제1호 발로뛰는 중소기업 호민관

국회의원 정태근

『중소기업을 살린다』
국정감사 자료집 제 9 호

손에 든 시한폭탄, 스마트폰

- 스마트폰 보안위협 -

2010. 10.

국회 지식경제위원회
국회의원 정태근

손에 든 시한폭탄, 스마트폰

1 | 이동하는 컴퓨터

□ 스마트폰은 부가기능이 많은 휴대전화기가 아닌 전화기능이 추가된 초소형 컴퓨터

□ 전세계 스마트폰 판매량이 '10년도 2분기 기준 전년 동기 대비 50.5% 증가하는 등 스마트폰은 급속히 확산 中

2 | 만연한 스마트폰 보안위협

□ 스마트폰에 감염된 악성코드는 개인정보 유출뿐만 아니라 사용자 위치 추적, 음성 도청 등의 악성행위도 가능하여 일반 PC에 비해 더 심각한 보안위협에 직면

□ 항시 몸에 휴대하는 스마트폰은 도난 및 분실의 위협이 상시 존재하며, 도난 및 분실 시 스마트폰에 저장된 메일서버 계정정보 등이 악용될 수 있어 명의 도용 문제 심각

3 | 현실화되고 있는 피해사례

□ 국내를 포함하여 러시아, 네덜란드 등에서 스마트폰 악성코드를 이용한 금전적 목적의 공격 발생

□ 게임으로 가장하여 스마트폰에 설치된 후 사용자의 위치를 추적하는 악성코드 발견

□ 이미 '07년부터 미국에서는 스마트폰을 이용한 음성 도청 사건이 사회적 이슈로 부각

□ 모바일 뱅킹 프로그램으로 위장하여 계좌 비밀번호 유출 사건 발생

4 | 스마트폰 보안기술 개발 시급

□ 절반에 가까운 스마트폰 사용자가 보안에 대한 필요성을 인식하지 못하고 있어 사용자들의 보안의식 제고 절실

□ 배터리 제약, 낮은 하드웨어 성능과 같은 스마트폰의 특성을 고려하면서 사용자 위치추적, 음성 도청 등과 같은 새로운 보안위협을 해결하기 위한 기술 개발 시급

< 목 차 >

I. 개요

1. 스마트폰 특징

□ 전화기능이 탑재된 초소형 컴퓨터

o 스마트폰은 기존의 음성통화를 제공하는 휴대전화와 스케줄링 및 정보관리 기능을 제공하는 개인용 휴대정보단말기(PDA, Personal Digital Assistant)를 결합한 복합형 통신 단말기

