특집 09

스마트폰 환경에서의 보안 위협

목 차

장 상 근
(하우리 보안대응센터)

1. 서 론

1992년, IBM에서 최초로 Simon 이라는 스마트 폰을 선보였지만, 그 당시 미비한 모바일 네트워크 인프라와 당시 기술적 구현 등의 문제로 스마트폰의 성장이 걸음마 상태였지만, 2000년대에 들어 터치스크린의 구현, 최초의 스마트폰 전용 상용 OS인 Symbian OS가 출시되면서 스마트폰 시장이 비즈니스를 중심으로 성장하기 시작하였다.

최근 들어서는 고도화된 모바일 네트워크 인프라, 기기의 고성능화, 다양한 플랫폼들과 컨텐츠들이 충족되면서 국내를 포함하여 전 세계적으로 스마트폰 사용자가 증가 추세에 있다.

하지만, 컴퓨터에서 취약점 과 악성코드가 존재하듯이 스마트폰에서도 다양한 보안 위협이 점차적으로 발생되어지고 있다.

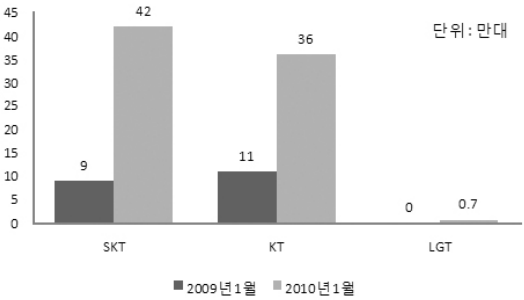
2. 스마트폰 시장 동향

최근 Apple社의 iPhone이 출시되면서, 전 세계적으로 일반 휴대폰에서 스마트폰으로 시장이 급변하고 있다. 이러한 급변 현상이 일어난 배경으로는 더 이상 기본적인 이동통신 서비스(음성 및 문자 데이터 송.수신)만을 통해서는 사용자에 대한 욕구를 만족 시키지 못하지만, 스마트폰은 장소에 구애 없이 기본 이동통신 서비스와 더불어 자유롭게 인터넷 접속이 가능하다는 점과 다양한 어플리케이션들이 제공된 다는 이점은 스마트폰을 통해 본격적인 유비쿼터스 세상을 열어가는 기반이 되어준다고 볼 수 있다. 이에 대한 근거로 세계적인 조사기관 중에 하나인 Gartner 에서의 내놓은 스마트폰 시장 관련 보고서와 함께 Gartner에서는 2013년이면 사실상 스마트폰이 PC를 대체할 것이라고 예측도 한 상황이다.

〈표 1〉에서와 같이 스마트폰 판매가 2008년 3분기 총 판매수가 36,557.4에서 2009년 3분기에는 41,067.6으로 약 13% 증가 할 정도로 성장세가 뚜렷하고, 국내 스마트폰 시장 동향 또한 불과 한달 사이에 급격히 스마트폰 판매가 증가할 정도로 스마트폰에 대한 관심세가 뚜렷한 것을 확인 할 수 있다.

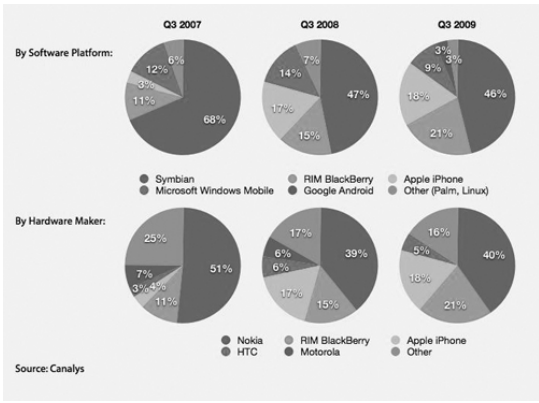
〈표 1〉 스마트폰 시장 점유율(출처 : Gartner)

업 체	2009 3분기 판매수(천대)	2009년 3분기 시장 점유율(%)	2008 3분기 판매수(천대)	2008년 3분기 시장 점유율(%)
Nokia	16,156.4	39.3%	15,472.3	42.3%
RIM	8,552.7	20.8%	5,800.4	15.9%
Apple	7.040.4	17.1%	4,720.3	12.9%
HTC	2,659.5	6.5%	1,656.3	4.5%
Samsung	1,320.6	3.2%	1,114.8	3%
Others	5,368.0	13.1%	7,793	21.3%
Total	41,067.6	100%	36,557.4	100%



(그림 1) 국내 이동 통신사 자료

이러한 시장 성장 가능성에 힘입어 스마트폰 플랫폼의 주도권을 두고 여러 플랫폼들이 시장에 나타나 사용자의 선택 폭을 넓게 해주고 있는 상황이다. (그림 2)는 스마트폰 플랫폼 시장 과 하드웨어 제조사 점유율에 대해 Canalys에서 조사한 자료이다.

