무선랜 워드라이빙 공격의 위험성과 대응방안

최영남* · 조성목**

The Risk of Wardriving Attack Against Wireless LAN and its Counterplan

Young-Nam Choi* · Sung-Mok Cho**

요 약

IEEE 802.11 무선 랜은 구축이 용이하고, 이동성과 편이성 등의 장점이 있어 캠퍼스, 기업, 핫 스팟 영역의 공중망에 이르기까지 응용범위를 급속히 넓혀가고 있다. 그러나 무선 랜은 RF를 매체로 사용하기 때문에 근본적으로 보안이 취약해서 개인정보와 기업 내부자료의 침해 위험성이 증가하고 있으며, 특히 무선 랜에서 보안 취약성을 찾아내는 워드라이빙 공격은 더욱 더 심각성을 더해가고 있다.

본 논문에서는 무선 랜에 대한 워드라이빙 공격을 위한 여러 과정과 준비단계에 대하여 전반적으로 살펴보고, 무선 랜에서의 워드라이빙 공격으로부터 정보침해 사고를 예방할 수 있는 대응방안을 제시한다. 이를 위해 무선 랜에서의 워드라이빙 공격에 적합한 장비를 제작하였고, 제작된 장비를 사용하여 서울시 양재동 일대의 무선 랜 AP 보안 취약성을 조사하였다.

ABSTRACT

The application range of IEEE 802.11 wireless LAN has rapidly expanding from campus, enterprise to the public network of Hot Spot area due to the advantages of easiness of construction, mobility of wireless client station, convenience of usage and so on. However the security of WLAN(Wireless LAN) is vulnerable inherently because of using RF as a medium, and so the dangers of infringement of personal information and inside data of enterprises have increased and wardriving attack searching for security vulnerability in wireless LAN has become more serious especially.

In this paper, we find out the overview of various procedures and preparatory stages for wardriving attack against wireless LAN, and propose complementary methods to prevent information infringement accidents from wardriving attack in wireless LAN. For this purpose, we make an equipment which is suitable for wardriving in wireless LAN and show security vulnerability of AP(Access Point) operation in WLAN around Yangjae-Dong in Seoul as a result of using the equipment.

키워드

WLAN(Wireless LAN), RF(Radio Frequency), Wardriving, AP(Access Point)

* (주)터보테크 기술연구소 연구원

** 동명대학교 정보보호학과 부교수 (교신저자)

접수일자 : 2009. 04. 03

심사완료일자 : 2009. 04. 28

Ⅰ. 서 론

무선랜 기술은 무선전파를 이용함으로서 모든 단말이 선으로 연결됨으로 인해 발생하는 고가의 시공비와 소모성자재의 잦은 파손, 이동이 잦은 노트북이나 PDA 단말 사용의 불편함 등을 극복하였다.

선로가 필요치 않은 편의성과 더불어 속도면의 한계를 극복한 무선랜은 지금 우리생활의 곳곳에 자리 잡아가고 있으나, 무선랜의 전파신호를 감청하거나 변조하는 새로운 정보침해유형이 발생하고 있고, 이러한 침해유형은 매우 위협적인 요소로 부각되고 있다.[1]

무선랜을 이용한 공격은 무선전파를 이용한다는 점에서 공격의 근원지를 파악하기가 어렵고 통신자원의 무단점유라는 1차적 피해보다 무단점유된 내부네트워크의 각 호스트에 2차적 피해가 발생할 수 있어 그 위험성은 매우 높다. 또한 점유당한 네트워크의 호스트에 2차적 피해가 발생할 경우 피해호스트에서 발생하거나 피해호스트를 경유한 통신패킷을 감청할 수 있다는 점도 유의할 필요가 있다.

워드라이빙이라 함은 위에서 기술한 무선랜 공격을 위해 공격자가 컴퓨터와 무선랜 어댑터, 무선랜 안테나를 가지고 차량을 이용하여 취약네트워크를 탐색하고 탐색된 네트워크를 공격하는 행위를 말한다. 차량을 이용한 워드라이빙은 접근성이 강하고 불특정 다수의 네트워크가 공격자에게 침해당할 소지가 있기 때문에 무선랜 워드라이빙은 무선네트워크를 구성한 기업이나 개인에게 매우 위험한 요소이다.[2-3]

본 논문에서는 무선 랜에 대한 워드라이빙 공격을 위한 여러 과정과 준비단계에 대하여 전반적으로 살펴보고, 무선 랜에서의 워드라이빙 공격으로부터 정보침해 사고를 예방할 수 있는 대응방안을 제시한다. 이를 위해 무선 랜에서의 워드라이빙 공격에 적합한 장비를 제작하였고, 제작된 장비를 사용하여 무선 랜 AP 보안 취약성을 조사하였다.