o 대부분의 스마트폰은 멀티태스킹 기능 제공

□ 프로그램 개발자를 위한 표준화된 인터페이스와 플랫폼 제공

o 범용 운영체제를 사용하여 애플리케이션 개발 및 배포 용이

□ 네트워크 통신 기능 향상

o 무선랜을 통해 높은 대역폭의 인터넷 서비스 제공

2. 스마트폰 도입 추세

□ 전 세계적으로 스마트폰 판매량의 폭발적 증가

o '10년 2분기 스마트폰 판매 전년 동기 대비 50.5% 성장

*** 출처 : 2분기 스마트폰 판매, 전년 동기 대비 50.5% 증가(ITdaily, '10.08)**

o '08년 대비 '09년 판매량이 23.8% 증가하였으며, '13년까지 매년 20% 증가 예상

*** 출처 : Competitive Landscape: Mobile Devices, Worldwide, 4Q09 and 2009 (가트너, '10.02)**

[그림 1] 스마트폰 판매량 증가 추세

□ 국내 스마트폰 사용자의 급격한 증가

o 아틀라스 리서치에 따르면 스마트폰의 국내 휴대전화 시장 점유율이 '09년 3분기 1.9%에서 '10년 2분기 16.6%로 증가

*** 출처 : SKT-삼성, KT-애플 잡았다(아시아경제, '10.06)**

o '10년 2월 스마트폰 이용자 125만명에서 9월 기준으로 390만명 돌파

*** 출처 : 즐겨라! 스마트 추석...명절 연휴 풍속도 확 바꾸는 스마트폰 100배 즐기기 (쿠키뉴스, '10.09)**

o 방송통신위원회와 이동통신 3사의 전망에 따르면 '10년 스마트폰 가입자 수가 600만명, '11년에는 1650 ~ 1800만명으로 전망

*** 출처 : 국내 스마트폰 '비약적 성장'(파이낸셜뉴스, '10.08)**

o 중저가 보급형 스마트폰들의 출시로 인해 소비자층 확대 예상

- '10년 10월부터 연말까지 25종의 신생 스마트폰 출시 계획

*** 출처 : 신생폰 연말까지 25개 와르르...스마트폰** 大戰**(쿠키뉴스, '10.09)**

□ 국내 기업의 모바일 오피스 도입 증가

o 많은 국내 기업들이 업무처리의 효율성을 위해 메일, 업무 결재, 일정 관리, 직원 검색 등이 가능한 모바일 오피스 시스템 도입 추진

o 40여 개의 삼성그룹 관계사를 비롯하여 대한항공·한진해운·사이버로지텍·GS칼텍스 등 55개 기업이 모바일 데스크 도입('10년 3월 기준)

