스마트폰 보안사고 분석*

김정배, 안석화, 이옥연
국민대학교 수학과
kimjb1985@gmail.com, {shahn , oyyi}@kookmin.ac.kr

Analysis for Security Accidents and relative methods of Smartphone

Jung-bai Kim, Seok-hwa Ahn, Okyeon Yi
Dept. of Math. Kookmin University

요 약

스마트폰 보급의 확산으로, 어플리케이션 마켓 및 다양한 인터넷 기반 서비스가 활성화되었다. 그러나 모바일 악성코드로 인한 공격 및 피해가 증가하고 있고 향후에는 더욱 지능화된 다양한 형태의 악의적 행위에 의한 정보 유출, 불법 과금, 부정 사용 등과 같은 보안 위협 일어날 것으로 예상된다. 본 논문은 스마트폰에서 보안사고의 사례와 취약점을 분석하고 대책 방안을 위한 연구 방향을 제시하고자 한다.

1. 서론

무선 네트워크와 모바일 단말의 급속한 발전은 이동통신시장의 큰 변화를 가져왔다. 특히, 스마트폰의 보급이 확산되면서 우리는 메일 확인을 위해 PC를 켜지 않아도 되고 은행거래를 하기 위해 은행에 가지 않아도 된다. 언제 어디서나 인터넷이 가능하며 휴대성을 제공한다. 스마트폰은 기존의 일반 휴대폰에 비해 여러 가지 장점을 갖지만 그중 가장 큰 장점은 어플리케이션의 설치가 자유롭다는 점이다. 기존의 일반 휴대폰은 제조사에서 설정한 기능만 제한적으로 사용할 수 있었던 반면 스마트폰은 사용자 스스로 여러 가지 기능을 추가하여 기호에 맞게 함으로서 높은 편의성 및 다양한 정보에 대한 접근성을 제공한다. 이러한 많은 장점으로 인해 전 세계에 급속도로 스마트폰 보급이 확대되고 있으며 시장규모 또한 증가하고 있다[1, 2].

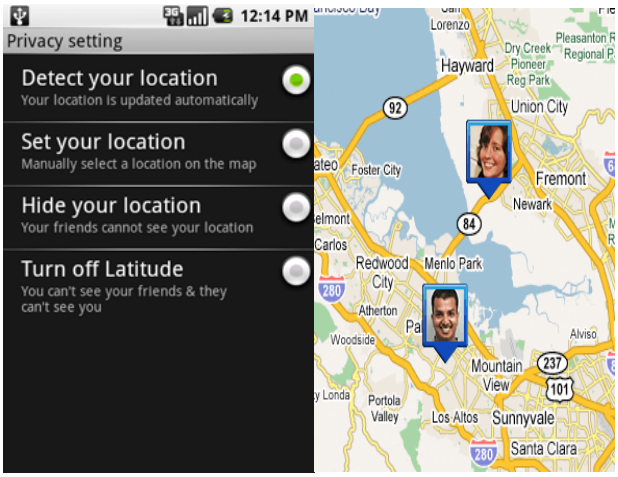
그러나 이 같은 스마트폰의 확산은 동시에 다양한 보안사고를 초래하고 있다. 개방형 모바일 환경에서는 표준화된 개발환경이 개발자에게 공개되기 때문에 누구나 어플리케이션의 제작 및 배포가 가능하다. 그렇기 때문에 검증되지 않은 다수의 어플리케이션이 개발 및 배포되고 있으며 웜, 바이러스 등 악성 어플리케이션이 스마트폰에 설치되어 보안 사고를 일으킬 수 있는 것이다. 특히 주식, 증권, 뱅킹 같은 금융 어플리케이션들은 개인정보 및 인증서, 패스워드 등 중요 정보를 다루고 있고 이러한 정보가 노출될 시 고객 및 은행은 금전적으로 피해를 입을 수 있다[4].

* 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (20100024870)

2. 보안사고 사례

2.1 개인정보유출 사고

스마트폰은 사용자의 위치, 생활 패턴, 주소록 등 개인정보를 이용하여 다양한 서비스를 제공하고 있다. 주변의 병원, 편의점 등을 보다 쉽게 찾을 수 있으며 개인 취향에 맞춰 추천된 서비스를 이용할 수 있다. 하지만 보호되지 않은 개인정보는 악의적인 목적에 의해 악용될 수 있으며 실제로 다양한 보안사고가 발생되고 있다.



