중소기업융합학회 논문지 제4권 제4호 pp. 13-18, 2014 ISSN 2234-4438

스마트폰 사용으로 인한 사용자 프라이버시 피해 현황 분석

정윤수[1*]
[1*]목원대학교 정보통신융합공학부

Tracking Analysis of User Privacy Damage using Smartphone

Yoon-Su Jeong[1*]
[1*]Department of Information Communication Engineering, Mokwon University

요 약 스마트폰 개발의 발전으로 인하여 사용자의 스마트폰 사용율이 PC 사용율보다 점점 높아지고 있는 실정이다. 스마트폰 사용이 대중화되면서 스마트폰 사용자의 개인신상정보, 금융 정보와 같은 중요한 프라이버시 정보들을 보호하는 연구는 현재 미미한 상태이다. 본 논문에서는 현재까지 연구되었던 스마트폰의 다양한 취약점에 대해서 분석하고 스마트폰 보안 공격 방법에 대한 대응방법 및 스마트포 소비자 분쟁 해결 기준들을 제시한다. 특히, 스마트폰에서 발생하기 쉬운 보안 위협(네트워크, 악성코드, 훔쳐보기 공격 등)을 통해 사용자의 개인정보 유출이나 금전적 손실과 같은 직접적인 피해를 최소화하기 위한 방법들을 분석한다.

키워드 : 스마트폰, 사용자, 보안, 피해현황

Abstract The usage rate of user due to advances in smartphone development is higher than the usage rate to use a PC. However, smartphone usage popularized research to protect sensitive information, such as smart phone users personal information, financial information is a small state. In this paper, we analyzed the various vulnerabilities in smartphone studies to date have been looking into the corresponding port smart consumer dispute resolution methods and criteria for smartphone security attack methods and analysis. In particular, the threat of such a network, malware, Peep attack of the security threats arising from the smartphone they can avoid or mitigate threats to minimize the smartphone security damage is done to the disclosure of personal information, such as direct damage or financial loss the analysis of that method.

Key Words : Smartphone, User, Security, Damage tracking

1. 서론

최근 스마트폰 사용율이 컴퓨터 사용율보다 높아지면서 스마트폰을 이용한 다양한 서비스가 개발되고 있다[1,2,3]. 스마트폰은 사용상의 편리함과 휴대가 편하다는 장점이 있어 스마트폰 사용자는 별다른 생각 없이 중요한 정보를 스마트폰에 저장하곤 한다[4,5,6,7].

해커는 스마트폰에 저장된 사용자의 중요 정보들을 악의적인 공격방법을 통해 유출할 수 있기 때문에 사용자의 개인정보 유출 위협이 매우 높다. 해커가 사용하는 공격방법은 PC 환경에서도 가능했던 피싱, 파밍, 훔쳐보기 공격뿐만 아니라 각종 악성코드를 이용하여 스마트폰의 정보를 가져가거나 스마트폰을 좀비 PC로 만드는 등 다양한 공격 유형이 존재한다. 스마트폰은 PC에서는 없

Received 2014-10-17 Revised 2014-11-01 Accepted 2014-11-08
*Corresponding author: Yoon-Su Jeong (bukmunro@mokwon.ac.kr)

Table 1. Type of Malware

종류	의미
컴퓨터 바이러스	프로그램을 통해 감염되는 악성 소프트웨어
웜	컴퓨터의 취약점을 찾아 네트워크를 통해 스스로 감염되는 악성 소프트웨어
웜 바이러스	웜과 바이러스의 감염방법을 동시에 갖춘 악성 소프트웨어
트로이 목마	자가 복제능력이 없는 악성 소프트웨어
스파이웨어	사용자의 정보를 빼내는 악성 소프트웨어
애드웨어	컴퓨터 사용시 자동적으로 광고가 표시되게 하는 악성 소프트웨어
Hoax	악성코드에 대한 잘못된 정보로 악영향을 끼치는 소문
가짜 백신 프로그램	정당한 바이러스 방어 프로그램이라고 주장하고 잘못된 정보를 표시하고 사용·결제를 유도하고 제무적 정보를 도둑질하는 악성 소프트웨어
하이재커	의도치 않은 사이트로 이동을 시키고 팝업창을 띄우는 악성 소프트웨어

던 SMS 서비스를 이용하여 악성코드를 심은 후 공격하는 스미싱(Smishing)과 같은 신종 공격방법이 사용된다[9,10,11,12].

