WiBro 단말 취약에 대한 보안기술적용 비교분석

천우성* · 박대우*

*호서대학교 벤처전문대학원

Comparative Analysis for Security Technology to WiBro Terminals's Vulnerability

Woo-Sung Chun* · Dea-Woo Park*

*Hoseo Graduate School of Venture

E-mail : deux8522@daum.net · prof_pdw@naver.com

요 약

WiBro는 우리나라에서 세계표준화한 통신기술이다 WiBro를 사용한 무선 인터넷 서비스이용이 늘어나고 있다. WiBro 단말에서 이루어지는 인터넷 서비스는 무선에서 오는 취약점과 인터넷에 취약점을 모두 가지고 있어 취약점에 대한 보안기술이 필요하다본 연구에서는 WiBro 단말의 취약점을 연구하고 취약점에 대한 보안기술을 연구하였다 WiBro 단말의 취약점을 보안하기 위해 보안기술을 적용하여 보안기술 적용 전후를 비교 분석한다

ABSTRACT

WiBro the world is the communication technique which it standardizes from our country. The radio internet service use which uses WiBro is extending. Becomes accomplished from WiBro, terminals the internet service which is having a vulnerability in vulnerability and the Internet which come from the radio and the security technique is necessary in about vulnerability. It researched the vulnerability of WiBro terminals from the research which it sees and it researched a security technique in about vulnerability. To secure the vulnerability of WiBro, in order terminals it applies a security technique and around security technical applying comparison it analyzes.

키워드

WiBro, WiBro 보안기술, 취약점, Hacking

Ⅰ. 서 론

Smart Phone의 급속한 보급과 SNS(Social Network Service)의 활성화로 휴대폰의 활용도가 음성통화보다 데이터의 사용량이 늘어나고 있다 3G(3rd Generation)를 사용했을 때 무제한 데이터 요금제가 있었으나, LTE(Long Term Evolution)로 전환되면서 무제한 요금제가 없어지면서 기존의 3G 무제한 요금제를 사용하던 사용자는 LTE의 적량 데이터 요금제로 바뀌게 되어 휴대폰을 사용하여 데이터를 사용하는데 제약을 받고 있다.

또한, 넷북이나 울트라씬 노트북같이 가볍고 이동성이 용이한 PC(Personal Computer)의 보급과 무료 Wi-Fi의 보급으로 언제 어디서나 인터넷에 접속하여 SNS를 할 수 있게 되었다. 그러나 무료 Wi-Fi를 사용하려면 지정된 장소에서만 사용이 가능하여 이동성에서 용이하지 않다 그래서 사용자들은 이동성이 용이하고 휴대폰의 한정된 데이터요금에 비해 저렴하고 많은 데이터를 제공해 주는 WiBro 단말을 많이 사용하고 있다.

WiBro는 우리나라에서 세계표준화한 통신기술로 KT와 SKT가 사업자로 선정되어 2006년 6월 30일부터 상용화 서비스를 시작하였고 2007년 10월 국제전기통신연합(ITU)에서 3G 이동통신의 6번째 기술 표준으로 채택된 바 있다.

2012년 9월 데일리시큐의 기사에 따르면 모바일 디바이스에 Wi-Fi를 지원하는 WiBro Egg 제품에 취약점이 발견됐다. 이 취약점으로 인해 악의적인 공격자는 관리자 로그인 없이 설정변경이 가능한 것으로 나타났다[1].

WiBro 단말에서 이루어지는 인터넷 서비스는 무선에서 오는 취약점과 인터넷에 취약점을 모두 가지고 있어 취약점에 대한 보안기술이 필요하다.

본 연구에서는 WiBro 단말의 취약점을 연구하고 취약점에 대한 보안기술을 연구하였다. WiBro 단말의 취약점을 보안하기 위해 보안기술을 적용하여 보안기술 적용 전후를 비교 분석하고자 한다.

II. 관련연구

2.1 WiBro 취약점

무선 인터넷을 사용하기 위해서 AP(Acess Point)를 검색하는데 이때 SSID(Service set identification) 정보를 통하여 AP에 접속하여 인터넷을 사용하게 된다. 이때 사용자가 임의로 SSID를 마스킹하지 않으면 AP를 검색하는데 제약이 없어 사용자는 암호가 설정되어 있지 않은 AP에 쉽게 접속할 수 있다. WiBro AP를 검색하여 AP의 정보를 알아내어 동일한 SSID의 WiBro AP를 공격자가 만들어 사용자 접속하도록 설정을 한다. 사용자가 암호가 설정되어 있지 않은 AP에 접속하여 인터넷을 통하여 특정 사이트 주소 입력할 경우, 가짜로 만든 사이트로 접속을 하게 만들 수 있다[2].

