Smart Phone에서 무료 WiFi 인터넷 접속 때 해킹 공격

장영현°, 표성배**, 송진영*, 박대우*
°배화여자대학 컴퓨터정보학과
*호서대학교 벤처전문대학원 IT응용기술학과
**인덕대학 컴퓨터소프트웨어과
e-mail: baewhaoa@paran.com, jedisong@naver.com, prof1@paran.com

A Study on Hacking Attack when Free WiFi Internet Access In Smart Phone

Young-Hyun Chang°, Jin-Young Song*, Dea-Woo Park*
°Dept. of, Computer Information, Baewha Women's University
*Dept. of IT Application Technology, Hoseo Graduate School of Venture
**Dept. of, Computer Software, Induk University

● 요 약 ●

최근 무료 WiFi Zone이 확대되고 있고, Smart Phone으로 무료 WiFi에 접속하여 인터넷으로 접속하여 메신저를 하거나, 메일 확인, 정보검색 등을 한다. 하지만 무료 WiFi Zone에서 Smart Phone으로 인터넷을 할 때, 개인정보를 해킹 당 할 수가 있다. 본 논문에서 안드로이드 O,S, Smart Phone에서 무료 WiFi를 이용하여 접속한다. 먼저 메신저와 웹사이트 로그인을 한다. 이때 AirPcap을 이용하여 패킷을 캡처한다. Packet 분석 툴인 WireShark를 사용하여 Packet의 내용을 분석하고, ID, PW와 메신저 대화 내용을 해킹한다. 해킹한 개인정보 ID, 비밀번호를 이용하여 인터넷 사이트에 접속을 하여 관리자 권한을 획득한다. 그리고 Smart Phone에서 WiFi접속 시 공격에 대한 보안대책을 제시한다. 본 연구는 Smart Phone에서 무료 WiFi 접속 때, 보안성 강화연구와 무선 해킹과 방어 기술 발전에 초석이 될 것이다.

키워드: 스마트폰(Smart Phone), 와이파이(WiFi), 개인정보(Personal Information), 해킹(Haking), 보안성 강화(Security tighten)

I. 서론

Smart Phone 사용자들이 늘어나고, 통신사업자들의 경쟁이 심화되면서 Smart Phone 사용자들이 WiFi을 이용한 무료 서비스가 많이 활용되고 잇는 추세이다.

무료 WiFi Zone에서는 Smart Phone으로 인터넷에 접속하여 스트리밍 형식으로 통해 실시간으로 음악을 듣고, 대용량의 영화를 다운 받으면서, 친구와 메신저를 이용하여 대화를 주고 받거나, 또한 중용한 업무를 하기도 한다.

그림 1. Smart Phone 주요 이용 기능(복수응답, %)
Fig. 1. Sart Phone features the main use (multiple responses,%)

그림 1은 2010년 7월, 방송통신위원회와 한국인터넷진흥원이 발표한 Smart Phone 이용실태 조사결과 보고서이다. Smart Phone 이용자는 Smart Phone을 통해 '인터넷 접속(95.9%)'을 가장 많이 사용하는 것으로 나타나고 있다. GPS를 이용한 지도, 위치기반서비스 등이 79.4%, 신규 모바일앱 설치 및 이용률은 78.3%, 이메일은71.9%로 나타난다. 이처럼 Smart Phone을 이용해 시간과 장소에 상관없이 인터넷에 쉽게 접근할 수 있다.

하지만 무료 WiFi Zone에서는 보안이 되지 않는 무선 공유기를 이용하여 Smart Phone으로 인터넷에 접속하고, 중용한 개인정보를 주고받는다면 해커의 공격에 당할 수 있다.

본 논문에서는 안드로이드 Smart Phone으로 무선 공유기에서 접속하여 인터넷을 할 때, 정보를 주고받는 Packet을 Sniffing하고, Capture하여 사용자의 신상정보, ID나 비밀번호을 획득 할 수 잇는 가를 싱험한다. 그리고 획득된 개인정보를 이용하여 인터넷 웹에 접속하여 관리자 권한을 취득 할 수 잇는 가를 확인 한다. 그리고 Smart Phone으로 인터넷에 접속 때 보안 대책에 대해 연구한다.

