Smart Phone 인터넷 접속시 패킷 분석 연구

송진영* □ 박대우*

*호서대학교 벤처전문대학원 IT응용기술학과

A Study of Packet Analysis in Smart Phone Internet Access

Jin-young Song* □ Dea-woo Park*

*Hoseo Graduate School of Venture

E-mail : jedisong@naver.com □ prof1@paran.com

요 약

Smart Phone 사용이 증가되고 있다. Smart Phone에서 인터넷에 접속하여 원하는 뉴스나 동영상을 보거나 어플리케이션을 다운받아서 실행할 수 있다. 하지만 무선인터넷은 인터넷의 취약점으로 인하여 Smart Phone 보안의 취약성도 발견되고 있다. 본 논문에서는 안드로이드 Smart Phone에서 인터넷에 접속할 때에 발생하는 취약점을 분석한다. Smart Phone에서 사용하는 정보를 네트워크 패킷 분석 툴을 이용하여 패킷을 캡처하고, 내용을 분석한다. 분석한 내용을 기반으로 Smart Phone에서 인터넷 이용 시 메신저, ID, 비밀번호를 확인하여, 실제 인터넷에서 ID, 비밀번호로 접속하여 개인정보를 탈취할 수 있는 해킹 과정을 시연한다. 본 연구는 Smart Phone에서 해킹과 보안과정을 연구하여 인터넷 정보통신 강국 코리아의 보안성을 강화 시키는데 기여할 것이다.

ABSTRACT

Smart Phone is the increasing use. Smart Phone can be run on that New or videos you want to connect to the Internet for downloading and viewing applications. But the wireless Internet have been found that Due to the vulnerability of the Internet, Smart Phone security vulnerabilities. This paper analyzes the vulnerability. Smart Phone droid that occur when connecting to the Internet. For information on Smart Phone to use to analyze network packet analysis and packet capture tools. Analysis is based on information from the Internet when you use Smart Phone Hack will demonstrate the process. Messenger, ID, to confirm the password, the actual internet ID, password access to the personal information that can be seized. In this study, hacking and security of the Smart Phone will contribute to the research process that Internet information and communication powers to strengthen the security of Korea.

키워드

Smart Phone, Packet Analysis, Android, WireShark

Ⅰ. 서 론

최근 Smart Phone의 보급으로 어플리케이션, 동영상, 음악 등을 인터넷를 이용해 보고 듣거나 활용할 수 있다.

또한, 소셜 네트워크 서비스인 SNS (Social Network Service)이나 이메일을 PC로 통하여 확인하지 않고 Smart Phone으로 실시간으로 확인하고 답장을 보낼 수 있다. 이처럼 Smart Phone은 인터넷에 쉽게 접근할 수 있는 손안의 PC가 되고 있다.

그림 1[1]에서 2010년 7월 무선인터넷 사용률을 살펴보면, 1시간이상 사용자가 41.6%이상으로 나타나있다. 이 처럼 Smart Phone을 이용한 무선인터넷 이용률은 계속 상승될 것이다.

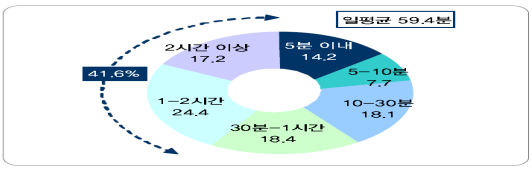

그림 1. Smart Phone 일 평균 인터넷 이용시간

하지만 Smart Phone에서 취약점이 발견되는 무선 인터넷을 이용하여 금융정보 등 업무 정보를 주고받는다면, 해커는 주고받는 패킷을 캡처하여 도청하고, 개인 정보에서 ID나 비밀번호를 획득하여, 공격자의 개인 이익을 취할 수 있는 악의적인 목적으로 사용할 수 있다.

본 논문에서는 안드로이드 Smart Phone으로 인터넷에 접속할 때에 발생하는 취약점을 분석한다. 즉 Smart Phone에서 사용하는 정보를 네트워크 패킷 분석 툴을 이용하여 패킷을 캡처하고, 내용을 분석하여, 분석한 내용을 기반으로 Smart Phone에서 인터넷 이용 시 메신저, ID, 비밀번호를 확인하여, 실제 인터넷에서 ID, 비밀번호로 접속하여 개인정보를 탈취할 수 있는 해킹 과정을 시연한다. 그리고 발견된 취약점을 보안 할 수 있는 보안대책을 수립하여 Smart Phone의 보안성 강화에 이바지 하겠다.