- 스마트폰을 통해 회사 인트라넷에 접속하여 메일 열람과 결재, 일정관리, 직원 조회 등 가능

*** 출처 : 스마트폰 혁명 ② – 모바일 오피스 시대 개막(이코노미플러스 통권 65호, '10.03)**

o 도시철도공사는 지하철 유지관리시스템(UTIMS)를 구축하여 스마트폰을 이용한 현장 사고 접수, 작업 지시 수령 보고에 활용

*** 출처 : 도시철도공사, 현대차 등 모바일 오피스 도입 확산(조선일보, '09.01)**

o 국내 500개 이상의 기업이 통신사들과 모바일 오피스 구축 계약 체결

*** 출처 : SK텔레콤, 모바일오피스 도입기업 500개 돌파(디지털데일리, '10.08)**

3. 스마트폰에 의한 환경변화

□ 생활 패턴의 변화

o 언제 어디서나 인터넷에 연결되어 있어 온·오프라인의 융합

- 실시간 소통에 적합한 소셜 네트워크 유행

o 이메일, 인터넷 뱅킹 등 신속하고 편리하게 개인 업무 처리 가능

o 모바일 오피스를 통해 외부에서도 실시간 업무 처리 가능

□ 새로운 비즈니스 모델 창출

o 전세계 스마트폰 애플리케이션 시장은 '10년 68억 달러에서 '13년 295억 달러로 약 4배 이상 확대 전망

*** 출처 : Big Boost is Forecast for App Stores(가트너, '10.01)**

□ 기업 간 경쟁구도 변화

o 디스플레이, 카메라 화소 등 하드웨어 중심으로 전개되던 기업간 경쟁이 애플리케이션과 같은 콘텐츠 중심으로 이동

*** 출처 : 스마트폰이 열어가는 미래(삼성경제연구소 보고서, '10.02)**

□ 보안 위협 증가

o 스마트폰은 항상 휴대하고 켜져 있다는 특성으로 인해 기존의 데스트탑보다 더 심각한 보안 위협에 직면

o 공개된 개발 환경과 플랫폼을 이용하여 누구나 쉽게 어플리케이션을 개발할 수 있어 악성코드에 대한 보안 위협 증가

o 오픈 마켓을 통해 악성 프로그램들이 자유롭게 유포되고 있어 피해 사례 증가

o 악성코드에 감염될 경우 이메일, 문자, 사진 및 개인 위치 정보 노출 등 심각한 사생할 침해 발생

Ⅱ. 스마트폰 보안위협

1. 악성코드 위협

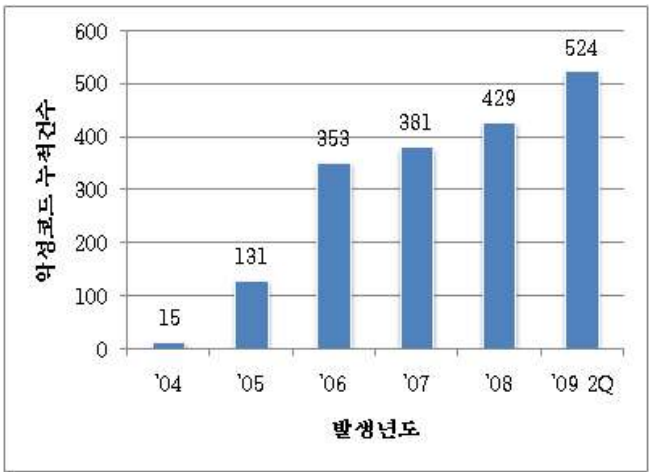
□ 악성코드의 공격 대상이 스마트폰으로 확대

o 스마트폰에서도 범용적인 운영체제를 사용함에 따라 악성코드 개발 및 유포 용이

o 일반 PC보다 스마트폰에 악성코드를 설치하면 사용자 위치 추적, 음성 도청 등 더 많은 개인정보 획득 가능

□ 지속적으로 증가하는 스마트폰 악성코드

o 발견된 스마트폰 악성코드 수는 '09년 2분기에만 524건으로 '08년도 악성코드 수를 상회



[그림 2] 모바일 악성코드 증가 추이

*** 출처 : 인터넷침해사고 동향 및 분석 월보(한국인터넷진흥원, '09.09)**

□ 악성코드 전파 경로 다양화

o 문자메시지, 웹서핑, 오픈마켓, 애플리케이션 취약점 등을 통해 악성코드 감염 가능

2. 분실 및 도난 위협

□ 심각성

o 스마트폰은 작고 가볍우며 항상 휴대하기 때문에 도난 및 분실의 위험 상존

□ 분실 및 도난에 따른 보안위협

o 개인정보 유출

- 분실 및 도난시 스마트폰에 저장된 개인정보 유출 가능

o 스마트폰 사용자 신분 도용

- 불법 습득자는 스마트폰에 저장된 메일서버, 메신저 등의 로그인 정보를 이용하여 소유자의 명의를 도용 가능

- 소유자의 사회적 지위와 신분에 따라 금전요구와 같은 피싱공격을 수행할 경우 심각한 피해 발생 가능

o 금전적 피해

- 불법 습득한 스마트폰으로 전화통화, SMS/MMS, 인터넷, 각종 유료 부가서비스 등을 사용하여 과금 피해 발생 가능

3. 무선랜 보안위협

□ 스마트폰은 3G 데이터 통신뿐 아니라 무선랜(Wi-Fi)을 통해 웹서핑, e-mail 열람 등 인터넷 서비스 이용 가능

□ 무선 AP의 보안 설정이 취약한 경우 허가받지 않은 사용자의 무단 접속 및 패킷 스니핑[1]을 통한 개인정보 유출 가능

o 평문통신을 하거나 안전하지 않은 암호화 통신을 수행하는 경우 패킷 스니핑을 통해 쉽게 도청 가능

□ 비인가 AP을 통해 인터넷에 접속할 경우 통신내용 도청 및 피싱 공격 가능

o 유동인구가 많은 지역에 가짜 AP를 설치하고 스마트폰 사용자의 접속을 유도하여 개인정보를 수집하거나 피싱사이트로 유인 가능

1) 패킷 스니핑이란, 네트워크에서 전달되는 패킷을 가로채어 그 내용을 보는 행위

4. 탈옥 및 루팅 위협

□ 탈옥과 루팅을 이용하여 제조사가 설정한 보안기능 해제 가능

o 애플은 자사에서 운영하는 앱스토어에서 다운로드한 애플리케이션만을 아이폰에 설치할 수 있도록 제한하고 있으나 탈옥한 아이폰에서는 임의의 애플리케이션 설치 가능

o 안드로이드에서는 사용자가 설치한 애플리케이션이 관리자 권한으로 동작할 수 없지만, 루팅한 안드로이드에서는 관리자 권한으로 애플리케이션 실행 가능