사용자는 정상적으로 사이트에 접속하였다고 생각하지만 사실은 사용자가 접속하려는 사이트와 똑같이 만든 가짜 사이트에 접속을 하게 되는 것이다. 그리고 사용자는 ID와 Password를 입력하면 ID와 Password의 정보를 받아오고 사용자가 접속한 사이트의 로그인과정을 거치지 않고 실제 사용자가 접속하려던 사이트로 접속하게 한다. 이때 사용자는 “새로고침”으로 사이트에 다시 접속한줄 알고 ID와 Password를 다시 입력하여 정상 사용을 하게 된다[3].

2.2 WiBro Hacking 공격

• 바이러스(Virus)

컴퓨터 프로그램이나 메모리에 자신 또는 자신의 변형을 복사해 넣는 악의적인 명령어들로 조합하여 불특정 다수에게 피해를 주기 위한 목적으로 제작된 모든 컴퓨터 프로그램 또는 실행 가능한 코드[4]

• 악성프로그램공격

컴퓨터 시스템에 악성프로그램을 설치하게 유도하거나 고의로 감염시키는 해킹기법으로 주로 백 도어 등을 이용하여 상대방의 주요 정보를 빼내기 위한 목적으로 이용함[5]

• 서비스거부공격(DoS : Denial of Service)

특정 네트워크에서 허용하는 대폭을 모두 소모시키거나, 공격대상(victim) 시스템의 자원(CPU, 메모리 등)을 고갈시키거나, 시스템 상에서 동작하는 응용프로그램의 오류에 대한 공격으로 서비스를 못하도록 만드는 공격[6]

• 분산서비스거부공격(DDoS : Distributed DoS)

DoS용 에이전트를 여러 개의 시스템에 설치하고, 이 에이전트를 제어하여 DoS 공격을 함으로써 보다 강력한 공격을 시도할 수 있으며, 공격자에 대한 추적 및 공격트래픽의 차단을 어렵게 만드는 공격 형태[7]

III. WiBro 단말 취약점 연구

3.1 WiBro 단말

WiBro 서비스를 이용하기 위해서 PC에 USB(Universal Serial Bus)로 직접 연결하는 USB 단말과 Egg라는 무선 단말이 있다. USB 단말의 경우 무선에서는 WiMAX : IEEE802.16e-2005로 신호를 받지만 PC 내부에서는 USB 모뎀으로 인식한다. 그래서 PC가 악성코드에 감염되어 있을 경우 사용자의 정보가 유출된다. 또한, Egg의 경우 Egg단말까지는 WiMAX : IEEE802.16e-2005로 통신을 하고 사용자 PC와는 Wi-Fi : IEEE802.11 b/g로 사용자 PC에서 무선인터넷을 설정하여 Egg 단말을 잡는 형식으로 이루어진다. Egg의 경우에는 사용자 PC와 무선으로 접속을 하기 때문에 무선 인터넷의 취약점을 그대로 가지고 있다.

3.2 WiBro 단말 취약점

• PKMv1의 단방향 인증으로 인한 취약성

TTA의 WiBro 표준 문서와 IEEE 의802.16e표준 문서를 보면 키 관리 프로토콜로써 PKMv1(PKM version1)과 PKMv2(PKM version2)를 지원해야 하도록 명시하고 있다. PKMv1은 양방향 인증을 지원 하지 않는 취약점을 지니고 있다.

• UICC(Universal Integrated Circuit Card)칩을 이용한 인증과정에서 생기는 취약성

사용자 입장에서 UICC칩과 그에 따른 PIN은 일종의 아이디와 비밀번호와 같은 것이라 말할 수 있다. 사용자의 편의와 보안성 강화를 위해 사용되는 UICC칩이지만, 사용자의 부주의로 인해 분실 혹은 도난을 당하거나, PIN이 유출 되는 경우에는 단말 도용의 위험을 가진다.

• EAP-AKA(Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement)인증 과장에서의 취약성

EAP-AKA인증 프로토콜 자체에 보안 취약성이 존재하는 것은 아니나, 이를 WiBro 시스템에 적용하는 과정에서 보안 취약성이 발생할 수 있다.

3.3 WiBro 단말 취약점 분석

WiBro 서비스에서 발생할 수 있는 취약점 중에서 무선 구간에서 발생 가능한 취약점은 다음 표와 같다. 실제 사용자가 서비스를 제공 받는 과정에서 일어날 수 있는 것들이며, 대응방안을 고려해야 한다. WiBro 기술은 기술적인 특징을 기반으로 Physical Layer와 MAC Layer의 취약점을 다음과 같이 구분할 수 있다[8].

• PHY(Physical) Layer

·Dos형태의 공격이 가능하다.

·Jamming attack, Scrambling attack

– 소음을 발생시켜 전파 방해 하는 공격이다.

·Water torture attack : 휴대용 장치의 한정된 자원을 사용하지 못하도록 한다.

·기타 : 위조 공격, 재생공격 가능 적법한 송수신자의 채널을 무선 환경에서 공격자가 사용가능하다.

• MAC(Media Access Control) Layer

·단말기와 기지국의 초기 연결 시 사용하는 메시지의 노출 위험성 있다.