Ⅱ. 본 론

1. 무선랜 워드라이빙 환경 구축

무선랜 워드라이빙은 기본적으로 보안이 취약한 무선랜 네트워크를 찾아 해당 무선랜 네트워크를 무단으로 사용하는 것이 1차적인 목적이다. 따라서 차량을 이용해 이동하며 이용 가능한 AP를 찾기 위해 노트북이나 PDA와 같이 사용자가 무선랜 명령을 입력하여 수행할 수 있는 공격용 호스트와 무선랜 어댑터, 무선랜 안테나 등이 필요하다.[4-5]

워드라이빙 공격은 차량을 이용해 이동하며 무선랜 네트워크를 공격한다. 그러나 일반적으로 차량에는 항상 유도 전기장이 발생하게 되는데 유도전기장으로 인하여 차량 내에서 외부전파를 수신하는 것이 원활치 못할 수 있다. 따라서 원활한 워드라이빙을 위해서는 사용되는 안테나와 공격 호스트 등에서 전기를 인가받을 때 차량의 접지와 전위차를 제거해주면 전기장과 전파방해, 전류유도 노이즈 등을 상당부분 해결할 수 있다.

2. 무선랜 워드라이빙의 과정과 방법

무선랜의 워드라이빙 방법은 공격대상 네트워크의 구성방식과 암호화 방법에 따라 달라지며 무수히 많은 경우의 수에 따라 적절히 공격방법을 선택해야 한다. 보편적인 무선랜의 환경에서는 무선랜 이용의 편의성으로 인해 암호키가 설정되어 있지 않은 경우가 많은데 이런 네트워크는 매우 취약하다. 차량으로 해당 네트워크의 근처로 접근하여 네트워크에 접속하는 것만으로 공격은 성공한다. 따라서 본 논문에서 살펴볼 워드라이빙 방법은 무선랜 암호키가 설정되어 있는 네트워크에 대해서만 다루도록 한다.

2.1 WEP Key 방식 네트워크의 공격

국내 보급된 많은 무선랜 네트워크는 WEP Key 방식을 이용한다. WEP키는 알려진 바와 같이 MAC헤더 이후에 붙는 IV/Key-ID가 평문으로 노출된다는 점, WEP seed를 RC4 PRNG에 의해 생성된 키스트림을 재사용함으로서 세션 연결 중에 프레임이 계속 전송되면 중복된다는 점이 취약하다. 따라서 무선랜으로 구축된 네트워크에 적절한 공격을 가하게 되면 WEP Key의 키스트림을 복원할 수 있다. WEP Key를 이용하는 무선랜 네트워크는 무선랜 AP와 접속 호스트 사이를 공격하는 기법과 Clientless 환경에서 무선랜 AP에 Fragmentation 공격을 가하는 기법이 있다.

2.2 WPA Key 방식 네트워크의 공격

WEP Key 방식의 무선랜 네트워크 보안은 구조적 결

함으로 인한 취약성을 가지고 있어 지금은 발전된 형태의 WPA Key 방식의 보안을 많이 이용하는 추세다. 그러나 아직도 많은 무선랜 네트워크에서 WPA를 보편적으로 사용하고 있지는 않다. WPA는 WEP Key 암호화를 보완하는 TKIP(Temporal key Integrity Protocol) IEEE802.11i 표준을 기반으로 하고 있고 인증부분은 802.1x 및 EAP를 도입해 성능을 높였다. 특히 패킷 당 키 할당기능과 키 값 재설정 등으로 인하여 WEP Key 방식의 무선랜 네트워크 보안환경에 비해 매우 강력해졌다. 그러나 WPA Key는 인증이 발생하는 과정에서의 4 Way-Handshake 부분을 캡쳐하여 사전파일을 이용하면 대입형태로 이를 공격할 수 있다. 다만, 사전파일에 존재하지 않는 어려운 키를 이용할 경우 이를 크랙하기는 쉽지 않다. 현재 사전파일에 존재하지 않는 어려운 키에 대한 대입공격은 시간이 지남에 따라 원활해지고 있다. 이는 무차별 대입방식에서 Process Unit 의 속도에 따라 시간을 매우 단축시킬 수 있기 때문이다.[6]