II. 관련 연구

2.1. Android O.S. Smart Phone

2010년부터 급속하게 사용된 아이폰과 안드로이드 O.S. Smart Phone은 다양한 인터페이스와 기능이 하나의 작은 기기에서 제공됨으로 인하여 손안의 PC가 우리의 실생활에서 실현되게 되었다(1).

안드로이드(Android)(2)는 Smart Phone, 모바일 디바이스를 위한 운영체제와 미들웨어 그리고 핵심 응용 프로그램을 포함하고 있는 소프트웨어 스택이다. 안드로이드는 개발자들이 자바(Java) 언어나 C++, Perl 등 스크립트 언어로 응용 프로그램을 작성할 수 있으며, 컴파일된 바이트코드를 구동할 수 있는 런타임 라이브러리를 제공한다. 또한 안드로이드 SDK를 통해 응용 프로그램을 개발하기 위해 필요한 각종 도구들과 API를 제공한다.

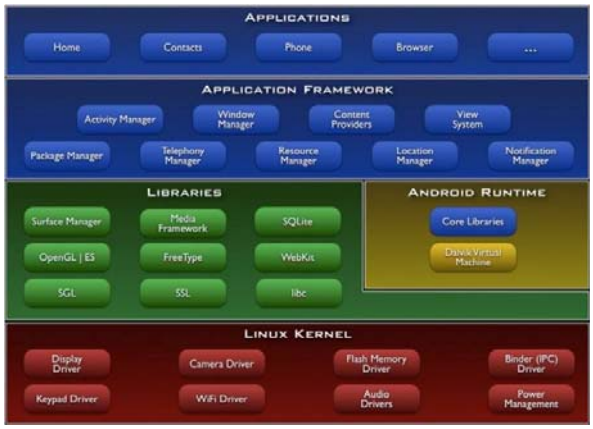

그림 2. 안드로이드 아키텍처
Fig. 2. Android Architecture

안드로이드 O.S.는 그림 2처럼 리눅스 2.6 커널 위에서 동작하며, 다양한 안드로이드 시스템 구성 요소에서 사용되는 C/C++ 라이브러리들을 포함하고 있다. 안드로이드는 기존의 자바 가상 머신과는 다른 가상 머신인 Dalvik[4] 가상 머신을 통해 자바로 작성된 응용 프로그램을 별도의 프로세스에서 실행하는 구조로 되어 있다. 안드로이드의 주요 특징은 어플리케이션 프레임워크이며 Webkit 이라는 엔진에 기반을 둔 통합 브라우저를 사용한다.

그리고 OpenGL ES 1.0스펙을 따르는 2D, 3D 를 지원하고 SQLite라는 데이터 저장소를 사용하며, MPEG4, MP3, JPG,GIF 등의 미디어 지원을 한다. 하드웨어에 의존적이긴 하지만 GSM 전화 기술과 블루투스, EDGE, 3G, WiFi 기술과 Eclipse 상에서 수행할 수 있는 개발 환경을 지원한다. 또한, 에뮬레이터와 디버깅 툴, 메모리 및 성능 프로파일링, 이클립스 플러그인도 포함되어 있다.

안드로이드 2.1 버전의 특징은 멀티터치 지원, 블루투스 2.1을 지원하고, HTML5[5]를 정식 지원한다. 그리고 화면 가상 키보드 성능을 향상시키고, 카메라 지원 기능 향상, 멀티미디어 재생 기능 향상 특징을 가지고 있다.

2.2 WiFi

WiFi란 무선 랜의 표준 규격인 IEEE802.11b의 별칭이라고 할 수 있다. '와이파이(WiFi)'라고 쓰이게 되었다.

