WiBro 인터넷 금융거래 취약점분석과 해킹공격

송진영*, 박대우*

*호서대학교 벤처전문대학원 IT응용기술학과

Vulnerability Analysis and Hacking Attack about WiBro Internet Financial Transaction

Jin-Young Song*, Dea-Woo Park**

*Dept. of, IT Application Technology, Hoseo Graduate School of Venture

E-mail : jedisong2083@gmail.com, prof1@hoseo.ac.kr

요 약

2011년 현재 유무선 인터넷을 이용해 VoIP, e-mail 통신을 하며, 금융거래인 은행거래, 주식거래, 안전결제 서비스를 이용하고 있다. 하지만 유무선 인터넷에서 침해사고가 발생하여 VoIP, e-mail이나 은행거래, 주식거래, 안전결제에 취약점 가능성이 있다. 2011년 3월 개인정보보호법 국회통과로 금융거래에서 개인정보를 보호해야 한다. 본 논문에서는 WiBro 인터넷 금융거래에서 VoIP, e-mail이나 은행거래, 주식거래, 안전결제를 할 때, SecuiScan을 이용하여 취약점을 분석한다. 취약점을 분석한 결과, 발견된 취약점을 이용하여 실험실 환경에서 해킹공격을 실시한다. 해킹결과 분석과 침해사고 유형에 따른 보안성 강화를 위한 보안 대책을 제시한다. 본 논문의 연구는 WiBro 인터넷 금융거래 보안성 강화에 기여할 것이다.

키워드

Wibro, 인터넷 금융거래, 취약점, 해킹공격

Ⅰ. 서 론

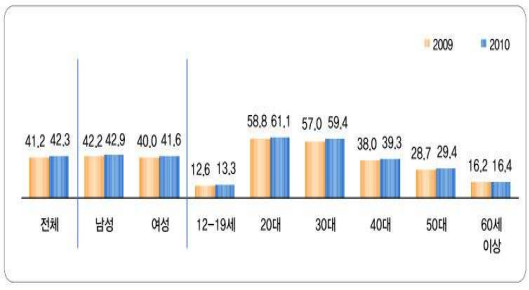

그림 1. 인터넷뱅킹 이용률(%)

그림 1은 2009년과 2010년의 인터넷뱅킹 이용률과 이용자를 나타낸 표이다[1]. 만 12세 이상 인터넷 이용자의 42.3%가 1년 이내 인터넷뱅킹을 이용한 것으로 나타났으며, 1개월 이내 인터넷뱅킹을 이용한 경우도 31.6%로 나타나 있다.

그러나 2011년 4월 7일 현대캐피탈에서 42만여 명의 이름, 주민등록번호, 카드번호, 비밀번호, 휴대전화 번호, 이메일 주소 등이 유출되는 해킹 피해사례가 발생하였다.

2011년, 스마트폰 및 노트북을 이용하여 무선인터넷 이용률은 59.3%이고, 특히 WiBro 이용률은 16.4%가 이용하고 있다.

이로 인하여, WiBro(Wireless Broadband Internet) 인터넷 금융거래 시 해킹 공격이나 DDoS(Distributed Denial of Service) 등이 발생할 수 있으므로, 본 논문에서는 WiBro 인터넷 금융거래시 취약점분석과 해킹공격에 대한 연구가 필요하다.

Ⅱ. 관련 연구

2.1. WiBro 인터넷

WiBro 확대를 위해 노트북 대여서비스 및 UICC(Universal Integrated Circuit Card) 개발하

여, 타 사업 영역과 연계한 공동마케팅 등 추진되고 있다. 현행 WiBro에 VoIP(Voice Over Internet Protocol)를 도입하게 되면 기존 유선통신 및 이동통신 사용자와 저렴한 비용으로 음성 및 영상통화 가능하다. 국내 WiBro 시장규모는 2011년까지 가입자 기준으로 400만 명에서 500만 명에 이를 것으로 전망된다[2].