2.3 RADIUS 환경에서의 액세스 포인트 공격

앞서 살펴본 바와 같이 WEP과 WPA를 이용한 무선랜 네트워크는 IV(Initialization Vector) 패킷을 수집하여 재사용되는 시점을 통해 Key를 Crack 하거나 인증과정에서의 4Way Handshake를 이용하여 대입방식으로 공격이 가능하다. 이러한 암호키스트림 방식의 무선랜 보안모델의 보안성을 좀 더 강화하기 위해 외부 인증서버로 RADIUS(Remote Authentication Dial In User Service)를 이용한다. 사전대입을 통한 Key의 크랙을 최대한 방어하고 추가적으로 인증서를 이용한 인증까지 도입된 형태의 네트워크는 공격자의 입장에서 시간 및 비용 측면을 다시 고려하게 하는 효과적인 방법이다. 그러나 RADIUS를 이용한 네트워크도 AP에서 RADIUS Server와의 통신을 중계해 주기 때문에 해당 AP를 공격하면 작동불가능 상태로 돌입하게 된다. 많은 네트워크 장비들은 Fail Open 원칙을 따르기 때문에 보안상 문제가 있더라도 가용성을 목적으로 보안기능을 무력화 한 다음 서비스 하는 경우가 많다. Fail Close 원칙을 따르는 AP라 하더라도 공격자가 임의의 조작된 AP를 공격대상 AP와 같은 채널에 같은 SSID 및 변조된 MAC어드레스를 사용하여 위치시킨다면 공격대상 AP가 작동 불가능 상태가 되는 순간 해당 AP에 접속되어있던 Client 컴퓨터들은 공격자가 준비한 AP로 재인증하여 접속하게 된다. 이러한 공격과정에서 이용되는 조작된 AP를 흔히 Rogue AP라고 부른다. 과거의 Rogue AP는 네트워크 관리자들이 통제하지 못하는 액세스 포인트 정도로 그 위험성을 상대적으로 낮게 평가하였으나 오늘날 Rogue AP의 공격대상 Host로는 노트북 컴퓨터나 데스크탑 컴퓨터, PDA 단말, 바코드스캐너, 복사기, 프린터 등 네트워크 관리자가 보안적인 조치를 취하기 어려운 모든 장치에 위협이 되고 있다.

2.4 실제 무선랜 공격을 위한 준비

무선랜을 점유하기 위한 워드라이빙 공격은 상황에 따라 알맞은 방법을 선택해야 한다. 대상 무선랜의 위치가 공격자의 위치와 얼마나 멀리 떨어져 있는지, 대상 무선랜이 몇 층 높이에 있는지, 각도는 얼마나 되는지에 따라 워드라이빙 공격에 이용할 무선랜 안테나의 종류를 달리하거나 차량의 위치를 달리하는 등 여러 요소를 고려해야 한다. 또한 공격자의 차량위치에 고압전선이 지나가거나 고출력 위성송수신기기 등이 있을 경우 고려해야 할 요소는 더 많아진다. 그림 1은 대상 무선랜에 따라 사용할 수 있는 안테나들이다. 안테나는 좌측부터 지향성 백파이어 안테나, 고지향성 야기안테나, 무지향성 안테나이다. 지향성 백파이어 안테나의 특징은 전파집신의 범위가 상대적으로 좁아 공격자가 원하는 방향의 전파만을 수신할 수 있다. 따라서 대상 무선랜에 대한 대략의 위치가 파악되거나 특정 방향 혹은 건물의 특정 층에 대한 무선랜을 공격할 경우 주로 사용된다.

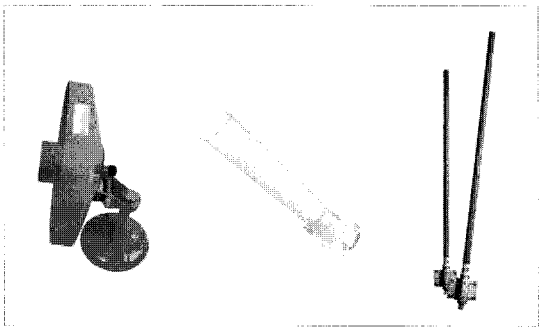

그림 1. 워드라이빙에 사용되는 무선랜 안테나
Fig. 1 WLAN antenna for wardriving

고지향성 야기안테나는 전파집신 범위가 매우 좁기 때문에 방향에 따라 신호 수신률의 차이가 크지만 공격

자가 원하는 하나의 전파를 수신하기에 매우 적합하고 주변 신호잡음의 영향을 매우 적게 받는다. 따라서 대상 무선랜에 대한 정확한 위치가 파악될 경우 사용하기 적합하다. 또한 고지향성 안테나는 노이즈의 영향을 적게 받기 때문에 대상 무선랜과 공격자 사이에 고압전선이나 신호잡음원이 존재할 경우 신호잡음원 사이의 공간을 통해 전파를 수신하기에도 적합하다. 반면 무지향성 안테나의 경우 앞서 기술한 두 가지 안테나와는 정 반대의 특성을 보이는데 무지향성 안테나는 안테나의 위치나 방향에 영향을 전혀 받지않고 상하좌우 및 전후의 모든 방향에 존재하는 무선랜 신호를 수신하기에 적합하다. 따라서 공격자가 임의의 네트워크에 접속하는 것 자체를 목적으로 할 때 적합하다.[7]

