WiBro 서비스를 이용한 응용프로그램의 취약점 분석 및 보안 대책 연구

천우성* · 박대우**

A Study of Security Measures and Vulnerability Analysis on the Application using
WiBro Service

Woo-Sung Chun* · Dea-Woo Park**

요 약

WiBro(Wireless Broadband)서비스는 우리나라에서 세계표준화한 4세대 통신이다. WiBro 통신기반을 사용한 인터넷기반 응용프로그램을 통한 서비스이용이 늘어나고 있다. WiBro 서비스에서 인터넷기반 응용프로그램으로 서비스 이용할 때, 응용프로그램의 취약점을 분석할 필요가 있다. 본 논문에서는 WiBro 서비스에서 인터넷을 이용할 때 취약점을 분석하고, 인터넷기반 응용프로그램에 대한 해킹공격이 발생할 수 있는 취약점을 분석한다. WiBro 서비스와 응용프로그램의 취약점 분석을 통해 보안대책을 연구한다.

ABSTRACT

WiBro(Wireless Broadband) service is the world standardized fourth-generation communications in Korea. The services through internet-based applications using WiBro communication-based is increasing. WiBro service in the Internet-based applications when using the service, the application may need to analyze the vulnerability. In this paper, we use the Internet when in WiBro service, to analyze the vulnerability. And, Internet-based applications for vulnerabilities that could lead to hacker attacks is analyzed. It will be studied that security measures through analysis of vulnerability of WiBro services and applications.

키워드

와이브로, 인터넷기반 응용프로그램, 취약점, 해킹 공격, 보안대책

Key word

WiBro, Internet-based Applications, Vulnerability, Hacking Attacks, Security Measures

* 정회원 : 호서대학교 벤처전문대학원(제1저자)

** 종신회원 : 호서대학교 벤처전문대학원(교신저자, prof_pdw@naver.com)

접수일자 : 2012. 06. 01

심사완료일자 : 2012. 06. 01

I. 서 론

WiBro(Wireless Broadband Internet)는 2006년에 정보통신부 주도로 개발한 이동통신 기술로 인구밀집 지역에 고속·대용량 데이터를 전송하면서 음성서비스를 부가적으로 제공한다. 4세대 WiBro는 3세대 WiBro에서 진화한 기술로 유럽이 주도하는 LTE(롱텀에볼루션) 기술에 비해 6배 빠른 전송속도를 구현한다. '와이브로 어드밴스드(WiBro-Adv)'를 지칭한다.

정부는 유럽 주도의 LTE가 세계 시장의 대세이지만 WiBro도 LTE의 보완망으로 오는 2015년 세계 시장의 10~20%에 이르는 수요가 있을 것으로 예상하고 있다.

특히 우리나라 중소·중견 기업들이 WiBro 장비의 생태계를 형성하고 있어 WiBro를 적극 육성할 필요가 있다는 것이 정부의 인식이다[1].

WiBro는 IEEE 802.16e 국제표준으로 이동 단말기를 이용하여, 정지 및 자동차로 이동 중에도 고속으로 무선 인터넷과 금융업무가 가능한 서비스이다. 본 연구는 WiBro 서비스의 인터넷 이용에 사용되는 애플리케이션에 대한 해커의 공격(DoS/DDoS, 피싱(Phishing), 바이러스, 악성코드, 개인정보 자료 해킹 등)을 실시하고, 서비스 취약점 분석과 공격에 대한 정보의 침해, 재산 피해 등을 분석한다.

II. 관련연구

2.1. WiBro

WiBro는 2.3 GHz 대역의 주파수를 이용하며, 시속 60 km 이상의 이동성과 1 Mbps급의 전송속도를 제공하는 휴대 인터넷 서비스를 가리킨다. WiBro의 전파 전달 거리는 최대 48 km에 달함으로써, 핫스팟이라는 서비스 지역에서만 사용이 가능한 무선 랜, Wi-Fi 보다 서비스 반경이 10배 이상 넓다.

한국 기업들이 중심이 되어 개발한 WiBro 기술 표준 HPI(High-speed Portable internet)는 IEEE가 승인한 차세대 무선 광대역 전송 기술 표준 IEEE 802.16e에 부합되는 국제 기술 표준이다.

2.2. WiBro의 구성

WiBro망은 단말기(PSS), 기지국(RAS), 제어국(ACR)으로 이루어져 있다.