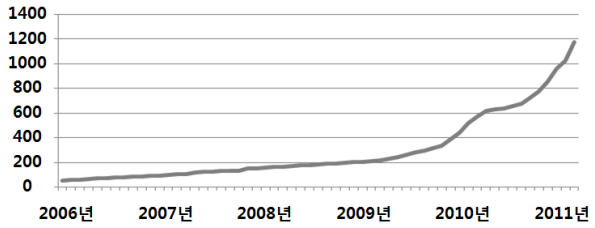
(그림 1) 일반적인 GPS 위치추적 기능의 어플리케이션 실행 화면

(그림1)는 GPS를 이용한 개인정보 수집의 예를 보여준다.

태국 업체가 개발한 상용 어플리케이션 FlexiSpy는 스마트폰의 통화기록, SMS(Short Message Service) 내용 , GPS(Global Positioning System) 추적 등 많은 개인정보를 사용자 몰래 특정 웹서버 또는 제 3자에게 유출시켰다.

국내에서는 연인들의 위치를 확인할 수 있는 어플리케이션이 등장하기도 했다. 이러한 어플리케이션은 위치정보를 감시하는 스파이웨어를 내장함으로서 악용이 가능하지만 아무런 제제 없이 배포되었다.[7]

2.2 악성코드 피해사례



(그림 2) 전 세계 스마트폰 악성코드 발생 추이

(그림2)은 스마트폰의 불법 어플리케이션에 의한 악성코드의 증가를 나타낸다[5].

스마트폰의 다양한 외부 인터페이스는 사용자가 손쉽게 네트워크 서비스를 이용할 수 있도록 지원하여 내부 API (Application Program Interface) 인터페이스제공은 개발자가 보다 편리하게 개발할 수 있게 하였다. 하지만 다양한 외부 인터페이스 제공으로 악성코드의 전파경로가 다각화되었고 내부 인터페이스 제공은 악의적인 개발자가 모바일 어플리케이션에 악성코드를 쉽게 은닉할 수 있게 한다.

2004년 블루투스를 통해 전파되는 최초의 모바일 악성코드로 알려진 Cabir는 감염된 단말을 지속적으로 스캐닝함으로서 배터리의 수명을 단축시킨다. 또한 블루투스를 통해 주변 단말을 감염시켜 감염된 단말의 화면에 “Cabir”라는 글자가 나타나는 것이 특징이다.

PbStealer는 국내에서 발생한 첫 휴대폰용 트로이 목마 악성코드이다. 사용자의 정보를 phonebook.txt파일에 저장, 블루투스를 통해 파일을 무작위로 전송하여 개인정보를 유출시키고 지속적인 접속을 시도하여 배터리의 수명 단축 및 네트워크 전체의 장애를 유발한다.

Commwarrior는 MMS(Multimedia Messaging Service)를 경유하여 확산되는 최초의 바이러스이다. MMS를 사용하여 전 세계에 텍스트 메시지를 전송할 수 있으므로, 단거리 통신인 블루투스를 사용하는 Cabir보다 넓은 범위를 감염시킬 수 있고, 또한 확산 속도도 매우 빠르다.

2006년 러시아에서 제작된 RedBrowser는 단말의 메시징 서비스나 전화를 지속적으로 시도하여 과금을 발생시키는 악성코드이다. 감염된 단말은 사용자 모르게 SMS를 전송함으로써 사용자에게 금전적 피해를 입힌다.

현재 악성코드의 전파경로는 악의적인 웹페이지로 인한 감염, 사용자 다운로드를 통한 감염, SMS/MMS를 통한 감염, 외부 메모리를 통한 감염 등이 있다.[3]

2.3 금융거래 보안사고

스마트폰으로 전자 금융 서비스가 가능해짐으로써 사용자의 편의성은 증대된 반면 금융거래 사고에 대한 잠재적인 보안위협이 예상되고 있다. 실제 2009년 8월 11일부터 9월 1일까지 독일 소재의 한 은행에서 개인 고객 PC에 대한 메모리 해킹으로 한화 약 4억원이 인출되는 사건이 발생하기도 했다. PC 기반의 금융서비스 기술을 확대 적용한 스마트폰 금융 서비스에서도 유사한 보안사고가 일어날 수 있다.

3. 보안기술

3.1 백신

안철수 연구소는 스마트폰과 관련해 발생 가능한 악성코드와 사용자들의 요구, 제조사들의 요구까지 다각도로 분석하여 모바일 전용 어플리케이션을 제공하고 있다. 주요 기능으로 안티바이러스, 도난방지, 안티스팸, 네트워크 관리, 업데이트가 있다. 어플리케이션의 정보 접근 권한판단에서 과도한 개인 정보를 이용하는 어플리케이션에 대한 삭제 알림 제공, 도난 방지(Anti-Theft) 기능까지 모바일 단말에 최적화된 기능이 총망라된 모바일 단말 전용 종합 보안 어플리케이션으로, 안전하고 편리한 모바일 환경을 구축하고 있다[6].