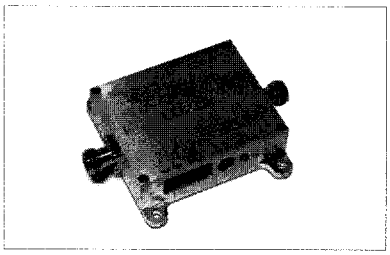

그림 2. 신호증폭기
Fig. 2 A signal amplifie

한편, 무선랜 공격의 거리범위를 넓히고자 한다면 신호증폭기를 이용하여야 한다. 그림2는 1W 신호증폭기를 나타내는데 이를 이용하면 무선신호를 집신하는 무선랜 안테나에 인가되는 전원의 전류량을 높이고 무선신호의 신호세기를 증폭하여 무선랜 어댑터로 전달할 수 있어서 상대적으로 원거리에 위치한 무선랜의 신호를 수신할 수 있다.

2.5 실제 무선랜 공격과정

앞서 기술한 여러 요소가 고려되고 무선랜에 대한 공격이 준비되었을 때 공격과정은 다음과 같다. 첫째. 대상 무선랜의 AP에 대한 정확한 정보를 파악하여야 한다. AP가 암호알고리즘을 이용하거나 RADIUS 인증서버를 사용할 경우 또는 MAC어드레스를 통한 인증을 사용할 경우에 따라 공격방법을 달리 선택해야 하기 때문이다. 대상 AP의 정확한 정보를 파악하기 위하여 리눅스에서는 그림 3과 같이 Kismet 이라는 유틸리티를 일반적으로 사용한다. 둘째. 공격자의 입장에서 침투를 원하는 대상 무선랜이 별도의 인증이나 암호화 기능이 동작하지 않는다면 보편적인 방법으로 무선 AP에 접속하여 해당 네트워크를 점유하는 것으로 공격이 성공한다. 그러나 대상 무선랜의 암호화 기능이 동작한다면 해당 암호기법을 우회하기 위해 WEP 키스트림을 Crack 하거나 WPA 암호를 사전대입하여야 한다. 뿐만 아니라 외부 인증 서버가 있는 경우 앞서 기술한바와 같이 Rogue AP 등을 준비하여 인증서버를 우회하여야 한다.

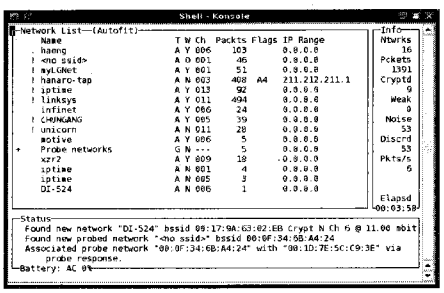

그림 3. 무선랜 탐색 프로그램
Fig. 3 A program searching for WLAN AP

본 논문에서는 WEP 키스트림의 Crack을 기준으로 기술한다. WEP 키스트림을 Crack 하기 위해서는 무선 전파를 통해 전송되는 신호를 우선 Dump 하여야 한다. 무선 신호를 Dump할 때는 주로 그림 4와 같은 리눅스 기반의 Airodump 유틸리티를 많이 이용한다.

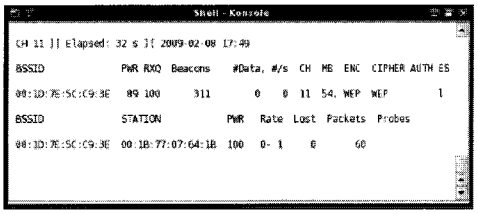

그림 4. 무선신호 Dump 유틸리티 Airodump
Fig. 4 Airodump utility for wireless signal dump

셋째. 공격자는 대상 무선랜의 취약한 IV를 모으기 위해서 대상 무선랜에 접속한 사용자의 접속을 인위적으로 방해하여 재접속을 유도할 필요가 있다. 취약 IV는 무선랜 접속의 인증과정에서 가장 많이 발생하고 무선랜에 접속되어 사용되는 과정에서는 인증과정이 발생하