사업자 별로 휴대 인터넷 사용자의 인증을 위한 AAA(Authentication, Authorization, Accounting)서버, IP 이동성 제어를 위한 Home Agent 등이 구축 가능하다[2].

① 제어국(Access Control Router : ACR)

- IP 라우팅, 이동성 관리
- 인증/보안, QoS, 멀티캐스트
- 과금, 통계생성
- RAS간 이동성 제어/자원관리

② 기지국(Radio Access Station : RAS)

- 802.16e 규격 무선접속
- 무선자원 관리/제어
- 이동성, 연결제어
- QoS, 하향링크 멀티캐스트

③ 단말기(Portable Subscriber Station : PSS)

- 무선 접속
- IP기반 서비스접속/이동성
- 단말 인증/사용자 인증/보안
- 타 망과의 연동

2.3. 애플리케이션

정보기술에서 말하는 애플리케이션이란, 기술, 시스템 및 제품 등을 사용하는 것을 말한다.

응용프로그램은 사용자 또는 다른 응용프로그램에게, 특정한 기능을 직접 수행하도록 설계된 프로그램이다. 응용프로그램의 예로는 워드프로세서, 데이터베이스 프로그램, 웹브라우저, 개발 도구, 페인트 브러시, 이미지 편집 프로그램, 통신 프로그램 등이 있다. 응용프로그램은 컴퓨터의 운영체제와 여러가지 다른 지원프로그램들의 서비스를 사용한다. 응용프로그램이 다른 프로그램에 공식적으로 작업을 요청하거나 통신하는 수단으로 사용되는 것을 API라고 부른다.

III. WiBro 서비스를 이용한 응용 프로그램의 취약점 분석

3.1. WiBro 서비스 보안 취약점

WiBro 서비스에서 발생할 수 있는 취약점 중에서 무선 구간에서 발생 가능한 취약점을 가지고 있다[3][4]. 실제 사용자가 서비스를 제공 받는 과정에서 일어날 수 있는 것이며, 대응방안을 고려해야 한다. WiBro 기술은 기술적인 특징을 기반으로 Physical Layer와 MAC Layer의 취약점을 구분하여 표 1과 같이 정리 할 수 있다[5][6].

표 1. WiBro 기술적 취약점 분류
Table. 1 Technical Vulnerability Classification of WiBro

PHY Layer	MAC Layer
<ul style="list-style-type: none"> · Dos형태의 공격이 가능함 · Jamming attack, Scrambling attack - 소음을 발생시켜 전파 방해 하는 공격 · Water torture attack : 휴대용 장치의 한정된 자원을 사용하지 못하도록 함 · 기타: 위조 공격, 재생공격 가능 적법한 송수신자의 채널을 무선 환경에서 공격자가 사용가능 	<ul style="list-style-type: none"> · 단말기와 기지국의 초기 연결 시 사용하는 메시지의 노출 위험성 · 휴 간 이동 시 각 네트워크 접근에 대한 보안 취약성 · 인증 취약점 (가장의 위험, 중간자 공격 가능)

3.2. 인터넷 서비스 취약점

WiBro AP를 검색하여 찾은 WiBro AP의 정보를 가지고 동일한 이름의 WiBro AP를 만들어 사용자 접속하도록 한다. 그림 1은 Google 사이트에 접속하는 화면이다.

무선의 특성상 SSID를 사용자가 임의로 숨기지 않는 이상 AP를 검색하는데 제약이 없어 사용자는 암호가 설정되어 있지 않은 AP에 쉽게 접속한다. 사용자가 특정 사이트 주소 입력할 경우, 가짜로 만든 사이트로 접속을 하게 설정한다.

그림 1. Google 접속
Fig. 1 Google login screen

사용자는 정상적으로 접속하였다고 생각하지만 사실은 사용자가 접속하려는 사이트와 똑같은 가짜 사이트에 접속을 하게 된다. 그리고 사용자는 ID와 Password를 입력하게 된다. 사용자의 ID와 Password의 정보를 받아오고 사용자가 접속한 사이트의 로그인과정을 거치지 않고 실제 사용자가 접속하려던 사이트로 접속하게 한다. 이때 사용자는 “새로고침”으로 사이트에 다시 접속할줄 알고 ID와 Password를 다시 입력하여 정상 사용을 하게 된다. 또한 Sniffing을 통해 접속당시 Packet을 분석하여 ID와 Password를 알아낸다. 그림 2는 Cain & Abel을 통해 Google 사이트 접속 시 사용자의 ID와 Password를 Sniffing한 화면이다.