3.2 인증

3.2.1 공인인증서

전자상거래를 할 때 신원을 확인하고, 문서의 위조와 변조, 거래 사실의 부인 방지 등을 목적으로 공인인증기관이 발행하는 전자적 정보로서, 일종의 사이버 거래용 인감증명서이다. 공인인증서 내에는 가입자의 전자서명 검증키, 일련번호, 소유자이름, 유효기간 등의 정보를 포함한 일련의 데이터를 포함하고 있다. 이렇게 생성된 전자서명은 실제 서명과 같은 법적 효력을 가지며 전자상거래, 인터넷뱅킹, 증권, 보험, 서류 발급, 세금 납부 등 다양한 분야에서 활용되고 있다. 현재 국내 공인인증기관으로 지정된 곳은 금융결제원, 한국정보인증, 한국증권전산(코스콤), 한국전자인증, 한국무역정보통신(트레이드사인) 등 5곳이며 은행과 증권회사 등은 공인인증서를 직접 발급하지는 않고 접수 및 등록만을 대행한다.

3.2.2 OTP(일회용 비밀번호)

OTP란 One Time Password의 약자로서 인증이 요구될 때 마다 새롭게 사용할 수 있는 1회성 패스워드를 생성하는 보안 시스템이다. 일반 패스워드와는 달리 인증이 끝나면 폐기되기 때문에 재사용이 불가능하며 주로 인터넷뱅킹, 인터넷 결제 등 전자금융거래에서 보다 안전한 보안을 제공하기 위해 사용된다. OTP생성 방식에는 비동기화 방식과 동기화 방식이 있다. 비동기화 방식의OTP는 OTP 단말과 인증서버 간에 키를 제외한 미리 설정되어있는 동기화 기준 정보가 없는 방식이고 동기화 방식의 OTP는 OTP 단말과 인증서버 간에 미리 공유된 비밀정보와 동기화

정보에 의해 OTP 값이 생성되는 방식이다. 비동기화 방식에 비해, OTP단말과 인증서버 간에 반드시 동기화가 이루어져야 올바른 인증을 할 수 있다는 제약점이 있으나, 사용자 입력 편의, 기존의 ID/PW 어플리케이션과의 호환성 등 비동기화 방식의 단점을 보완 할 수 있다[8].

3.2.3 NFC(Near Field Communication)

NFC는 전자태그(RFID)중 하나로 비접촉 근거리 무선통신 모듈로 10cm의 가까운 거리에서 단말기 간 데이터를 전송하는 기술을 말한다. 언제 어디서나 스마트폰으로 간단하게 결제가 가능하고 카드결제 기능 외에도 계좌이체, 명함, 자료 등을 교환할 수도 있다[9].

NFC는 교통카드와 같은 주파수를 이용하지만 교통카드와는 다르게 양방향 통신이 가능하다. 즉, 정보의 읽기와 쓰기가 가능하다는 장점이 있다. 공개키와 개인키를 기반을 한 타원곡선암호알고리즘을 사용하고 데이터간의 기밀성과 무결성을 제공하기 때문에 보다 안전한 근거리 무선통신을 할 수 있다. 인터넷 결제 시 공인인증서에 번거로운 절차 대신 NFC를 이용해 자신을 증명할 수 있다. 대표적으로 모바일 단말기 간 접촉 응용서비스, 개인정보 관리 응용서비스, 정보 제공 및 맞춤형 광고 관련 응용서비스에서 사용된다[9].

4. 분석 및 대책 방안

스마트폰의 GPS 시스템은 개인 위치정보를 노출한다. 이를 설정하지 않는다하더라도 3G 이동통신망 뿐만 아니라, 무선 랜 및 블루투스 기능이 기본적으로 탑재되어있어 대략적인 단말의 위치정보는 노출이 가능하다. 서비스 개선이나 어플리케이션의 기능 구현 등 선의의 목적으로 시작했지만 악의적인 용도로 사용 될 경우 다양한 문제가 발생할 수 있다. 제조사 및 통신사들은 이러한 정보가 기록됨을 사용자가 확실히 인지할 수 있게 알려주어야 하며 사용자 또한 이를 인지하여 불필요한 정보의 유출을 스스로가 방지할 수 있어야 한다.