지 않기 때문에 공격자는 사용자의 재접속을 유도하여 취약 IV를 단시간 내에 모을 수 있다. 무선 접속을 인위적으로 방해하는 유틸리티는 주로 그림 5와 같은 리눅스 기반의 Aireplay를 이용한다. 넷째. 정상적으로 IV 패킷이 Airodump에 의하여 모아지고 있다면 Airodump의 화면출력 상에 Data 필드의 값이 상승하게 된다. 과거의 WEP 키스트림을 Crack하는 알고리즘의 경우 IV 패킷을 추출하는 과정이 복잡하여 수십~수백만개의 무선 패킷을 Dump 해야 하였지만 최근의 알고리즘은 매우 효율적이어서 4만여 개의 무선패킷만 Dump 되면 Crack을 할 수 있다.

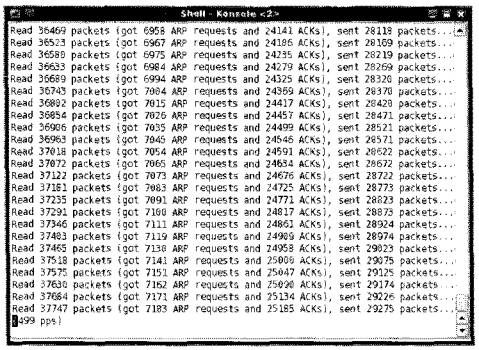

그림 5. 무선랜 접속 방해 Aireplay 유틸리티
Fig. 5 Aireplay utility for injection and fake identification

앞서 기술한 과정을 통해 취약한 무선 패킷이 Dump 되었다면 Dump 된 패킷을 Crack 하여야 한다. WEP 키스트림을 Crack 하기 위해서는 공개된 알고리즘을 이용해 직접 Source Code를 작성하여도 되지만 오픈소스로 공개된 유틸리티를 이용하면 편리하게 Crack 할 수 있다. WEP 키스트림을 Crack 하기위한 유틸리티로는 그림 6과 같은 리눅스 기반의 Aircrack을 이용하면 된다.

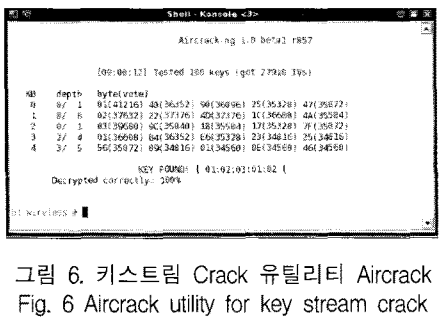

그림 6. 키스트림 Crack 유틸리티 Aircrack
Fig. 6 Aircrack utility for key stream crack

Ⅲ. 워드라이빙을 위한 장비제작과 실험결과

현재까지의 무선랜 워드라이빙 방법은 공격자의 행동을 다른 사람이 매우 쉽게 판별할 수 있고, 공격대상으로부터 가까운 거리에서 공격을 진행하므로 공격자들의 행동에 매우 제약이 있었다. 그러나 이러한 한계를 극복하기위해 많은 공격자들은 무선랜 전파의 비거리 향상을 위해 앞서 기술한 차량의 구조를 개조하거나 고성능의 안테나를 이용하게 된다. 최근에는 모바일 기기나 임베디드 기기를 적극 활용하여 무선랜을 공격하고 있다. 그림 7은 무선랜 해킹장비로 사용할 수 있도록 Linksys社의 WRT-54G의 제품을 개조하여 제작한 것이다. WRT-54G의 펌웨어로 리눅스 기반의 운영체제를 이용할 수 있다는 점을 활용하여 SD카드 메모리를 통해 무선랜 신호를 캡쳐하고, 캡쳐된 패킷은 WEP 키스트림을 크랙하는 등에 이용할 수 있도록 하였다.

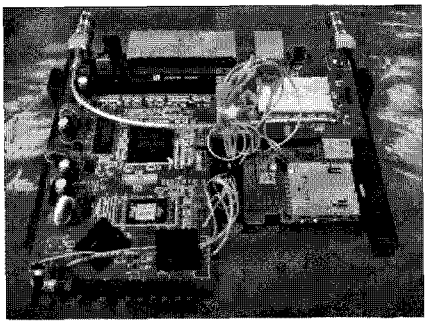

그림 7. 워드라이빙을 위해 제작한 장비
Fig. 7 An apparatus made for wardriving

그림 7과 같이 무선랜 공유기나 Host 모드로 동작하는 무선랜 어댑터가 내장된 임베디드 기기는 그 크기가 매우 작고, 차량 내부에 매립하기도 용이하기 때문에 소형화와 위장이 쉬워 무선랜 네트워크에 매우 위협적이다. 뿐만 아니라 기기 자체의 동작보다는 기기를 경유해서 PDA단말 등의 또 다른 모바일 단말을 통해 공격자가 쉽게 조작할 수 있다는 것이 또한 위험요소로 작용된다.