Ⅱ. 관련연구

2.1. 안드로이드

안드로이드는[2] 리눅스(Linux) 2.6 커널을 기반으로 강력한 운영체제와 포괄적 라이브러리 세트, 풍부한 멀티미디어 사용자의 인터페이스 , 폰 어플리케이션 등을 제공을 한다. 휴대폰에 안드로이드를 탑재하여 메신저 등을 이용할 수 있으며 , 휴대폰뿐만 아니라 다양한 정보 가전 기기에 적용할 수 있는 연동성을 갖추고 있다.

안드로이드가 기존의 휴대폰 운영체제인 마이크로소프트의 '윈도 모바일'이나 노키아의 '심바인'과 차별화 되는 것은 완벽한 개방형 플랫폼이다. 종전에서의 휴대폰 제조업체와 서비스업체마다 운영체제가 다르기 때문에 개별적으로 응용프로그램을 만들었다.

이에 비하여 안드로이드는 기반 기술인 '소스와 코드'를 모두 공개하며 누구라도 이를 이용해서 소프트웨어와 기기를 만들어 판매할 수 있도록 개방 하였습니다. 개발자인 경우 이를 확장 ,대체 또는 재사용하여 사용자들에게 보다 풍부하고 통합된 모바일 서비스를 제공할 수 있다.

2.2. WireShark

WireShark[3]는 수백 개의 네트워크와 네트워크 프로토콜을 지원한다. WireShark는 라이브 캡처, 오프라인 분석, 표준 3단 패킷 브라우저, 60,000이상의 디스플레이 필터, VoIP 분석, 수많은 다른 캡처 파일 포멧과 암호를 지원하고 있다. 전 세계적으로 공용 설치 기반이 있기 때문에 문서 자료와 온라인 지원이 이루어지고 있다.

Wireshark를 사용하여 현재 동작하는 네트워크 혹은 시스템에서 캡처되어 저장된 파일을 통해서 각각의 패킷에 대한 세부적인 데이터를 분석할 수 있다.

무선 인터넷 을 할 때에는 AP(Access Point)와 단말기가 MAC을 통해 IP, TCP, UDP 등과 같은 프로토콜을 통해서 정보를 주고받게 되는 정보 패킷을 캡처한다.

2.3. Smart Phone

Smart Phone은[5] PC와 같은 기능과 더불어 고급 기능을 제공하는 휴대전화로써, 어떤 사람들에게는 응용 프로그램 개발자를 위한 표준화된 인터페이스와 플랫폼을 제공하는 완전한 운영 체제 소프트웨어를 실행하여 전화나 e-mail, Internet, E-book, Game, Social Application, 내장형 키보드나 외장 USB 키보드, VGA 단자를 갖춘 고급 기능이 들어있는 소형 컴퓨터라 볼 수 있다.

Ⅲ. Smart Phone 인터넷 접속시 패킷 캡처

3.1. Smart Phone 네트워크에서 패킷 캡처

네트워크 패킷을 캡처하기 위해 같이 패킷 캡처 실험 환경을 구성하였다.

AirPcap : 802.11 무선 네트워크 패킷 캡처

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)

Smart Phone으로 무선 통신을 하고 있을 때, AirPcap을 이용하여 중간에 패킷을 가로채기를 할 수 있다. 이때 WireShark를 이용하여 캡처된 패킷을 분석을 할 수 있다.

3.2. WireShark에서 Packet Capture

패킷 캡처를 하기위해 대상인 Smart Phone의 네트워크 정보를 확인해야한다. 본 논문에서는 확실한 실험을 하고자 Smart Phone에 IP주소를 추출할 수 있는 안드로이드 어플리케이션을 설치하였다.