□ 탈옥을 통해 웹, 이메일 등 신뢰할 수 없는 곳에서 애플리케이션을 다운로드받아 설치하는 경우 악성코드 감염에 노출

o 탈옥된 폰을 대상으로 SSH 취약점을 이용하여 배경화면을 바꾸는 악성 코드 전파

*** 출처 : 아이폰서 동작하는 세계 첫 '웜'발견(전자신문, '09.11)**

□ 루팅된 안드로이드 폰에서는 악성코드가 관리자 권한으로 실행될 수 있어 주요 정보 유출 가능

o 안드로이드에서는 악성코드가 설치되더라도 타 애플리케이션의 데이터 접근이 제한되지만, 관리자 권한으로 실행된 악성코드는 타 애플리케이션의 데이타 접근 가능

5. SW 보안위협

□ 스마트폰용 SW에서 다양한 취약점이 발견되고 있으며 이를 이용한 악성코드 전파 및 공격 발생

o 대부분의 애플리케이션이 보안에 대한 아무런 검증 없이 배포되고 있어 많은 취약점 내포

<표 1> 스마트폰용 SW 취약점

스마트폰 운영체제	취약점
아이폰	• 악의적인 목적으로 만든 TIFF 파일을 통해 응용프로그램 종료되거나 임의의 프로그램 실행 가능 (CVE-2010-1811) • 악의로 만든 웹페이지 접속시 응용프로그램이 종료되거나 임의의 코드가 실행 (CVE-2010-1770, CVE-2010-1771, CVE-2010-1780~1788, CVE-2010-1791, CVE-2010-1793, CVE-2010-1812~1815)
안드로이드	• 안드로이드용 Adobe flash player의 0-day 취약점을 통해 임의의 코드 실행 가능(CVE-2010-2884) • 악의의 SMS를 수신하거나 악성코드 실행 시 시스템 재부팅(CVE-2009-2999)