무선접속장치(AP)가 설치된 곳을 중심으로 일정 거리 이내에서 Smart Phone이나 노트북 컴퓨터를 통해 초고속 인터넷을 이용할 수 있다. WiFi[4]는 보통 와이어리스랜(Wireless LAN) 이라고 하는데 이 기술은 네트워크 구축 시 유선 대신 무선주파수를 이용하여 네트워크를 구축한다. 무선주파수를 이용하므로 전화선이나 전용선이 필요 없으나 Smart Phone이나 노트북 컴퓨터에는 무선 랜 카드가 장착되어 있어야 한다.

WiFi는 1999년 9월 미국 무선 랜 협회인 WECA (Wireless Ethernet Capability Alliance; 2002년 WiFi로 변경)가 IEEE802.11b 방식을 표준으로 정했고, 이와 호환되는 제품에 WiFi 인증을 부여한 뒤 급속하게 성장하게 된 것이다.

2.3 패킷 분석 툴 WireShark

패킷 분석 툴 WireShark는 2006년 6월 상표권 분쟁으로 Ethereal에서 Wireshark(5)로 명칭이 바뀌었다. Wireshark는 tcpdump와 매우 유사한 기능을 제공한다. 그러나 추가로 GUI(Graphical User Interface)를 지원하고, filtering option과 정렬을 통해 더 많은 정보를 제공한다.

그리고 network interface를 promiscuous mode1로 설정함으로써 네트워크를 지나다니는 모든 packet(6)을 사용자가 볼 수 있게 해 준다. 그리고 알려진 프로토콜 중에서 일부분에 대해서는 직접 parsing을 하여 내용을 보여주기도 한다.

WireShark의 특징은 몇 백 개의 네트워크와 네트워크 프로토콜을 지원하고 분석 할 수 있고, Live capture와 offline 분석이 가능하다. 다양한 플랫폼에서 사용이 가능(Windows, Linux, Solaris, MAC OS X 등)하여 GUI 환경을 지원하고, 여러 개의 파일 포맷을 읽기, 쓰기 가능하도록 되어 있다. capture 파일들은 gzip으로 압축으로 되어있고, Ethernet / IEEE 802.11, PPP/HDLC 등을 읽어 들일 수 있다.

Capture된 Packet(7)을 분석할 때는 색상을 적용해 식별이 가능하도록 되어있으며, IPsec, Kerberos, SSL/TLS 등 암호화된 Packet을 분석할 수 있다. Capture된 결과를 XML 등으로 전송이 가능하다.

III. WiFi Zone에서 Smart Phone으로 인터넷 접속

3.1 안드로이드 Smart Phone에서 WiFi 접속

그림 3. WiFi 연결 장면
Fig. 3. WiFi connectivity scene

안드로이드 Smart Phone을 사용하여 WiFi Zone에서 인터넷에 연결하기 위해서는 Smart Phone에서 WiFi 설정에 들어가 Smart Phone 지역 내에 WiFi를 검색하여 신호강도가 좋은 WiFi를 연결시킨다. 다음 그림 3에서 SAMSUNG 무선 공유기에 Smart Phone을 접속시킨 장면이다.

3.2 Packet Sniffing과 Capture

안드로이드 Smart Phone으로 무료 WiFi Zone에서 인터넷에 접속 할 때, Packet을 Sniffing하고, Capture하기 위해 다음과 같이 실험환경을 구성하였다.

- AirPcap : 802.11 무선 네트워크 Packet Capture
- Galaxy S : 16GB 내장 메모리, 안드로이드 2.1, CPU 1GHz, 512MB RAM
- ASUS Notebook : Intel Core 2 duo 2.00GHz, 1GB RAM, 100GB 하드디스크, Windows XP
- WireShark : Version 1.2.9(SVN Rev 33171)

그림 4. AirPcap 컴퓨터 연결 장면
Fig. 4. Scene AirPcap computer connection

802.11 무선 네트워크의 Packet을 Sniffing하려면 AirPcap을 설치해야 한다. AirPcap은 USB형태로 되어있고 컴퓨터에 연결을 시킨 후 무선 Packet을 Sniffing할 수 있다. Sniffing후에 WireShark로 Packet을 Capture받고나서 분석하여 개인정보를 수집한다. 그림 4은 AirPcap은 WiFi 무선 네트워크 Packet을 Capture할 수 있는 도구이다. USB형태로 되어있어 컴퓨터에 부착을 시키고 AirPcap이 동작하기 위해서 설치프로그램을 설치한다.