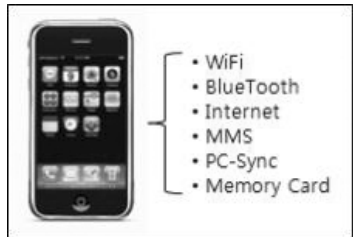


(그림 2) 스마트폰 플랫폼 점유율 및 제조사 점유율

현재 시점에서 스마트폰 시장을 긍정적으로 바라보는 시점이 많지만, 모바일 컨텐츠의 부족을 해소하기 위한 앱스토어처럼 컨텐츠를 활성화 할 수 있는 방안들, 과도한 무선 인터넷 요금 해결, 무선 통신망의 트래픽 처리용량 확대, 향후 발생 될지 모르는 모바일 보안 위협 등의 문제를 해결해야만 한다.

3. 스마트폰의 보안 위협

스마트폰이 과거에는 사용자도 적고, 플랫폼의 기능적 제약으로 인해 주목을 받지 못했지만, 현재 스마트폰은 고성능의 스펙을 갖추고 있으며, WiFi, BlueTooth 등 다양한 접속 경로를 갖추고 다른 매체들 간의 연결도 편리해 졌다.



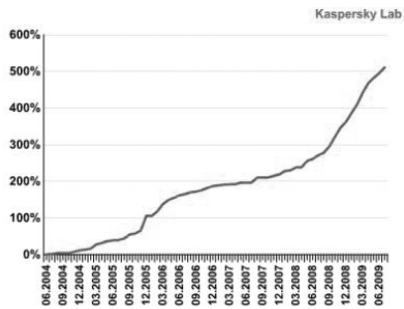
(그림 3) 스마트폰의 접속 경로

하지만, 보안을 고려해 본다면 접근성이 좋아 졌다는 것은 보안 위협에 노출 될 수 있는 영역이 더 많아 진 것이며, 악성코드 전파 경로 또한 다양해 졌다는 문제가 발생되었다. 또한 스마트폰

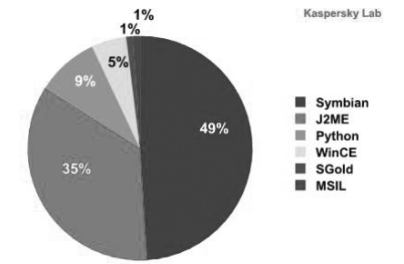
사용자가 증가할수록 스마트폰 어플리케이션들이 다양해 질수록 취약한 영역이 많아지고, 취약점을 이용한 공격들과 더불어 SNS(소셜 네트워크)를 통한 사회 공학적 공격 기법들이 나타날 수 있으며, 이외에 다양한 보안 위협이 발생할 수 있다. 이러한 스마트폰 보안 위협에 대응하기 위해서는 스마트폰이 주로 이용하는 무선 네트워크망에 대한 보안 강화 와 암호화 기술, 개인 정보 보호를 보호하기 위한 기술적인 측면과 법적인 측면에 대한 연구가 필요로 되고 있다.

3.1 모바일 악성코드

2004년 6월 14일 최초의 스마트폰 악성코드인 Cabir Worm 이 블루투스를 통해 전파된 이후 현재까지 수천 종의 스마트폰 악성코드가 발견되고 있으며, (그림 4)처럼 카스퍼스키랩 보고서에 따르면 모바일 악성코드가 빠르게 증가하고 있다는 것을 확인할 있다. 그리고 (그림 5)를 통해 다양한 플랫폼에서도 모바일 악성코드들이 활동하고 있다는 점도 알 수 있다.



(그림 4) 모바일 악성코드 증가.(2004~2009)



(그림 5) 플랫폼별 모바일 악성코드 현황

이러한 모바일 악성코드로 인한 피해 유형은 스마트 폰의 내부 파일 변조 및 삭제형, 베터리 소모형, 금전적 피해 유발형, 정보 유출형, 특정 문자 메시지 보내기형, 스마트폰 원격 제어 기능 등을 하는 모바일 악성코드들이 주로 발견되어지고 있다.