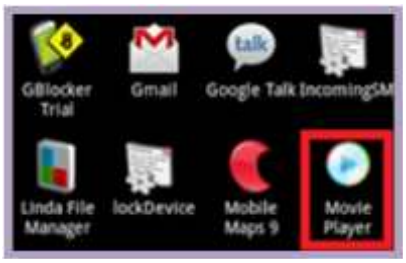
III. 피해사례

1. 금전적 손실

□ 무단으로 SMS 발송 후 이용료를 부과하는 악성코드 사례

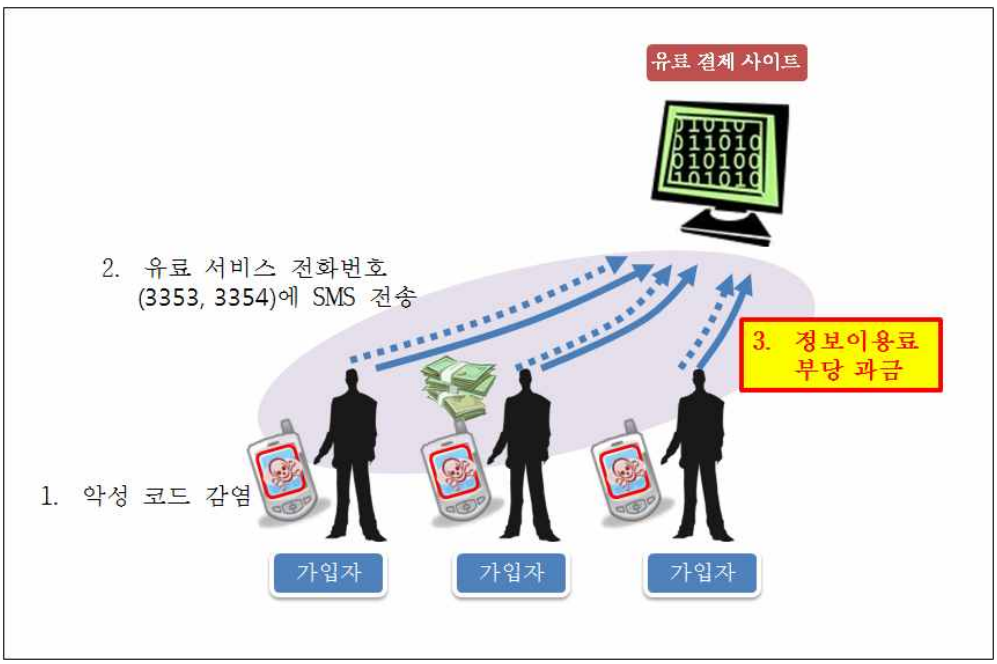
o Trojan-SMS라는 안드로이드용 악성코드가 러시아에서 발견

o Trojan-SMS는 멀티미디어 재생기로 가장하여 사용자의 설치 유도



[그림 3] 악성코드 설치모습

o 설치된 Trojan-SMS는 사용자 동의없이 유료 서비스 전화번호로 SMS를 발송하여 과금 유발



[그림 4] Trojan-SMS 동작 과정

*** 출처 : 러시아서 안드로이드폰 공격 바이러스 발견(SBS 뉴스, '10.08)**

□ 네델란드 아이폰 사용자를 대상으로한 금전적 목적의 공격 사례

o 두웜(Duh Worm)은 탈옥된 아이폰의 취약점을 이용하여 전파

o 두웜에 감염되면 아이폰이 해킹되었으니 특정 사이트에 접속하라는 경고 메시지 출력

[그림 5] 두웜에 의해 해킹된 아이폰

o 해당 사이트에 접속하면 개인정보를 보호하는 방법을 알려주는 대가로 5유로를 특정 페이팔 계좌로 보내도록 요구

o 네델란드의 많은 아이폰 사용자들이 공격자에게 5유로 입금

*** 출처 : 아이폰 해킹 전용 웜 등장...해커들 스마트폰 눈독(보안뉴스, '09.11)**

□ 국제전화를 통한 과금유발 시도 사례

o 윈도우 모바일용 악성코드인 트레드다이얼(TreDial)은 모바일 게임과 동영상 관련 유틸리티를 통해 유포

o 트레드다이얼은 사용자 동의 없이 50초 간격으로 국제전화를 시도하여 과금 유발

o 방송통신위원회와 안철수 연구소에 따르면 트레드다이얼에 의해 국내에서 총 155건 감염 발생

- 악성코드가 시도한 국제 전화번호가 실제로는 존재하지 않아 다행히 피해 미발생

[그림 6] 트레드다이얼 동작 방식

*** 출처 : 스마트폰 악성코드 트레드다이얼(서울신문, '10.04)**

2. 사용자 위치추적

□ 게임으로 위장하여 사용자 위치 정보 유출 사례

o 악성코드 Android-Trojan/Snake는 게임 기능을 제공하면서 사용자의 동의 없이 위치 정보 전송

*** 출처 : 안철수연구소 월간 보고서('10.08)**

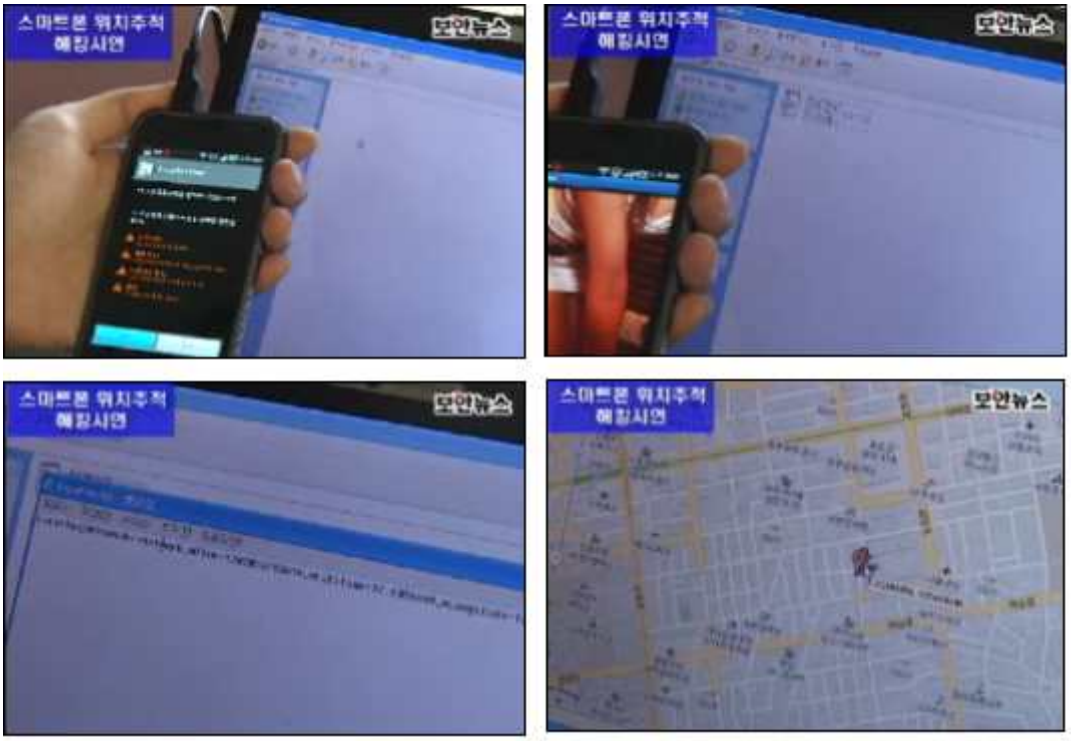
□ 안드로이드폰 사용자의 위치추적 시연 사례

o 국내 스마트폰 보안 업체에서 악성 프로그램을 이용하여 안드로이드폰 사용자의 위치를 추적하는 방법 시연