2.2. 인터넷 금융거래

온라인 뱅킹 거래 시스템은 금융 조회, 이체 지불 등의 거래 서비스를 제공하는 시스템이다. 은행거래는 인증서 기반으로 발생을 하며 모든 데이터는 암호화로 되어 있다[3]. 서비스는 사이버 메일 센터, 휴대폰, PDA와 같은 모바일 디바이스를 이용하는 WAP(wireless application protocol) 서비스, VoIP 기술을 활용하여 웹 상담기능을 제공 하는 Web Phone, Call Banking과 연동이 되고 있다.

2.3. WiBro 인터넷 네트워크 구성

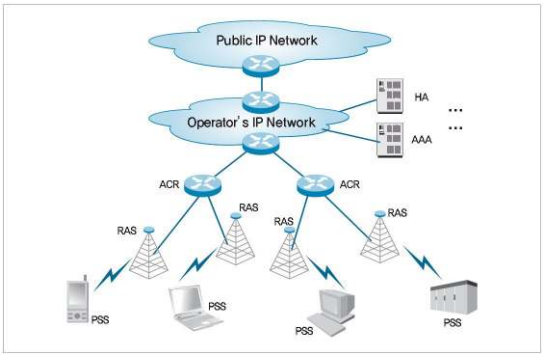

그림 2. Wibro 망 구성도

그림 2는 WiBro 망구성도를 나타낸다[4].

WiBro 망구성은 크게 4가지 요소로 구분할 수 있다. 서비스를 이용하는 사용자 단말기(PSS : Portable Subscriber Station), 무선으로 정보를 전달하는 기지국(RAS : Radio Access Station), 이동성/과금/세션 등을 관리하는 제어국(ACR : Access Control Router) 및 각종 부가서비스를 제공하는 서버들로 구성된다.

Ⅲ. WiBro 인터넷 금융거래 취약점 분석

3.1. VoIP

WiBro에서 VoIP 서비스의 보안 위협으로는 피싱에 이용, 통화내용 불법도청, 주요 시스템에 대한 DoS 공격, 불법 광고 전송을 위한 스팸, 정상적인 사용자로 위장하여 요금을 지불하지 않고 VoIP 서비스를 불법적으로 사용하는 서비스 오용 공격 등이 있을 수 있다[5].

인터넷상에 공개되어 있는 VoIP 해킹 도구를 이용하여 쉽게 도청공격 수행이 가능하며, 통화정보 및 내용에 대한 노출로 인한 심각한 프라이버시 침해가 가능하다.

3.2. 은행거래

현재 인터넷 뱅킹을 이용한 금융거래의 보안 위협으로는 은행 홈페이지와 같은 사이트를 만들어서 해킹하는 피싱, 악의적으로 피해자 PC내부에 외부에서 원격조종 할 수 있는 멀드롭 형태의 바이러스를 심어 공격하는 방법, 해당 은행 관리 시스템의 루트를 공격하는 고객 정보 유괴 해킹, 은행 근처에서 무선 랜카드와 AP를 장착한 노트북 컴퓨터로 인터넷 무선 공유기에서 나오는 데이터를 가로채는 패킷 스니핑과 무선 이동형 해킹, 스마트폰을 이용한 DDoS 공격 등이 있다[6].

3.3. 주식거래

WiBro 인터넷을 이용하는 한명의 사용자의 HTS(Home Trading System)에 문제가 생길 경우, 동일한 프로그램을 다운로드하는데서 취약점이 발생된다. 해커들은 사용자를 가장해 자신의 PC에 HTS 프로그램을 내려 받은 뒤 디버깅 프로그램을 통해 충분한 시간을 갖고 소스코드를 들여다볼 수 있기 때문이다.

3.4. 안전결제

사용자가 PC에 저장한 공인인증서로 금융거래를 하기 위해서는 별도의 해킹 방지, 암호화 프로그램 등이 모두 '액티브 엑스(ActiveX)' 방식으로 설치된다는 점에 문제가 있다. 해커가 만든 '액티브 엑스'가 PC에 깔릴 경우 각종 바이러스와 스파이웨어 같은 악성코드에 감염되면 PC에 저장된 공인인증서의 무단복제가 가능하다[7].