(그림 6) Worm/Commwarrior

(그림 7) Worm.SymbOS.Yxe

이외에 모바일 피싱인 SMS 와 Phishing 의 합성어인 스미싱(SMiShing)은 문자 메시지에

특정 사이트를 접속할 수 있도록 유도하여, 접속 될 경우 개인 정보를 탈취해 가는 VBS/Eliles 라는 모바일 악성코드가 발견되기도 하였으며, Commwarrior 라는 악성코드는 감염된 스마트폰의 전화번호부에 등록되어진 사람들에게 MMS 메시지를 보내는 기능을 하는 악성코드가 발견되었다. 앞으로는 WiFi를 이용하여 악성코드를 전파하는 악성코드가 발생 될 수 있고, 최근 모바일 악성코드 동향에 비추어 볼 때 개인적인 측면에서는 SNS(소셜 네트워크)를 통한 개인 정보 유출 및 피싱을 활용한 모바일 악성코드의 출현이 발생 될 수 있다. 그리고 국가기관, 기업에

서 스마트폰을 도입할 경우에는 악성코드 제작자가 공공기관 네트워크 및 기업 네트워크에 침입할 수 있는 모바일 악성코드들이 출현할 가능성이 높아지고 있다.

3.2 모바일 App 취약점 공격

앱스토더를 중심으로 수 없이 많은 스마트폰용 어플리케이션들이 개발되어 지고 있다. 하지만 수 많은 어플리케이션에 대한 정밀한 보안 검증을 할 수 있는 환경이 되지 않아 취약한 어플리케이션들의 취약점들을 이용한 공격이 나타나고 있다.

```
<html>
        Copyright Georgi Guninski
        <br>
        Cannot be used in vulnerability databases
        <br>
        Especially securityfocus/mitre/cve/cert
        <script>
        var s=String.fromCharCode(257);
        var ki="";
        var me="";
        for(i=0;i<1024;i++)
        {ki=ki+s;}
        for(i=0;i<1024;i++)
        {me=me+ki;}
        var ov=s;
        for(i=0;i<28;i++) ov += ov;
        for(i=0;i<88;i++) ov += me;

        alert("done generating");
        var fuckbill=escape(ov);
        alert("done escape");
        alert(fuckbill);
        </script>
</html>
```

(그림 8) iPhone Safari exploit Code

최근에 발생된 예로 iPhone에서 웹 브라우저로 사용되고 있는 사파리의 취약점을 이용한 원격 실행 DOS 취약점 Exploit 코드가 공개된 사례도 있다.

이러한 모바일 어플리케이션들이 다양해 질수록 특정 인기 어플리케이션들의 보안 취약점을 노린 공격은 불법적인 네트워크 접근 및 모바일 기기 제어 권한 획득 등의 문제가 발생될 수도 있으며, 검증되지 않은 무료 제공 모바일 어플리케이션에 악성코드를 숨겨놓을 수 있다는 문제가 제기되고 있다.

3.3 모바일 플랫폼 공격

모바일 플랫폼의 취약점을 이용하여 제한되어진 환경에서 벗어나 다양한 기능과 어플리케이션을 구동시키기 위한 연구가 활발히 진행중에 있다. 최근 사례로 iPhone에서 제한된 기능을 사용하기 위해 JailBreak를 하여 제한된 기능을 사용할 수 있도록 한 것이 이슈화 되고 있다.

```
root@iphone's password:
Welcome to Darwin!
iPhone$ uname -a
Darwin iPhone 9.0.0d1 Darwin Kernel Version 9.0.0d1: Wed Sep 19 00:08:43 PDT 200
7; root:xnu-933.0.0.203.obj~21/RELEASE_ARM_S5L8900XRB iPhone1,1 Darwin
iPhone$ ls -l /
total 17
drwxrwxr-x  23 root admin  782 Oct  8 11:31 Applications
drwxrwxr-t  10 root admin  340 Sep 19 22:12 Library
drwxr-xr-x   3 root wheel  102 Sep 19 21:39 System
drwxr-xr-x 102 root wheel 3468 Oct  8 10:17 bin
drwxrwxr-t   2 root admin   68 Sep 19 02:42 cores
dr-xr-xr-x   3 root wheel  728 Oct  8 11:19 dev
lrwxr-xr-x   1 root admin   11 Sep 19 22:11 etc -> private/etc
drwxr-xr-x   5 root admin  170 Oct  8 10:01 iTunes_Control
lrwxr-xr-x   1 root admin   11 Sep 19 22:11 mach -> mach_kernel
drwxr-xr-x   4 root wheel  136 Oct  8 01:13 private
drwxr-xr-x  16 root wheel  544 Oct  8 10:16 sbin
lrwxr-xr-x   1 root admin   15 Sep 19 22:11 tmp -> private/var/tmp
drwxr-xr-x   8 root wheel  272 Oct  8 10:39 usr
lrwxr-xr-x   1 root admin   11 Sep 19 22:11 var -> private/var
iPhone$ date
Mon Oct  8 11:37:22 EDT 2007
iPhone$
```