그림 8은 개조된 WRT-54G를 이용할 때 설정할 수 있는 원격 터미널 설정 항목의 화면이다. 그림 9에 나타난 바와 같이 개조된 WRT-54G를 이용할 경우 일반 x86기반의 시스템처럼 원격 터미널 상에서 리눅스의 모든 작

업을 수행할 수 있으므로, 차량에 매립하여 공격자의 행위를 숨기기에 용이할 뿐만 아니라 수월한 공격 형태를 취하기에 매우 적합하다. 그림 9는 원격 터미널 설정을 한 뒤 터미널 에뮬레이터를 통해 WRT-54G를 작동한 화면이다. 개조된 WRT-54G에서 사용자의 명령입력은 원격 SSH나 TELNET 프로토콜을 통해 처리되고, 화면출력도 입력과 동일한 프로토콜을 통해 처리된다. 내부 무선 어댑터로는 Broadcom 社의 무선 칩셋이나 Atheros社의 칩셋이 이용되고, 무선어댑터에서 수신한 패킷의 덤프를 저장하기 위해 외부 스토리지로 SD/MMC카드를 이용할 수 있도록 제작되었다.

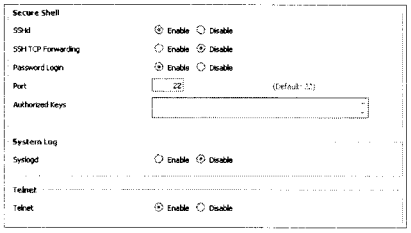

그림 8. 터미널 접속설정
Fig. 8 Terminal configuration

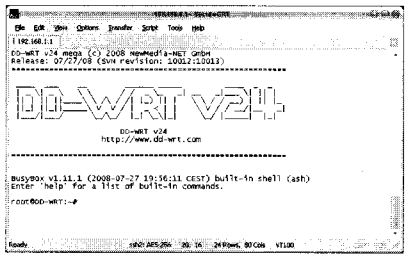

그림 9. 터미널 에뮬레이터
Fig. 9 terminal emulator

앞서 기술한 과정을 통해 공격이 성공적으로 이루어지면 WEP 키스트림을 Crack 함으로서 보안설정이 되어 있는 무선랜 AP를 공격자가 점유할 수 있다. 그림 10은 제작된 장비를 사용하여 앞서 기술한 과정을 통해 WEP 키스트림을 Crack 하거나 보안설정이 되어있지 않아 공격자가 직접 접근가능한 무선랜 AP의 분포도를 실제 지도에 표시한 것이다. 각 무선랜 AP는 정확한 위치나 고도를 파악하기에는 무리가 있으나 무선랜 신호세기와 지향성 안테나를 이용한 방향 측정을 통해 대략의 위치를 파악할 수 있다. 보다 정확한 위치를 파악하기 위해서는 PC에 사용할 수 있는 GPS 모듈을 이용하여야 한다. GPS 모듈을 이용하면 신호의 세기와 GPS 정보를 결합하여 더 세밀한 정보와 정확한 위치를 파악할 수 있다.

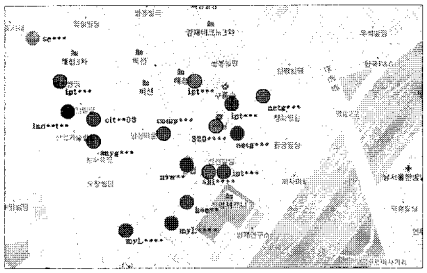

그림 10. 공격가능 AP 분포도
Fig. 10 An attackable AP distribution map

또한, x86 기반의 CPU는 현재 매우 저가에 생산되고 있고 윈도우즈뿐만 아니라 리눅스나 BSD와 같은 다양한 운영체제를 수용할 수 있으며, 컴퓨터 크기는 매우 작아지고 있다. 이러한 추세로 미루어 보아 x86기반의 컴퓨터 자체가 차량에 내장될 가능성이 점쳐지고 있어 무선랜 워드라이빙 방식은 획기적으로 변화될 것으로 판단된다. 현재의 모바일 및 임베디드 기기들은 x86기반의 CPU가 아니기 때문에 무선랜 해킹에 사용되는 각종 어플리케이션 툴들이 리눅스와 오픈소스 OS를 기반으로 개발된다는 점에서 소스코드를 컴파일하는데 어려움이 있었다. 그러나 모바일 CPU 기반의 기기들이 x86 기반으로 변화되어 차량에 매립된다면 리눅스에서 사용하는 소스코드를 별도의 수정이나 플랫폼의 변경 없이 원하는 때에 컴파일하여 이용할 수 있게 된다.[8]