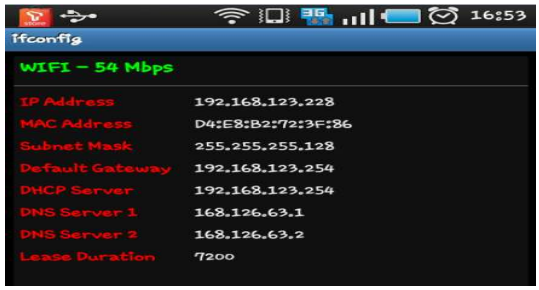

그림 2. Smart Phone 네트워크 주소

그림 2와 같이 Smart Phone 네트워크 주소를 알 수 있다. 그림 2에서 중점적으로 봐야 할 것은 IP Address와 MAC Address인데 이 두 개의 주소는 WireShark내에서 패킷을 분석 시 필요한 정보들이다. IP Address는 192.168.123.228, MAC Address는 D4:E8:B2:72:3F:86으로 되어있다.

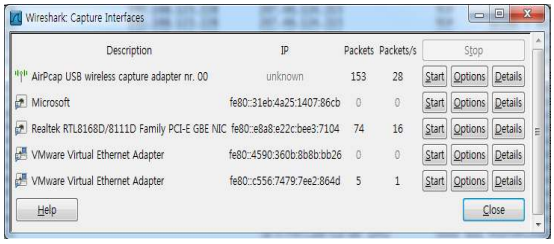

그림 3. AirPcap 설정

Smart Phone의 패킷을 캡처하기 위해 실험 컴퓨터에 AirPcap을 설치한다. AirPcap은 무선 패킷을 캡처를 도와주므로 그림 3과 같이 WireShark에서 AirPcap을 지정한 후 Smart Phone에서 나오는 패킷을 캡처한다.

Ⅳ. Smart Phone 인터넷 접속시 패킷 분석

4.1. Smart Phone 메신저 패킷 분석

다음은 Smart Phone으로 메신저를 사용할 때 패킷을 캡처하는 실습이다. 실습방법은 Smart Phone에서 메신저 어플리케이션을 다운받아 설치한 후 대화하는 도중에 AirPcap으로 무선패킷을 [6] 캡처한다. 패킷을 캡처 후 WireShark를 이용하여 패킷을 분석한다.

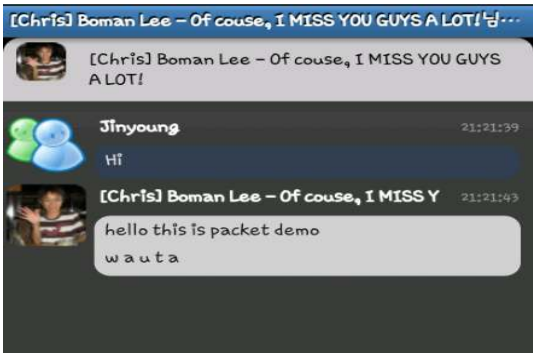

그림 4. 메신저 대화

그림 4는 실험을 하기위해 상대방과 대화를 요청하고 서로 대화하는 장면이다. 이 과정은 전달된 대화의 패킷을 캡처하기위한 장면이다.

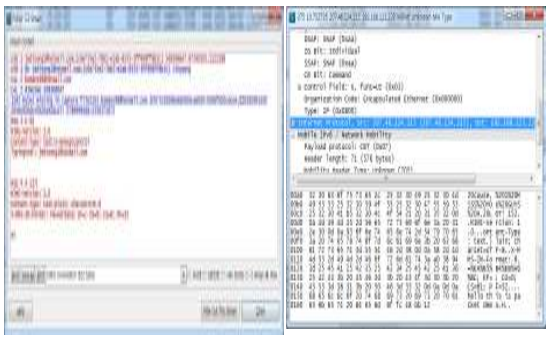

그림 5. 메신저 패킷 캡처

다음 그림 5는 캡처한 패킷을 WireShark로 분석한 화면이다. 캡처한 패킷의 Source IP 와 Destination IP, Protocol를 확인하여 대화한 내용이 들어있는 패킷을 찾는다. 그림 5의 왼쪽 그림은 'HI' 라고 적혀있는 패킷을 보여주는 그림이고, 오른쪽 그림은 'hello this is packet demo' 라고 적혀있는 패킷을 보여주는 그림이다.

이처럼 Smart Phone에서 WiFi를 이용하여 메신저로 대화한 패킷을 캡처하여 육안으로 확인할 수 있다.

4.2. Smart Phone 웹 사이트 접속 패킷 분석

Smart Phone은 WiFi나 3G로 이용하여 일반 PC처럼 인터넷에 접속하여 자신이 원하는 사이트에 접속을 할 수 있다. 이때 해당 사이트에 로그인하기위해 아이디와 비밀번호를 적게 되는데 무선 패킷 캡처툴을 이용하여 아이디와 비밀번호를 획득할 수 있다.

