하지 않는 사이트에 접속하는 경우 아이디와 패스워드가 그대로 노출될 수 있다. 이것은 심각한 보안 위협을 가져오게 되며, 패킷을 가로채는 쪽에서 필터링을 거치면 아주 간단하게 개인정보를 추출하는 것이 가능하다.



<그림 5> ID와 패스워드 노출

위의 실험 결과를 바탕으로 실제 20% 이상 신호강도를 가지고 있는 무선 AP 환경에서 개인정보를 추출해 본 결과 <그림 5>와 같이 대다수가 개인정보 보호에 취약한 것으로 나타났으며, 특히 패킷을 암호화하여 전송하지 않는 사이트에 로그인을 하는 경우 수집된 패킷에 ID와 패스워드가 그대로 패킷 수집 결과에 나타났다. 14회의 실험을 수행한 결과는 다음 [표 1] 과 같다.

[표 1] 무선 AP에서의 개인정보 수집 가능 여부

신호강도/측정항목	실험 대상 사이트	ID와 패스워드 수집가능 여부
25%	S쇼핑몰(1)*	○
30%	S사이트(2)	○
29%	E사이트	○
40%	W사이트(1)	○
32%	S사이트(3)	○
33%	H사이트	○
26%	S사이트(4)	○
28%	W사이트(2)	○
35%	S사이트(5)	○
40%	S사이트(6)	○
22%	K사이트	×
27%	N사이트	×
31%	G사이트	×
34%	S사이트(7)	×

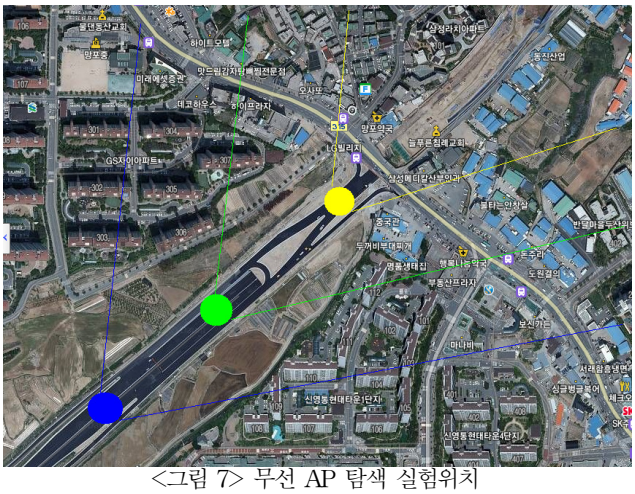
* 해당 사이트 주소를 이니셜로 기재함

4. 안테나의 크기와 무선 AP의 거리에 따른 신호강도 분석

보안의 관점에서 무선랜 신호는 너무 멀리 날아가며, 복도, 주차장 혹은 이웃하는 건물로까지 새어나간다. 그러나 성능이라는 측면에서 되는 신호는 사용자의 필요나 기대보다 훨씬 못 미치는 경우가 종종 있다. 무선랜 AP는 탁 트인 공간 에서는 300m 정도까지 쉽게 도달할 수 있으며 침입을 하려는 경우 비교적 장애물이 없는 방향으로 안테나를 지향하게 되면 비교적 쉽게 타인의 AP에 접속하는 것이 가능하다. Wi-Fi 장치들은 Equivalent Isotropically Radiated Power(EIRP)로 일컫어지는 주어진 신호 세기로 RF 에너지를 방사함으로써 802.11 프레임들을 전송한다. 이 출력 파워는 케이블과 커넥터에 의해 감쇠될 수 있으며 앰프나 이득이 큰 안테나에 의해 증가되어질 수 있다. 최대 EIRP는 제품에 따라 다르며 법적인 한계의 영향을 받는다. RF에너지가 송신기의 안테나로부터 방사될 때 파면은 전파가 진행하는 방향에 있는 공기와 장애물을 통해 나아간다. 자유 공간 경로 손실은 에너지가 공기 중으로 산란될 때 손실되는 파워를 나타내며 주파수와 거리의 함수로 나타내어진다. 다시 말하면, 수신기가 멀리 있으면 있을수록 파워 손실은 커지며 그로 인해 신호 세기 지수(Received Signal Strength Indicator)는 낮아지게 된다. Airespace의 디자인 노트는 802.11b/g에 사용되는 2.4GHz 신호에 대해 벽판으로 되어 있는 담의 경우 4dB, 벽돌 담에 대해서는 8dB, 그리고 콘크리트 벽에 대해서는 10~15dB의 손실이 발생한다고 추정하고 있다. 본 논문에서는 원거리의 Wi-Fi 신호를 크기가 각각 다른 4개의 안테나를 사용하여 거리별로 측정하여 무선 AP의 신호강도와 거리의 상관관계를 알아보는 실험을 수행하였다.

<그림 6> 지름이 다른 4개의 안테나

실험을 위해 <그림 6>과 같이 지름이 각각 다른 사설 안테나를 제작하여 원거리에서 무선 AP를 탐지하고 접속이 가능한지 시도해 보고, 안테나의 지름과 무선 AP의 거리를 각각 달리하여 신호강도의 차이가 어떤지 분석해 보았다.