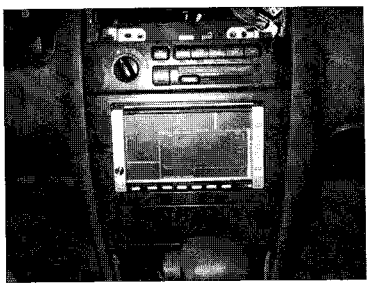

그림 11. x86플랫폼 카PC
Fig. 11 x86 flatform based car PC

그림 11은 이러한 x86 기반의 CPU를 사용하여 만들어진 카PC 장비이다. 카PC는 x86 기반의 CPU를 이용함으로서 윈도우즈, 리눅스, BSD등의 오픈소스 운영체제 및 유닉스 운영체제 등 다양한 플랫폼의 이종전환이 가능하다. x86 기반의 카PC가 저렴해지고 보급화되면 무선랜 해킹추이는 차량과 무선랜, 전파간섭등의 전문지식이 없는 일반인들도 쉽게 접할 수 있는 환경이 될 것으로 예상된다.

Ⅳ. 무선랜 워드라이빙의 대처방안

1. 일반적인 대처방안

무선랜 워드라이빙은 1차적인 네트워크 점유에 대한 위험뿐만 아니라 2차적인 네트워크의 공격까지 그 위험범위가 굉장히 넓다. 따라서 무선랜 네트워크의 관리자는 이러한 공격의 위험성을 미리 파악하고 특성을 확인하여 종합적인 관리대책과 정책을 수립할 필요성이 있다. 무선랜 워드라이빙으로부터 무선랜 네트워크를 안전하기 보호하기 위해 다음과 같은 항목을 확인할 필요가 있다.

① 사용자 네트워크에서 무선랜이 필요한지 고민한다. 만일 사용하고 있는 네트워크에서 무선랜의 사용을 하지 않거나 사용빈도가 극히 낮다면 이런 네트워크 연결방식을 유선으로 전환할 것을 고려해야 한다. 데스크탑 PC등의 고정식 호스트를 이용하는 환경에서 네트워크 시공단가를 낮추기 위해 무선랜을 이용하는경우가 많은데 보안상의 문제는 유선 이더넷 방식이 아직까지 안전하다는 점을 상기해야 한다.

② 무선 AP는 방화벽 외부 네트워크에 위치시킨다. 불가피하게 무선랜 네트워크를 이용해야하는 상황이라면 무선 AP를 방화벽 외부 네트워크에서 동작하도록 시공하는 것이 좋다. 무선랜 AP나 인증서버가 무선랜 공격으로 인해 공격자에게 점유되더라도 내부네트워크에 대한 2차 침해를 예방할 수 있다.

③ 중앙집중식 인증서버(RADIUS)를 구축한다. RADIUS 환경에서는 별도의 인증서버를 이용하게 되므로, 공격자가 무선랜 네트워크의 Key 스트림을 해석하여 접근에 성공하여도 인증을 거치지 않으면 내부네트워크의 자원을 사용할 수 없기 때문에 보안상 효과적이다.

④ 재정적인 여유가 된다면 W-IPS를 도입한다. 아직 국내에 시판중인 W-IPS는 패킷 Replay를 탐지하여 효과적으로 차단하지 못한다. 그러나 W-IPS를 이용하면 앞서 기술한 Rogue AP를 효과적으로 탐지할 수 있다. 일반적인 Station 탐색으로는 이러한 Rogue AP를 탐색하기 어려우며 통제할 수 없는 AP에 대한 효과적인 모니터링에 이용할 수 있다.

⑤ 인력적인 여유가 된다면 지속적으로 모니터링한다. 회사 네트워크와 같이 중요자원이 네트워크에 존재하는 경우 인력적인 여유가 된다면 잉여 네트워크 IP 자원이 어떤 무선랜 Station에서 사용되고 있는지를 지속적으로 모니터링할 필요가 있다.

2. 네트워크 시공단계에서의 예방적 대처방안

일반적인 방법이 소극적인 무선랜 워드라이빙의 대처방안이라면 네트워크 시공단계에서 예방적인 대처방안이 가능하다. 많은 사무실 건물들은 사무실의 시공단가, 단열측면, 전기배선 등을 고려하여 샌드위치패널을 많이 이용하고 있는데, 이 패널은 철근콘크리트구조의 일반적인 건물보다 무선전파의 투과율이 높아 무선랜 Station의 탐색이 용이하다.