그림 2. Google 접속 시 ID와 Password Sniffing
Fig. 2 Sniffing of ID and Password in Google Access

3.3. 서비스 거부 공격 취약점

DoS공격은 특정 IP에 대량의 Packet을 일순간에 보내어 네트워크 트래픽이 증가하여 정상적인 서비스를 마비시키는 것이며, DoS공격을 우회 경로를 통해 Zombie 시스템에 심어 놓고, 한 번에 같은 곳을 공격하는 것이 DDoS공격이다.

그림 3. DoS v5.5 Final 프로그램
Fig. 3 DoS v5.5 Final Program

그림 4. DoS Packet 분석
Fig. 4 Analysis of DoS Packet

그림 3과 같이 공격 대상 단말의 IP Address (192.168.1.100)로 DoS v5.5 Final 프로그램을 이용하여 80port를 통하여 초당 12,000Byte로 공격 하였으며, 그림 4와 같이 Wireshark를 통해 DoS Packet을 분석하였고, 그 영향으로 공격 대상단말은 트래픽의 증가로 인해 서비스의 지체 현상을 볼 수 있었다.

IV. WiBro 서비스를 이용한 응용 프로그램의 보안 대책

4.1. 인터넷 서비스 보안 대책

사용자가 WiBro로 인터넷 서비스 이용 할 경우, 해커가 만든 가짜 사이트로 사용자가 접속되도록 유도하는 방법을 사용한다. 해커는 특정 회사의 근처에서 WiBro를 검색하고, 그 회사에서 사용하고 있는 무선AP의 이름을 확인한다. 그리고 동일한 이름의 무선AP를 만들어 사용자가 접속하도록 유인하여 정보를 빼내게 된다. 무선랜의 특성상 무선 AP의 이름에 대한 제약이 없어, 사용자는 쉽게 가짜 무선 AP에 접속하는데, 이때 사용자가 특정 사이트 주소를 입력할 경우, 해커가 만든 사이트로 접속하게 된다.

접속된 무선AP는 해커의 게이트웨이를 통해, 해커가 지칭한 사이트로 연결하는 것이다. 그리고 사용자가 가짜 사이트에서 로그인 ID와 Password를 입력하면 이 정보들이 해커의 컴퓨터에 저장된다. 이와 같이 가짜 무선 AP를 통하여 사용자의 ID와 Password를 알아내어 E-mail이나 MMS 서비스를 사용할 수 있게 된다.

로그인시 SSL(Secure Sockets Layer)을 적용시켜야 한다. SSL 적용 시 로그인 정보를 암호화해서 보내므로 회원들의 계정이나 기타 정보를 보호해줄 수 있다. 그림 5는 SSL을 적용한 사이트에 대한 Sniffing 실험 결과이다.

SSL을 적용하였을 때, Cain & Abel로 분석을 통해 ID와 Password가 나타나지 않는 것을 확인하였다.

Protocol	Time	Source	Destination	Length	Info
HTTP	0.000000	192.168.1.105	192.168.1.1	1024	GET / HTTP/1.1
DNS	0.000000	192.168.1.105	192.168.1.1	1024	Standard query type A
SSL/TLS	0.000000	192.168.1.105	192.168.1.1	1024	Handshake

그림 5. SSL 적용 사이트의 Sniffing 결과
Fig. 5 Sniffing Results of SSL applying Site

4.2. PKMv2 인증

WiBro에서는 PKMv2를 통해 망 접속을 위한 단말 및 네트워크 간 양방향 인증, 암호화된 데이터 통신에 사용될 TEK(데이터 암호화 키) 교환이 가능하다.

WiBro 표준에서는 무선네트워크에서의 단말과의 안전한 통신을 위한 인증 및 기밀성을 제공하기 위해 보안 부계층(Security Sublayer)을 정의하고 있으며, 보안 부계층 내 PKM을 정의한다. 현재 PKM은 버전 2를 사용하고 있으며, 인증 방식으로 RSA인증 방식과 EAP인증 방식의 다른 메커니즘을 사용할 수 있다. 두 가지 인증 방식 중 한가지를 선택하여 사용하거나, 두 가지 모두 사용할 수 있다.