<그림 7> 무선 AP 탐색 실험위치

<그림 7>의 위치와 같이 신호를 방해하는 장애물이 비교적 적은 곳을 선정하여 안테나를 이용, 무선 AP신호강도의 차이가 얼마나 발생하는지를 측정해 본 결과, 안테나의 지름이 크고 무선 AP와의 거리가 가까울수록 신호강도가 더 높게 나오는 것으로 나타났으며, 결과값을 표로 정리하면 [표 2]와 같다.

[표 2] 측정환경에 따른 무선 AP 검색결과

거리 150m		
지름	무선AP갯수	최대신호강도
50cm	42	57%
40cm	35	47%
30cm	28	42%
20cm	40	37%
거리 300m		
지름	무선AP갯수	최대신호강도
50cm	42	42%
40cm	35	37%
30cm	21	31%
20cm	37	26%
거리 500m		
지름	무선AP갯수	최대신호강도
50cm	56	31%
40cm	42	27%
30cm	28	25%
20cm	46	22%
침입가능한 무선 AP	35개	

무선 AP에 접속이 가능한 신호강도는 높을수록 유리한 것은 의심의 여지가 없으나, 신호세기가 상대적으로 낮은 경우에도 접속은 가능하다. 그러나 신호의 세기가 감소하면 802.11 장치는 통신을 지속시키기 위해 자동적으로 낮은 데이터 속도로 전환된다. 이런 경우 802.11 프로토콜 오버헤드로 인해 어플리케이션 처리율은 데이터 속도의 절반밖에 나오지 않게 된다. AP에 침입하여 패킷을 분석하는 경우 안정적으로 신호를 할 수 있는 환경이 마련되어야 하는데, 본 논문에서는 무선 AP 신호강도별 속도와 안정성, 신호지연율을 측정하는 실험을 수행하였으며 그 결과는 [표 3]과 같다.

[표 3] 신호강도별 속도측정 결과

신호강도 / 측정항목	다운로드	업로드	신호지연율
42%	12.7Mbps	16.0Mbps	8.0ms
25%	1.19Mbps	2.36Mbps	20.2ms
13%	22.5kbps	43.4kbps	298.0ms

5. 결론

본 논문에서는 개인이 사용하는 무선 AP에 대한 보안을 다음과 같이 제안한다.

첫째. 사설망을 통한 인증 및 암호화를 이용한다. 무선 데이터 암호화에는 안전성이 검증된 CCMP가 권장되며, CCMP의 경우에는 128비트 블록키를 사용하는 CCM(Counter Mode Encryption with CBC-MAC) 모드의 AES 블록 암호 방식을 사용한다. 이러한 WPA2 방식을 사용하기 위해서는 무선 AP와 무선 단말기 모두에서 WPA2를 지원하여야만 해당 기능을 사용할 수 있다. 현재 WPA2-PSK의 경우 초기 무선랜 인증 시 진행되는 4 웨이 핸드쉐이킹 단계의 무선 패킷수집을 통해 비밀키 유추가 가능한 문제가 있다. 이를 보완하기 위해서는 비밀키는 특수문자를 포함한 임의의 문자를 사용하여 최대한의 자리수를 사용하도록 한다.

둘째. MAC Address Filtering 을 이용하여 등록되지 않은 MAC 주소를 가진 무선기기의 접근을 차단하도록 한다. 802.11 네트워크에서 보안을 강화하기 위해 각각의 AP는 허가된 클라이언트 컴퓨터나 무선기기의 MAC 주소가 이 리스트에 포함되어 있지 않으면 클라이언트는 해당 AP에 접근하지 못한다. 따라서 SSID와 더불어 MAC 주소 필터링은 좀 더 향상된 보안 설정을 제공한다. 개인의 경우 가정이나, 사무실 혹은 자주 이용하는 장소의 무선 AP에 MAC 주소를 등록하여 사용한다면 개인정보가 유출될 가능성이 낮아진다. 하지만 이 방법은 MAC 주소가 효과적으로 관리될 수 있어야 하며, 따라서 규모가 작은 네트워크에 가장 잘 적용될 수 있다. 각 AP들은 관리하는 MAC 주소의 리스트를 수동으로 입력해 주어야 하며, <그림 8>과 같이 설정이 가능하다.

<그림 8> MAC Address Filtering 설정

참고문헌

[1] 국가정보원, 국가정보보호백서, 2008

[2] 한국인터넷진흥원, 정보보호 동향 브리핑, 2009.7

[3] 한국인터넷진흥원, 무선랜 보안 안내서, 2010.1

[4] 방송통신위원회 국정감사자료, 2009

[5] IEEE, "Wireless Medium Access Control(MAC) and physical layer(PHY) specification for Enhanced Security", IEEE Std 802.11i, 2004

[6] "Cafe Latte with a Free Topping of Cracked WEP - Retrieving WEP Keys From Road-Warriors" Md Sohail Ahmad, Vivek Ramachandran, 2007

[7] "Wireless Network Security for IEEE 802.11/a/b/g and Bluetooth(Draft)", NIST, 2007

[8] NIST 기술문서, SP 800-48 Rev.1 Guide to Securing Legacy IEEE 802.11 Wireless Network, Jul 2008

[9] "A Comprehensive Review Of 802.11 Wireless LAN Security and the Cisco wireless security suite", Cisco, 2002