o 공격자는 악성코드를 성인물로 가장하여 웹 등을 통해 배포

o 스마트폰에 설치된 악성코드는 사용자의 위치 정보를 공격자 서버로 전송

o 공격자는 전송된 위치정보를 이용하여 온라인 지도사이트에서 사용자의 정확한 위치 확인 가능



[그림 7] 해커의 위치 추적 시연

*** 출처 : 스마트폰 위치추적, 내 위치는 해커 손바닥!(보안뉴스, '10.08)**

3. 음성 도청

□ 미국에서 스마트폰에 의한 도청 피해 사례

o 미국에서 스마트폰에 악성코드를 삽입해 카메라를 통해 한 가족의 사생활을 훔쳐보고 대화내용을 도청하는 피해 사례 발생

o 악성코드는 사용자의 모든 통화 내역을 공격자에게 전송되고, 통화내용 도청도 수행

[그림 8] 미국에서 발생한 도청 사례

* 출처 : CELLULAR PHONES The Shocking Truth Reveal(CNN, '07.11)

□ 인터넷을 통해 판매 중인 스마트폰 도청 프로그램 사례

o 다양한 스마트폰에 대해 통화내역, SMS, E-mail 등을 무단 열람할 수 있는 도청 프로그램을 인터넷에서 구입 가능
  - 예) Flexispy, Mobile Spy, Mobistealth 등

o 5분내외의 시간동안 스마트폰을 물리적으로 점유한 상태에서 도청 프로그램 설치 가능

o 공격자는 원격에서 도청 프로그램을 통해 스마트폰의 통화내역, SMS 열람뿐만 아니라 음성 도청 가능

[그림 9] FlexiSPY를 통해 도청된 정보 리스트

*** 출처 : 스마트폰, 악성코드 안전지대 아니다(안철수연구소, '09.03)**

4. 금융정보 유출 사례

□ 모바일 뱅킹 프로그램으로 위장한 악성코드 사례

o Droid09라는 아이디를 가진 개발자는 39종의 미국 은행 및 신용조합의 인터넷뱅킹 프로그램으로 위장한 악성코드를 만들어 유포

o 악성코드는 이용자가 입력하는 은행 비밀번호를 공격자에게 전송

[그림 10] 인터넷뱅킹 피싱 프로그램 화면

o 안드로이드 마켓의 경우 애플리케이션에 대해 별도의 등록 심사

과정을 거치지 않아 해당 악성코드의 등록 및 유포에 악용

*** 출처 : 안드로이드용 인터넷뱅킹 비밀번호 유출 공포 확산(아이뉴스24, '10.01)**

5. 프라이버시 침해 사례

□ 배경화면 애플리케이션을 이용한 개인정보 무단 수집 사례

o '재키 월페이퍼'는 배경화면 관리 기능을 제공하면서 안드로이드폰 사용자의 휴대폰 번호, 가입자 ID, 등록 전화번호 및 이메일 계정은 물론 음성메일의 패스워드까지 수집