(그림 9) iPhone JailBreak

하지만 JailBreak 된 iPhone 은 기능 제한이 된 상황에서 일어나지 않는 보안 위협에 노출 될 수 있다는 문제점을 갖고 있으며, 위험도가 높은 모바일 플랫폼 공격이 출현한다면 이동 통신망 및 무선 네트워크 장애가 발생될 수 있다.

3.4 보안이 고려되지 않는 네트워크 접속

스마트폰이 사용하는 대표적인 네트워크망은 이동 통신사 망, WiFi(무선 인터넷 망), 블루투스등이 사용되는데 초창기 블루투스를 통해 전파되는 악성코드가 출현하였으며, 앞으로는 이동 통신사망, 보안이 취약한 WiFi 망에 접속함으로서 패킷 스니핑, 피싱 등의 공격에 노출될 수 있다.

(그림 10) SmartPhone 환경에서의 MITM 공격

(그림 11) iPhone Safari 로 접속중인 패킷 스니핑

(그림 10) 과 같이 어떤 특정 AP에 접속하여 인터넷을 사용하고 있는 특정 스마트폰을 대상으로 MITM(Man-in-the-Middle) 공격을 시도하여, (그림 11)와 같이 스마트폰 패킷 스니핑에 성공할 수 있다.

위와 같은 네트워크 취약성을 이용하여 통신 패킷 정보를 수집하여 원하는 정보를 획득하거나 네트워크망을 오염시킬 수 있는 문제가 발생할 수 있다.

4. 결 론

스마트폰 시대는 본격적인 유비쿼터스 세상으로 진입하는 계기가 되고 있으며, 스마트폰을 기반으로 한 새로운 서비스나 산업들이 조성될 수 있는 기회가 되었다. 하지만 그 동안 발견되지 않았던 새로운 보안 위협이 발생될 수 있는 가능성 또한 높아 만지고 있다.

스마트폰의 보안 위협은 이동통신망, 무선 네트워크, 블루투스 등 다양한 접속 경로가 있으므로 인해 악성코드등이 급속히 전파될 수 있는 좋은 환경이 될 수 있다. 해외의 경우에는 블루투스를 이용한 악성코드 전파에 대한 보안 위협 사례가 나오기도 했지만, 국내의 경우 현재까지 이슈가 될 만한 스마트폰 보안 위협이 발생되지 않고 있다. 하지만 국내 스마트폰 사용자가 급속하게 증가하고 있는 상황에서 철저한 보안 정책과 보안 시스템 구축에 소홀하게 된다면 최악의 경우에는 통신망 장애가 발생될 수 있다.

스마트폰의 보안 위협을 최소화하기 위해서는 통신 과정에서의 암호화 기술 사용, 스마트폰 보안 솔루션 개발, 무선 통신망 보안 장비등에 대한 연구가 필요로 되어진다.

참고문헌

[1] From 0 to zero-day on symbian : Finding low level vulnerabilities on symbian smartphones, 06/2009

[2] Study of MITM Attacks Against Smartphone Devices, Smobile systmes, Oct 22,2009

[3] An Analysis of the iKee.B (Duh) iphone Botnet, SRI INTERNATIONAL, 14 December 2009

[4] iPhone Privacy, Black Hat DC 2010, Nicolas Seriot

[5] Mobile Malware Evolution: An Overview, Viruslist, Sep 29 2009

[6] Competitive Landscape: Mobile Devices, Worldwide, 3Q09, Gartner, 11 November 2009

[7] 모바일 인터넷 정보보호를 위한 모바일 악성코드 동향 분석, 정보보호학회, 2009. 12

저자약력

장 상 근

2009년 세종대학교 컴퓨터공학과(학사)
2001년~2002년 J&G Ent. 연구원.
2007년~현재 하우리 보안대응센터 연구원.
관심분야 : 악성코드, 리버스 엔지니어링(자동 분석),
네트워크 보안, Management of Technology
이 메 일 : maxoverpro@paran.com