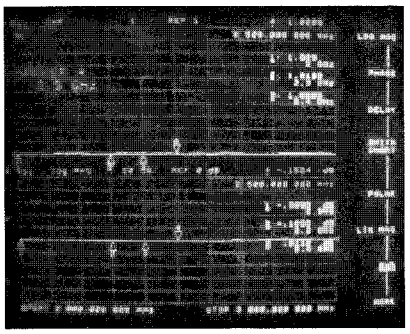

그림 12. 샌드위치패널의 RF 스펙트럼
Fig. 12 RF spectrum of sandwich panel

그림 12의 전파신호 스펙트럼에서 보듯이 샌드위치패널에서는 전파장과 전파수신 안정도율이 1:1로 매우 안정되게 수신되고 있는 것을 확인할 수 있다. 따라서 업무상 민감한 자료를 다루는 내부네트워크에서 무선랜을 불가피하게 이용해야 하는 회사라면 건물의 시공 및 준공단계에서부터 무선랜의 보안에 대한 예방적인 측면에서의 시공이 필요하다.

V. 결 론

본 논문에서는 최근 새로운 보안위협으로 부상 중인 무선랜 워드라이빙 공격과 발전된 형태의 공격방법 및 향후추이 그리고 이에 대한 대처방안을 살펴보았다. 이를 위해 무선 랜에서의 워드라이빙 공격에 적합한 장비를 제작하였고, 제작된 장비를 사용하여 서울시 양재동 일대의 무선 랜 AP 보안 취약성을 조사하였다. 워드라이빙의 기술과 대처방안을 살펴보면 무선랜 네트워크의 경우 유선 이더넷의 네트워크 환경보다 접근성에서 우수하지만 우수한 접근성에 따른 위험도 역시 비약적으로 증가한다는 것을 알 수 있다. 무선랜 네트워크는 접근성이 높아 기존의 네트워크 보안개념에서 적용하던 보안기술이 적용되지 않는 경우가 많다. 따라서 예방적인 차원과 전파통신의 구조적인 방법으로 보안을 하는 것이 필요하며, 네트워크 사용자의 잘못된 네트워크 사용을 면밀히 분석하고 판단하는 정책적 세심함이 필요하다. 네트워크가 구축된 후에는 전파통신의 구조적인 방법으로 접근하기 어렵기 때문에 시공 및 준공단계에서부터 무선랜 네트워크의 필요성과 향후 대책을 면밀히 검토하는 것이 반드시 필요할 것으로 판단된다.

참고문헌

[1] Duggan. J., "Threats to the Mobile Enterprise: Jurisprudence Analysis of Wardriving and Warchalking", International conference on information techmology, Vol.5 No.2 pp. 268-273, Apr., 2004.

[2] Mike Loukides, Colleen Gorman, "Security Power Tools", 1, pp. 101-129, pp. 225-241, Aug 2007.

[3] Mike Loukides, "802.11 Wireless Networks: The Definitive Guide", 2, pp. 114-238, Apr 2005.

[4] Duggan. J., "Wardriving around Campus: Assessing the security of selected campus WLANs", ed media proceedings 2004, Vol. 1, pp. 44-49., 2004.

[5] Sathu, H., "WarDriving Dilemmas", conference of the national advisory committee on computing qualifications, Vol. 1, pp. 237-242, Jul., 2006.

[6] Mark Silberstein, "High Performance Computing on GPUs using NVIDIA CUDA", Slides include some material from GPGPU tutorial at SIGGRAPH2007, 1, pp. 4-34, 2007.

[7] 유장환, "동축케이블 손실에 따른 안테나 성능비교", http://cafe.naver.com/rfeng

[8] 최영남(2008), "A change of war-driving trend",

저자소개

최영남(Young-Nam Choi)

2008년 8월 - 현재 (주)터보테크 기술연구소 연구원
2009년 현재 동명대학교 정보통신공학과재학

※관심분야 : 무선망 보안 시스템, 하드웨어 어플라이언스 보안

조성목(Sung-Mok Cho)

1988년 2월 경북대학교 전자공학과 (공학사)
1990년 2월 경북대학교 대학원 전자과(공학석사)
1995년 2월 경북대학교 대학원 전자과(공학박사)
2006년 3월 - 현재 동명대학교 정보보호학과 부교수

※관심분야 : 보안통제 시스템, 무선 네트워크 보안 영상처리