Ⅳ. WiBro 인터넷 금융거래 공격 분석

4.1. VoIP

WiBro를 WiFi로 변경시켜주는 EGG를 이용하여

두 대의 스마트폰을 접속시킨다. 또한 스마트폰과 VoIP를 할 때 도중에 스니핑을 할 수 있도록 노트북에 AirPcap, OmniPeek를 이용하여 스니핑 캡처(Sniffing Capture) 프로그램을 설치한다.

EGG에서 VoIP를 하는 사용자들의 패킷을 잡기 위해서는 Packet Sniffing을 설치한 노트북을 EGG에 접속하여 Arp Spoofing을 한다.

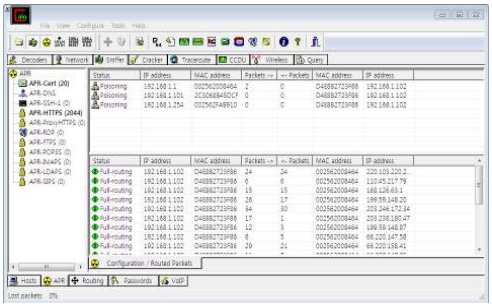

그림 3. Arp Spoofing

그림 3은 Arp Spoofing을 하는 장면이다. 노트북과 EGG를 연결하여 Arp Spoofing을 하면 Packet을 주고받는 장면을 캡처하였고, 통신하는 장면을 Wireshark를 이용해 Packet을 Sniffing하는 장면이다. 그림 5와 같이 VoIP를 이용하고 있는 해당 IP와 SIP가 나와 있는 것을 볼 수 있다.

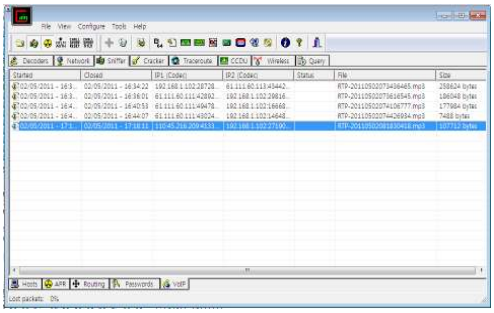

그림 4. VoIP 음성 파일

또한, 그림 4처럼 VoIP 음성 파일이 파일로 저장이 되어있는 것을 볼 수 있다. 본 연구에서는 총 다섯 번의 실험을 하였고, 7488bytes부터 258264bytes 까지의 데이터를 얻을 수 있었다.

이처럼 WiBro가 연결된 상태에서 VoIP를 이용한 결과 Sniffing을 이용해 Packet을 얻을 수 있다는 사실을 알 수 있었다.

4.2. 은행거래 공격분석

스마트폰에서 WiBro Packet을 WiFi Packet으로 변환시키는 EGG에 연결을 한 후 인터넷 뱅킹에 접속을 한다. 본 연구에서는 실제로 계좌이체를 실행하고, AirPcap, OmniPeek를 이용하여, Packet을 Sniffing을 하였다.

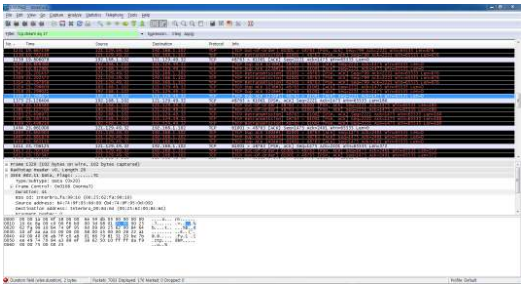

그림 5. 인터넷 뱅킹 Packet 분석 장면

그림 5는 인터넷 뱅킹에서 계좌이체시 패킷을 분석하는 장면이다. 본 연구에서 실험 장비인 스마트폰의 IP주소인 192.168.1.102와 인터넷 뱅킹 주소인 121.129.49.32 주소가 나왔지만 은행자체의 보안툴과 백신프로그램인 V3가 동작중이어서, ID, PW, 계좌이체 내용 등은 모두 암호화처리가 되어 분석이 불가능하였다.

4.3. 주식거래 공격분석

다음 그림 6은 주식 거래하는 장면이다. Packet Sniffing인 AirPcap, OmniPeek를 이용하여, 프로그램과 장비가 설치된 노트북을 가지고, 실제 주식거래하는 컴퓨터의 Packet을 Sniffing하여 분석을 실시한다.