4.3. EAP 인증방식

PKM EAP (Extensible Authentication Protocol) 인증방식은 IEEE802.1x 포트기반의 가입자 인증데이터 전송을 위한 표준 프로토콜로 EAP-MD5, EAP-TLS, EAP-AKA (Authentication and Key Agreement) 등 다양한 인증 프로토콜을 사용할 수 있으며, 사용자 인증 및 단말, 그리고 네트워크 간 상호인증이 가능하다. 또한 AAA 인증 서버를 통해 인증을 수행하기 때문에 사용자가 증가해도 기지국에 오버헤드가 생기지 않는다는 장점이 있다.

현재 PKMv2 EAP 기반 인증방식에 AKA 메커니즘을

적용한 EAP-AKA 인증방식으로 표준 및 사용화를 추진 중에 있다. EAP-AKA 인증방식은 현재 3GPP와 무선 랜 간의 연동 시 끊임 없는 서비스제공을 위해 필요한 보안 인증 프로토콜로 3GPP에서 제안한 상황이다. EAP-AKA의 경우 사전에 키를 공유하는 방식을 사용하여 인증을 하므로 키 노출에 대한 위험을 가지고 있다. 그러나 EAP-TLS의 경우 RSA인증 방식과 같이 X.509인증서를 사용하여 인증을 수행하므로, 이러한 위험요소를 갖지 않는다.

V. 결 론

한국이 국제표준으로 개발한 IEEE 802.16e를 사용하는 WiBro 서비스에서 애플리케이션으로 인터넷 서비스를 사용에서 취약점을 분석하여 공격을 실시하였다. 고도정보화사회의 역기능으로 발생한 해커의 시스템이나 바이러스를 통한 정보 탈취 및 피해, DoS/DDoS 공격을 통한 WiBro 시스템 자원을 마비시키는 피해가 발생하는 것을 확인하고, 취약점을 보완하기 위한 보안대책을 제시하였다.

향후연구에서는 WiBro 서비스를 통하여 이루어지는 mVoIP나 게임들에 대한 취약점 연구와 보안대책의 연구가 이루어져야 하겠다.

참고문헌

- [1] 한국인터넷진흥원, “와이브로 보안기술 안내서,” pp.1-158, 2010.
- [2] 김명균, 엄윤성, “WiBro망에서 VoIP를 이용한 그룹 통신 서비스 성능분석,” 한국해양정보통신학회 논문지, 제15권, 제6호, pp.1256-1264, 2011.
- [3] Dea-Woo Park, “A Study of Packet Analysis regarding a DoS Attack in WiBro Environments,” *International Journal of Computer Science and Network Security*, IJCSNS (1738-7906), 2008.
- [4] Woo-Sung Chun, Dea-Woo Park, “Security Vulnerability Analysis and Forensic Data Research to Attacks on Mobile Stock Trading System in WiBro Network,” *International Journal of Computer Science*

and Network Security, vol. 9, no. 12, 2009.

- [5] Dea-Woo Park, "A Study on Real-time Cooperation Protect System Against Hacking Attacks of WiBro Service," *International Journal of Maritime information and Communication Sciences*, vol.9, no.4, pp. 353-357, 2011.
- [6] 김종환, 전홍우, 신경욱, "WiBro 보안용 AES기반의 Key Wrap/Unwrap 코어 설계," *한국해양정보통신학회논문지*, vol.11, no.7, pp.1332-1340, 2007.

저자소개

천우성(Woo-Sung Chun)

2006년 숭실대학교
전산원 졸업
2006년 한국교육개발원
멀티미디어학 전공(공학사)

2009년 호서대학교 벤처전문대학원
IT응용기술학과(공학석사(정보보호전공))
2011년 호서대학교 벤처전문대학원
IT응용기술학과(박사과정)
※ 관심분야: 정보보호, 네트워크 보안, WiBro 보안,
추적기법, 포렌식

박대우(Dea-Woo Park)

1998년 숭실대학교
컴퓨터학과(공학석사)
2004년 숭실대학교
컴퓨터학과(공학박사)

2006년 정보보호진흥원(KISA) 선임연구원
2007년~현재 호서대학교 벤처전문대학원 조교수
※ 관심분야: 정보보호, 유비쿼터스 네트워크 및 보안,
보안 시스템, CERT/CC, e-Discovery, Forensic, VoIP
보안, 이동통신 및 WiBro 보안, IT-Convergence,
Cyber Reality 등