*** '재키 월페이퍼'는 수백만건의 다운로드 기록**

[그림 11] 안드로이드폰에서 재키 월페이퍼 설치 화면

*** 출처 : 중국서 개발한 안드로이드용 앱, 개인 정보 무단 수집(아시아경제, '10.07)**

□ 주식시세정보 제공 애플리케이션을 이용한 개인정보 수집 사례

o '10년 3월22일부터 8월30일까지 안드로이드 마켓에서 스마트폰용 주식시세정보제공 애플리케이션을 배포하고 사용자 동의를 받지 않은 채 개인정보 8만 3416건 취득

*** 출처 : 檢, 주식시세앱 개인정보 유출 적발(파이낸셜 뉴스, '10.09)**

□ 개인정보를 유출하는 다수의 불법 애플리케이션 유포 사례

o 미국 모바일 보안업체인 룩아웃이 최근 아이폰과 안드로이드폰의 애플리케이션 30만 건을 분석한 결과 약 30%의 애플리케이션이 사용자의 동의 없이 국적이나 위치정보 등 유출 가능 확인

* 출처 : 스마트폰 공짜앱 통해 개인정보 줄줄 샌다(한국경제, '10.08)

6. 단말기 불능화 사례

□ 안드로이드 SMS 처리모듈의 DoS 취약점

o 악성 SMS 메시지를 전송하여 안드로이드 폰이 일시적으로 셀룰러 네트워크와 연결이 단절되는 취약점 발견('09.06.19)

□ 단말기 부팅 방해 사례

o 2005년 발견된 'Fontal'은 손상된 글꼴을 설치하여 재부팅 방해

□ 애플리케이션 작동 방해 사례

o 2005년 발견된 'Hobbes'은 백신 프로그램으로 위장하여 설치 후 정상적인 애플리케이션의 사용 방해

□ 배터리 소모로 인한 단말기 불능화 사례

o 2007년 등장한 'Stearwar'는 과도한 블루투스 트래픽을 생성하여 급격한 배터리 소모 유발

7. DDoS 좀비로 악용 사례

□ 스마트폰을 이용한 분산서비스거부(DDoS) 공격 발생 경고

o 스마트폰 사용자 증가에 따라 DDoS 공격의 좀비로 악용 가능

o 스마트폰의 경우 항상 켜져있다는 점으로 인해 DDoS 공격에 항시 활용 가능하다는 심각성 존재

o 사용 트래픽 양만큼 과금되는 스마트폰 특성상 개개인에게 직접적인 금전적 피해 예상

* 출처 : 인터넷 침해사고 동향 및 분석 월보(한국인터넷진흥원, '09.12)

IV. 스마트폰 보안 기술 현황

1. 백신 기술

□ 패턴 기반 악성코드 탐지 기술 사용

o 알려진 패턴을 이용하여 악성코드를 탐지하므로 신규 악성코드 탐지 난해

o 일부 모바일 백신은 행위기반 탐지기술을 채택하고 있으나 오탐율 문제로 인한 실용성 미비

□ 스마트폰 운영체제에 따라 백신 기능에 제약 존재

<표 2> 스마트폰 백신 기능 제약

스마트폰 운영체제	기능 제약
아이폰	• 제한된 멀티태스킹으로 인해 악성코드에 대한 실시간 감시 난해 • 탈옥 여부에 대한 탐지 정도만 수행
안드로이드	• 일반 사용자 권한으로 동작하기 때문에 다른 애플리케이션의 폴더에 저장된 파일들에 대해서는 악성코드 검사 불가 • SD 메모리카드와 같이 읽기가 허용된 영역에 대해서만 백신 검사 수행 가능
윈도우 모바일	• PC에서와 동일하며, 기능 제약 부재(6.X 버전 기준)