·홉 간 이동 시 각 네트워크 접근에 대한 보안 취약성이 있다.

·인증 취약점(가장의 위협, 중간자 공격 가능)이 있다.

Ⅳ. WiBro 단말 취약점에 대한 보안기술적용 비교분석

4.1 WiBro 단말 보안기술

WiBro 기술은 기술적인 특징을 기반으로 Physical Layer와 MAC Layer의 취약점에 대한 보안기술은 다음과 같다.

• PHY Layer

·신호에 대한 파워 또는 대역폭이 증가한다.

·지속적인 모니터링을 통한 비정상 행위를 탐지한다.

·복잡한 메커니즘을 방지하기 위해 사용하지 않는 프레임을 폐기한다.

·배터리 또는 전산 자원의 고갈을 줄인다.

·상호 인증

• MAC Layer

·PKMv2를 기반으로한 AES 암호화 알고리즘을 활용한 데이터 암호화 및 HMAC/CMAC (Hash-based Message Authentication Code/Calculating Message Authentication Code)을 통한 메시지 무결성 인증한다.

·간단하고 효율적인 키 교환 방법인 PKI(Public Key Infrastructure)기법을 통해 해결.

·RSA/X.509인증을 통해 사용자 인증 PKMv2를 통한 사용자 상호 인증(중간자 공격 불가)한다.

4.2 WiBro 단말 보안적용

WiBro를 이용한 인터넷 서비스에서E-mail 서비스나 사이트에 로그인할 경우, SSL(Secure Socket Layer)인증서가 적용되어 사이트의 경우 접속한 사용자의 ID나 Password가 노출되지 않았다. 또한, Egg 단말과 사용자 PC 사이에서 무선 Packet Sniffing으로 노출된 Packet의 경우 PKMv2 인증, EAP 인증을 통하여 Packet이 암호화되어 Sniffing 도구를 통한 분석이 불가능 하였다.

SSID의 경우, 기본적으로 무선 AP를 검색하면 찾을수 있었지만 SSID 마스킹을 통해 사용자 보인만 접속하게 하여 다른 사용자에겐 식별이 불가능하게 하였다.

4.3 보안기술적용 전후 비교분석

표 1과 같이 WiBro 단말의 취약점에 대한 결과와 보안기술을 적용한 결과를 비교분석하였다.

표 1. 보안 기술 적용 분석

WiBro 단말 취약점	결과	보안기술	적용결과
ID, Password	노출	SSL	은폐
무선 Packet Sniffing	노출	PK Mv2 인증	암호화
		EAP 인증	
SSID	식별 가능	SSID 마스킹	식별불능

또한, 펌웨어 업데이트를 통하여 하드웨어의 보안을 강화할 수 있으며, 백신프로그램을 설치하고 주기적인 업데이트를 통하여 단말이나 PC에 바이러스나 악성코드의 감염으로 보호할 수 있다.

Ⅴ. 결 론

WiBro 단말을 이용하여 인터넷 서비스는 무선에서 오는 취약점과 인터넷에 취약점을 모두 가지고 있다. 본 연구에서는 WiBro 취약점과 해킹 공격에 대해 알아보고 WiBro 단말의 취약점과 분석하였다. WiBro 단말 보안기술을 연구하고 보안기술을 적용하였다. 보안기술적용 전후 비교분석을 통하여 보안기술을 적용하였을 때 WiBro 단말 취약점이 보안되는 것을 확인하였다.

향후연구로는 WiBro 단말에 대한 Physical Layer와 MAC Layer의 취약점 연구가 지속되어야 할 것이며 이에 대한 보안대책 또한 연구가 이루어져야 할 것이다.

참고문헌

[1] 길민권 기자, “와이브로에그, 관리자 로그인 없이 설정변경 취약점!,” 데일리시큐, http://www.dailysecu.com/news_view.php?article_id=2849, 2012. 09.

[2] Woo Bong Cheon, Keon il Heo, Won Gyu Lim, Won Hyung Park, Tai Myoung Chung, "The New Vulnerability of Service Set Identifier(SSID) Using QR Code in Android Phone," IEEE eXpress Conference Publishing, 2011. 5.

[3] 천우성, 박대우, "WiBro 서비스를 이용한 응용프로그램의 취약점 분석 및 보안 대책 연구" 한국정보통신학회논문지, v.16 no.6, pp.1217-1222, 2012.

[4] Md. Alimul Haque, Yashi Amola, N. K. Singh, "Threat Analysis and Guidelines for Secure Wi-Fi and WiMAX Network," World Applied Programming, Vol.2, No.2, pp.110-115, 2012. 2.

[5] 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.

[6] 한국인터넷진흥원, “와이브로 보안기술 안내서,” pp.1-158, 2010.

[7] 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.

[8] 김종환, 전홍우, 신경욱, "WiBro 보안용 AES기반의 Key Wrap/Unwrap 코어 설계,” 한국해양정보통신학회논문지, vol.11, no.7, pp.1332-1340, 2007.