검증되지 않은 무분별한 어플리케이션과 유해 사이트를 이용함으로써 발생하는 모바일 악성코드에 의한 피해는 백신의 설치로 많은 부분 예방할 수 있다. 그러므로 항상 백신을 설치하고 이를 실시간으로 모니터링 해주어 악성코드를 예방 하여야 한다. 하지만 이러한 백신이 있음에도 불구하고 일부 사용자들은 보안의식 결여와 편의성만을 추구하여 사용하지 않고 있다. 사용자는 항상 악성코드의 위험에 노출될 수 있다는 보안 의식을 가져야 한다.

단말기 내의 개인정보들은 물리적인 공격이나 분실에 의해 유출될 수 있다. USIM은 스마트카드의 보안기능(PIN & PUK)을 바탕으로 분실 시에도 개인정보를 복제하지 못하도록 보호하고 있으므로 개인정보를 USIM 내에서 저장, 처리한다면 오프라인 및 온라인상에서 정보가 유출되기 어려우므로 더 높은 안전성을 가질 수 있다.

다수의 국외 은행에서는 전자금융 거래 시 거래연동 인증기법인 마스터 카드사의 CAP(Chip Authentication Program)을 사용하고 있다. 이것은 전용리더기의 휴대로 인해 편의성이 다소 떨어지지만 계좌번호와 결제금액등 거래정보를 독립적으로 다루기 때문에 메모리 해킹에 안전하다. 또한 터치 스마트폰의 경우, 화면 터치를 통해 비밀번호 등 비밀 정보를 입력하기 때문에 KeyLog 공격이 가능하지만 터치 키패드의 위치를 바꾸는 방법을 사용하면 패턴을 기억한다해도 KeyLog 공격에 안전하다.

5. 결론

스마트폰의 급속한 발전 및 보급은 사용자의 실생활에 당양한 변화와 높은 편의성을 가져 왔지만 다양한 보안사고를 초래하고 있다. 스마트폰은 반드시 백신과 함께 사용하여 악성코드의 위험을 피해야 하며 어플리케이션의 개인정보수집에 대한 확실한 공지 및 사용자 인지가 필요하다.

스마트폰은 분명히 많은 보안문제를 가지고 있다. 사전 검증되지 않은 어플리케이션과 악성코드의 확산, 사용자의 보안의식 결여, PC에서 보안상 취약점들의 스마트폰에 적용 등 스마트폰 사용으로 야기되는 보안문제에 대한 연구가 이루어 져야한다. 이러한 연구에 대하여 정부기관, 이동통신사, 금융기관 등에서는 제도적, 기술적 대책 및 예방을 위한 노력이 요구되며 사용자 스스로 높은 보안의식을 가져야 할 것이다.

참고문헌

[1] 김기연, 조성제 “스마트폰 보안 취약점 동향” 한국정보과학회, 한국정보과학회 2010 한국컴퓨터 학술발표논문집 제37권 제2호(B) 2010.11, page(s): 90-94

[2] 최은영, 김미주, 정현철, “스마트폰 보안 강화를 위한 방안 연구”, 한국인터넷정보학회, 한국인터넷정보학회 2010년도 학술발표대회 2010.6, page(s): 781-785

[3] 강동호, 한진희, 이윤경, 한승완, 조현숙 외, “스마트폰 보안 위협 및 대응 기술”, 한국전자통신연구원, [ETRI]전자통신동향분석 전자통신동향분석 25권 3호

[4] 김기영, 강동호, “개방형 모바일 환경에서 스마트폰 보안기술”, 한국정보보호학회, 정보보호학회지, 제19권 제5호 2009.10, page(s): 21-28

[5] 방송통신위원회(KCC), 한국인터넷진흥원(KISA), “스마트폰 백신 이용 안내서 ”, 스마트폰 정보보호 민・관 합동대응반

[6] 안철수연구소, http://www.ahnlab.com/

[7] nProtect, http://www.nprotect.com/

[8] 허승표, 이대성, 김귀남, “모바일 환경에서 OTP기술과 얼굴인식 기술을 이용한 사용자 인증 개선에 관한 연구”, 정보·보안 논문지 제11권 3호(2011. 6)

[9] 임선희, 전재우, 정임진, 이옥연, “NFC 보안 기술 분석 및 UICC 적용 효과 연구” 한국통신학회, 한국통신학회논문지, 제36권 제1호(네트워크 및 융합서비스) 2011.1, page(s): 29-36