3.3 WireShark Packet 분석

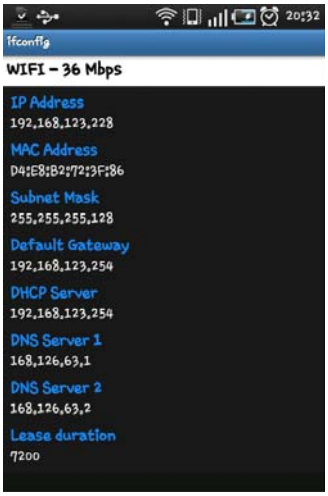

그림 5. Smart Phone IP 주소 확인
Fig. 5. Check Smart Phone IP address

그림 5는 Smart Phone에서 앱을 사용하여 Smart Phone IP를 확인하는 장면이다. 실험과정에선 3G 통신방식이 아닌 무료 WiFi 통신 방식을 사용하여서 Smart Phone IP주소는 192.168.123.228 이고, MAC주소는 D4:E8:B2:72:3F:86으로 되어있는 것을 확인할 수 있다.

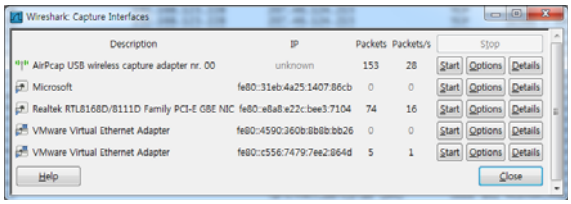

그림 6. WireShark에서 AirPcap 설정
Fig. 6. Set AirPcap in WireShark

무선 인터넷 Packet을 Sniffing한 후 Packet을 분석을 하려면 WireShark 분석 툴이 필요하다. 그림 6는 WireShark를 실행 후 Capture가 가능한 인터페이스를 보여주는 화면인데, Description에서 맨 윗줄에 AirPcap USB wireless capture adapter nr. 00이 보여주는 것을 알 수 있다. 위의 그림 4에서 AirPcap을 컴퓨터에 연결시킨 동작이 자동으로 WireShark에 인식이 되어 있는 것을 볼 수 있다.

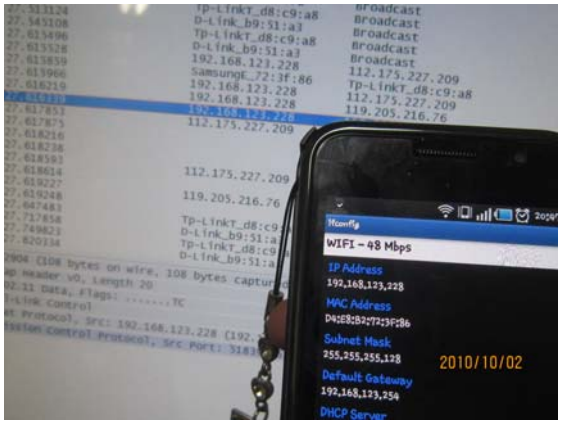

그림 7. WireShark에서 Smart Phone IP주소 확인
Fig. 7. Smart Phone IP address resolution from WireShark

그림 7에서 AirPcap 인터페이스에서 Start 버튼을 눌러주면, WireShark에서 현재 무선인터넷 Packet이 보여지고, 그림 6과 같이 Smart Phone IP주소도 확인이 되는 것을 볼 수 있다.

IV. WiFi Zone 인터넷 해킹과 보안 대책

4.1 WiFi Zone 인터넷 해킹

4.1.1 메신저 Packet 분석

Smart Phone은 메신저 앱을 다운로드받아 상대방과 대화 할 수 있다. 안드로이드 Smart Phone에서 메신저를 사용할 때 Packet을 Capture하는 실험을 하였다. Smart Phone으로 상대방과 메신저 대화하는 도중에 WireShark를 이용해서 무선 Packet을 분석해본다.