그림 6. 홈페이지 화면

다음 그림 6은 Smart Phone을 이용하여 홈페이지에 접속하는 장면이다. 사용자가 접속하기위해 아이디와 비밀번호를 누르면 입력한 정보는 홈페이지 서버에 전송하고, DB서버에서 아이디와 비밀번호를 확인한 후 일치가 되면 접속을 허가하게 된다.

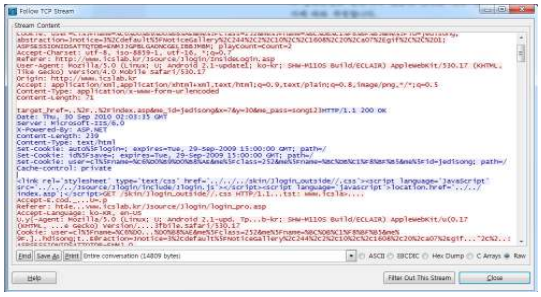

그림 7. 홈페이지 패킷 캡처

아이디와 비밀번호 정보가 고스란히 보여주고 있고, 서버에서는 200번의 메시지를 보내 정보가 일치한다고 전송이 되어있다. 이처럼 무선 패킷 캡처로 인해 민감한 정보를 획득할 수 있다.

4.3. 보안대책 강구

Smart Phone은 휴대성이 편하고, 인터넷 접근율이 높아져 언제 어디서든 편리하게 인터넷을 사용할 수 있지만, 그만큼 보안성에 비중을 크게 두어야한다.

그러기 위해서는 다음과 같이 보안을 설정한다.

① 사용하지 않는 네트워크 서비스는 종료시킨다.

② Smart Phone을 탈옥이나 루팅 등으로 임의로 구조 변경하지 말고 항상 최신 버전을 유지시킨다.

③ 안티 바이러스 소프트웨어를 사용한다.

④ 신뢰할 수 있는 어플리케이션만 다운로드 받는다.

⑤ 보안을 신뢰할 수 있는 웹 사이트만 접속한다.

⑥ 보안이 강화된 전자메일이나 메신저를 사용한다.

⑦ 원격에서 자신의 Smart Phone을 관리할 수 있는 서비스에 가입하여 이용한다.

V. 결 론

본 논문에서는 Smart Phone을 이용하여 Smart Phone의 인터넷 접속시 패킷을 분석하고, 그에 따른 취약점과 보안을 제시하였다.

2010년 9월[8] Smart Phone 가입자 절반이상이 PC대신 Smart Phone으로 e-Mail 이나 SNS를 이용하는 걸로 나타나있다. 이에 따라 Smart Phone의 사용량은 증가하고 있지만 보안에 대한 인식률은 낮은 편이다. 해커들을 이러한 점을 인식하여 개인정보를 탈취하여 악용되고 있다.

향후 연구로 3G 망에서 인터넷 이용 시 무선 패킷 분석 연구가 필요하다.

참고문헌

[1] 방송통신위원회, 한국인터넷진흥원, 스마트폰 이용실태조사, pp.9, 2010.07.

[2] 김정훈, 구글의 안드로이드와 안드로이드마켓, 한국콘텐츠학회지, 제7권 제2호, pp.29~36, 2009.6.

[3] Angela Orebaugh, Gilbert Ramirez, Josh Burke, Jay Beale, Wireshark and Ethereal network protocol analyzer toolkit, Syngress, pp. 52~53, 2007.

[4] 제갈병직, 스마트폰 시장과 모바일OS 동향, Semiconductor Insight, pp.9~18, 2010.05~06.

[5] Ravi Kalakota, Marcia Robinson, M-Business : Race to the Mobility, McGraw-Hill Companies, 2001.09.

[6] 천우성, 박대우, “WiBro 네트워크에서 메신저, VoIP 도청 및 포렌식 연구”, 컴퓨터정보학회지, 제14권 제5호, 2009.05.

[7] 홍범석, 이동통신 무선인터넷 망개방 현황과 시사점, 정보통신정책, 제19권 제13호, pp.1~17, 2007.07.

[8] 박영태, 스마트폰 가입자 절반 "PC 대신 휴대폰으로 이메일 SNS 이용", 한국경제, 2010.09. 29.