2. VPN 기술

□안드로이드, 아이폰, 윈도우 모바일 등 주요 스마트폰에서 다양한 VPN 기술들이 기본으로 탑재되어 있으며 기존의 VPN 서버 솔루션과 연동 가능

o IPSec, OPENVPN, Cisco VPN 등 지원

□사용자의 이동으로 스마트폰의 IP 주소가 변경되면 VPN 채널 단절 문제

o 이동 중 기지국이 변경되거나, 네트워크 통신방식이 변경될 경우, 스마트폰의 IP 주소가 재할당되고 VPN 채널 단절

3. 스마트폰 원격제어

□ 스마트폰의 분실 및 도난에 대비한 보안 솔루션

□ 원격으로 스마트폰을 관리할 수 있는 기업용 솔루션 존재

o 이메일 서비스를 기반으로 원격 애플리케이션 설치, 원격 잠금, 원격 자료 삭제, 위치 추적 등 가능

□ 개인용 스마트폰의 경우, 통신사의 부가서비스나 모바일 보안 애플리케이션 형태의 원격제어 솔루션 존재

o SMS를 기반으로 원격 잠금, 원격 자료 삭제, 위치 추적 기능 제공

4. 암호화 기술

□ 스마트폰의 운영체제에서 암 복호화를 위한 API를 제공하여 암호화 애플리케이션 개발 지원

o SSL 암호화 통신 및 데이터 암호화를 위한 API 제공

5. 키보드 입력 보안 솔루션

□ 터치 자판 배열을 무작위로 변경하는 가상 키패드 기술 상용화

o 모바일뱅킹 등에서 비밀번호를 입력할 때마다 자판 배열이 달라지므로 사용자가 터치한 위치를 기반으로 비밀번호 유추 난해

[그림 12] 가상 키패드 화면

6. 문서보안

□ 읽기 전용 뷰어에서 스트리밍 방식으로 문서를 열람할 수 있는 모바일 오피스 솔루션 출시

o 스마트폰 내부에 문서를 저장하지 않아 자료 유출 방지 효과

o 스마트폰 화면을 캡쳐하거나 외부 사진기를 이용하여 스마트폰 화면을 촬영할 경우 정보 유출 가능

o 화면 캡쳐 방지 기술이 적용되더라도 기술 수준에 따라 우회 가능

Ⅴ. 보안위협 대응방안

1. 사용자 인식 제고

□ 스마트폰 사용자의 절반은 보안문제에 무관심

o 스마트폰 사용자의 47.2%('매우 걱정됨' 9.5%, '걱정됨' 37.7%)만이 스마트폰 보안 문제를 걱정

*** 출처 : 2010년 스마트폰이용실태조사 보고서(한국인터넷진흥원, '10.07)**

□ 스마트폰 보안위협 완화를 위해서는 사용자의 보안의식 제고 필요

o 스마트폰을 전화기가 아닌 컴퓨터로 인식하고 백신 프로그램을 설치하여 악성코드 감염 예방 필요

o 오픈 마켓, 이메일, 메신저, SMS/MMS 메시지를 통해 다운로드받은 애플리케이션은 신뢰할 수 있는 경우에만 설치

o 스마트폰에 반드시 비밀번호를 설정하여 도난 및 분실시 개인정보 유출 방지

o 신뢰할 수 있는 무선랜에 접속하고, 반드시 암호화 통신 사용

o 스마트폰의 보안기능을 해제하거나 제한하는 탈옥이나 루팅 금지

2. 스마트폰 보안기술 개발 필요

□ 기존의 데스크탑에서는 존재하지 않던 새로운 보안위협을 해결하기 위한 기술 개발 필요

o 악성코드에 의한 음성 도청, 사용자 위치 추적 등과 같은 새로운 보안위협에 효과적으로 대응하기 위한 보안기술 개발 필요

o 항시 스마트폰을 휴대한다는 특성으로 인해 발생하는 분실 및 도난 문제를 해결하기 위한 보안기술 개발 필요

□ 스마트폰의 특성을 반영한 보안기술 개발 필요

o 스마트폰은 데스크탑에 비해 배터리 제약이 크고, 낮은 하드웨어 사양을 가지므로 이를 고려한 보안기술 개발 필요

- o 안드로이드, 아이폰 OS, 윈도우즈 모바일, 바다, 심비안 등 다양한 스마트폰 운영체제에 적용할 수 있는 보안기술 개발 필요
- o 스마트폰에서는 유선통신이 불가능하고 무선통신에만 전적으로 의존하므로 안전한 무선통신 사용을 위한 보안기술 개발 필요
- o 스마트폰의 이동성을 고려한 보안 기술 개발 필요