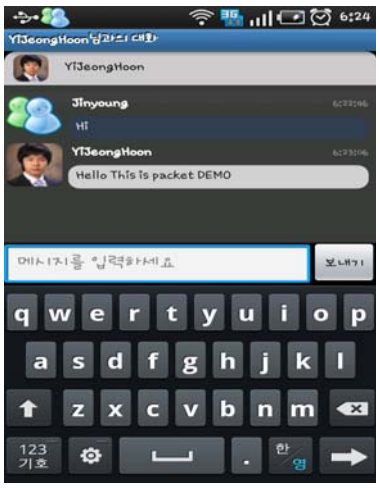

그림 8. 메신저 대화
Fig. 8. Messenger talk

그림 8은 메신저로 상대방과 대화하면 장면이다. 메신저로 대화한 후 WireShark를 이용해 패킷 안에 대화 내용이 있는지 확인한다.

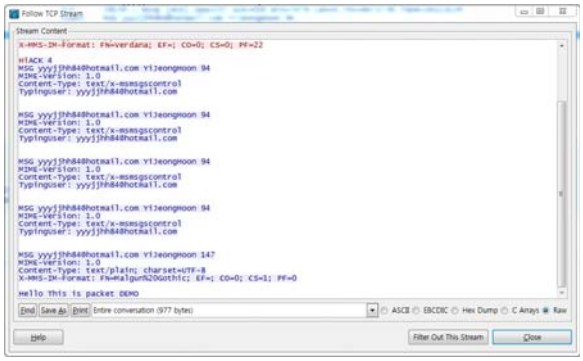

그림 9. 메신저 대화 Packet Capture
Fig. 9. Messenger Packet Capture

그림 9는 메신저로 대화 할 때 Packet을 분석하는 장면이다. Capture한 Packet의 Source IP 와 Destination IP, Protocol를 확인하여 대화한 내용이 들어있는 Packet을 찾는다. 그림 8에서보면 서로 대화한 글이 Packet에 저장되어 있는 것을 볼 수 있다.

이처럼 Smart Phone에서 WiFi를 이용하여 메신저로 대화한 Packet을 Capture하여 분석하면 육안으로 확인할 수 있다.

4.1.2 ID, 비밀번호 분석

안드로이드 Smart Phone의 WiFi를 이용하여 원하는 인터넷 사이트에 접속 할 수 있다. 이때 해당 사이트에 로그인하기 위해 ID와 비밀번호를 적게 되는데 WireShark를 이용하여 Packet을 Capture한 후 아이디와 비밀번호를 알아낼 수 있다. 알아낸 아이디와 비밀번호를 입력하여 해당 사이트에 접속하여본다.

4.1.3 웹사이트 로그인 및 관리자 권한 획득

그림 10. 홈페이지 로그인 접속 화면
Fig. 10. Homepage Sign-up screen

그림 10은 Smart Phone에서 무료 WiFi Zone에서 인터넷 홈페이지에 접속하는 장면이다. 일반 PC에서 접속하는 방법처럼 사용자가 접속하기 위해 아이디와 비밀번호를 입력하고, 입력한 정보는 홈페이지의 DB서버에서 아이디와 비밀번호를 일치한지 확인한 후 접속을 허가하게 된다.

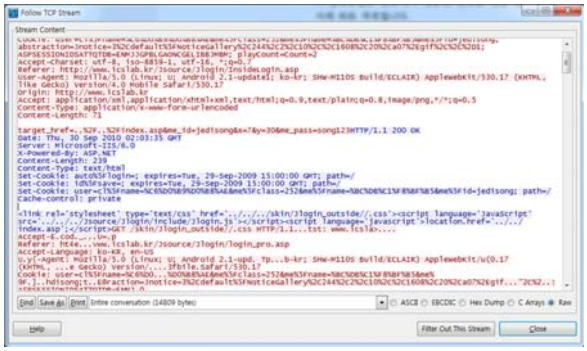

그림 11. 홈페이지 접속 Packet Capture 화면
Fig. 11. Homepage Connection Packet Capture screen

그림 11에서는 홈페이지 로그인 접속 아이디와 비밀번호 정보가 뜨는 것을 알 수 있다. Smart Phone에서는 아이디와 비밀번호를 전송하고, 서버에서는 200번의 메시지를 보내 정보가 일치한다고 전송이 되어있다. 이처럼 무선 Packet Capture를 하면 아이디와 비밀번호처럼 민감한 정보를 획득할 수 있다.