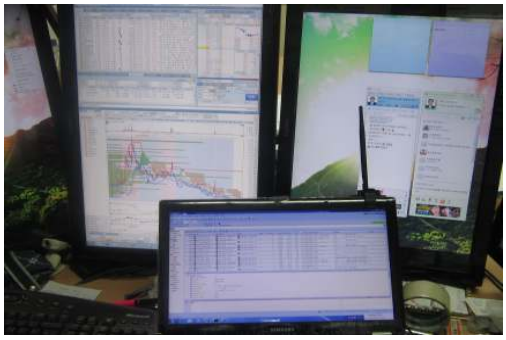

그림 6. 주식 거래 실험 환경

그림 6에서 주식 거래하는 컴퓨터의 IP주소인 192.168.1.100과 주식사이트의 IP주소인

118.107.173.31이 서로 Packet을 주고받으며 통신을 하고 있다.

Packet을 분석해 보면, Authentication에 대해서 나와 있는데, 이 부분을 분석한 결과 자체적인 보안툴과 V3로 공격 등을 막고 있어, Packet이 암호처리된 것을 볼 수 있다.

4.4. 안전결제 공격분석

다음은 안전 결제시 AirPcap, OmniPeek를 이용하여, Packet을 Sniffing 하는 실험 환경이다. 그림 7처럼, 그림 좌측에 Packet Sniffing 프로그램이 설치한 노트북을 이용하여, 그림 우측의 노트북에서 인터넷에서 물품을 구입하고, 결제하는 실험 장면을 Sniffing으로 하여 Packet을 캡처하였다.

그림 7. 안전결제 실험 환경

안전결제를 실행하고 있는 192.168.1.105 IP주소와 안전결제 사이트인 120.50.140.79 IP주소가 서로 Packet을 주고받으며 통신을 하고 있다.

WiBro에 보내는 Packet을 Sniffing하여 분석하면, ID, PW, e-mail, cpinfo 등이 나와 있는데, 이러한 정보가 자체 보안툴로 인하여 대부분 암호가 되어 있었다.

V. 결 론

본 논문에서는 WiBro 신호를 WiFi 신호로 변환시켜주는 EGG를 이용하여 EGG에서 VoIP, 인터넷 뱅킹, 주식거래, 안전결제를 사용할 때, AirPcap, OmniPeek를 이용하여 Packet를 Sniffing하고, Sniffing한 내용을 분석을 한 결과, VoIP에서는 음성파일 정보를 취득하였지만, 인터넷 뱅킹, 주식거래, 안전결제는 SSL, 자체 보안툴과 백신프로그램으로 인하여, Packet이 암호화되어 있었다.

향후 연구에서는 WiBro 신호를 WiFi 신호로 변환시켜주는 EGG에서 SSL을 Hacking하여, e-mail, 인터넷 뱅킹, 주식거래, 안전 결제시 Packet을 분석하는 연구가 필요하다.

참고문헌

[1] 방송통신위원회, 한국인터넷진흥원, 2010년 인터넷 이용실태조사 요약보고서, pp.19-22, 2010.09.

[2] 한국인터넷진흥원, 와이브로 보안기술 안내서, pp.1-158, 2010.01.

[3] Woo-Sung Chun and Dea-Woo Park, Security Vulnerability Analysis and Forensic Data Research to Attacks on Mobile Stock Trading System in WiBro Network, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.12, pp.291-298, December 2009.

[4] 최정훈, WiBro 보안 프로토콜에 관한 연구, 한국인터넷정보학회 추계학술발표대회, 제20회, pp.227-231, 2009.10.

[5] 손현구, 이영석, VoIP 이상 트래픽의 플로우 기반 탐지 방법, 정보과학회논문지, 제37권 제4호, pp. 255-316, 2010.08.

[6] 이진용, 이진범, 황성운, 안홍영, 보안공학연구논문지, 제6권 제5호, pp.323-336, 2009.10.

[7] 박남제, e-비즈니스 기술 : 모바일 RFID 비즈니스 응용을 위한 SMAP 기반 보안 서비스 제공 방안, 국제e비즈니스학회, 제11권, 제2호, pp.295-315, 2010.