그림 12. 관리자 권한으로 홈페이지 접속 화면
Fig. 12. Homepage login screen with administrator privileges

패킷 분석으로 알아낸 아이디와 비밀번호를 사이트 로그인창에 입력을 하여 아이디와 비밀번호가 맞는지 확인하여 본다. 그림 12은 획득한 관리자 권한으로 로그인하는 장면인데 관리자로 접속되는 것을 확인 할 수 있다.

4.2 Smart Phone으로 무료 WiFi 인터넷 접속 때 보안 대책

Smart Phone은 무선 인터넷을 이용해 무료 WiFi 인터넷 접속 때에는 편리하고 싸게 인터넷을 사용할 수 있지만, 보안에 유의하여야 한다. 위 실험과 같은 해킹 공격과 침해사고를 막으려면 다음과 같은 보안을 설정한다.

① 루팅이나 탈옥 등 Smart Phone의 플랫폼 구조를 해킹하지 않는다.
② 사용하지 않는 WiFi와 같은 무선 네트워크 서비스는 종료시킨다.
③ Smart Phone에 중요한 데이터는 암호화하여 저장한다.
④ 항상 최신 업데이트를 유지한다.
⑤ 보안이 신뢰할 수 있는 웹 사이트를 이용한다.
⑦ 앱스토어 등에서 구입하는 어플리케이션이 아닌 비공식 루트로 어플리케이션을 설치하지 않는다.
⑧ 보안이 가능한 e-mail을 사용한다.

V. 결론

무료 WiFi Zone에서 Smart Phone 사용자들은 웹서핑을 하거나 메신저을 주고 받고, e-mail, SNS, 음악과 영화 감상, 문서 편집 등 이동하면서 여러 가지 일을 할 수 있다. 그러나 해커들의 공격대상이 되고 있고, 침해사고가 발생한다.

본 논문에서는 안드로이드 Smart Phone을 이용하여 무료 WiFi Zone를 이용하여 무선 네트워크 접속할 때, AirPcap을 사용하여 Packet을 Sniffing하고, WireShark를 이용해 Capture하고 분석하여, 개인정보의 ID와 비밀번호를 취득 한 후 개인 홈페이지를 해킹하는 실험을 하고, 보안대책을 제시하였다.

향후 연구로는 3G 망에서 인터넷 이용 시 무선 Packet 분석 연구가 필요하고 WiFi 존에서의 취약점을 알아본다.

참고문헌

[1] 제갈병직, “스마트폰 시장과 모바일OS 동향,” Semiconductor Insight, 9-18쪽, 2010.
[2] 정승일, “안드로이드 플랫폼과 스마트폰 기술 발전 동향,” 대한전자공학회논문지, 33(1), 2000-2001쪽, 2010.
[3] 김선자, 김홍남, “모바일 플랫폼 발전 방향과 WIPI,” 정보과학회지, 24(7), 31-37쪽, 2006. 8.
[4] 고석훈, “안드로이드 플랫폼 동향,” 한국콘텐츠학회지, 8(2), 45-49쪽, 2010. 6.
[5] Angela Orebaugh,Gilbert Ramirez,Josh Burke, “Wireshark and Ethereal network protocol analyzer toolkit”
[6] 천우성, 박대우, “WiBro 네트워크에서 메신저, VoIP 도청 및 포렌식 연구,” 컴퓨터정보학회지, 14(5), 2009. 5.
[7] 박대우, “WiBro에서 침입 패킷 분석과 대응 연구,” 컴퓨터정보학회지, 12(3), 2007. 7.