스마트폰은 기존의 휴대전화기에 비하여 빠른 데이터 처리속도, 대용량 저장공간, 대형화된 화면 등을 제공함으로써 다양한 개인정보의 저장과 운영, 서비스에 대한 활용을 가능하게 하였으나, 스마트폰 내에 저장된 개인정보의 사용에 따라 안전성 확보라는 문제점이 존재한다[13,14,15].

스마트폰에 저장되어 있는 개인정보는 사용자의 개인 ID로써의 역할 뿐만 아니라 스마트폰을 통한 전자적 지급결제를 위한 결제정보로써의 역할을 수행하고 있으므로 결제시의 금융정보의 송·수신 등에서 발생 가능한 내외부의 직간접적인 위협으로부터 보호될 수 있는 방안이 동시에 고려되어야 한다[2,9].

또한 스마트폰을 이용한 모바일 금융결제 서비스의 확산과 안전한 사용을 위하여 스마트폰에 저장되는 모든 정보를 보호하기 위한 기기 보안과 운영 어플리케이션을 포함한 시스템 보안 및 네트워크 보안 등을 위한 다양한 보안기술이 요구된다[5,7,16,17,18].

본 논문에서는 현재까지 연구되었던 스마트폰의 다양한 취약점에 대해서 분석하고 스마트폰 보안 공격 방법에 대한 대응방법 및 스마트폰 소비자 분쟁 해결 기준들에 대해서 조사・분석한다. 특히, 스마트폰에서 발생하는 보안 위협 중 네트워크, 악성코드, 훔쳐보기 공격 등의 위협들이 개인정보 유출이나 금전적 손실과 같은 직접적인 피해로 이루어지기 때문에 스마트폰 보안 피해를 최소화하기 위한 위협 회피 방법들을 분석한다.

이 논문의 구성은 다음과 같다. 2장에서는 스마트폰 피해 분석 및 스마트폰 악성 프로그램에 대해서 설명한다. 3장에서는 스마트폰 보안 위협에 대해서 분석하고, 마지막으로 4장에서는 이 논문의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

2. 스마트폰 피해분석 및 악성 프로그램

2.1 스마트폰 피해 분석

악성 프로그램에 의해 감염된 스마트폰은 PC 감염보다 훨씬 위험한 경우가 많다. 최근에는 금융거래가 일상화되면서 스마트폰을 이용하는 서비스(뱅킹 애플리케이션 등)가 악성 프로그램에 감염되어 사용자의 개인정보가 유출되는 사례가 늘고 있다. 특히, 스마트폰이 악성 프로그램에 감염될 경우 스마트폰 이용자들은 거래은행 정보와 비밀번호 같은 중요한 사용자 개인정보가 쉽게 노출될 수 있다. 이 같은 결과는 크게 2가지 이유로 인하여 발생되는 경우가 많다. 첫째, 해커가 스마트폰 사용자의 개인정보를 쉽게 유출시킬 수 있는 환경일 경우, 둘째, 스마트폰이 PC보다 더 많은 개인 정보와 금융 정보를 가지고 있어 금전적 이득이나 개인정보를 탈취하기 쉬운 경우이다.

현재까지 발견된 스마트폰의 악성 프로그램은 대부분 스마트폰 사용자의 개인정보를 유출하는 경우가 대부분이다. 예를 들어, 'Geunimi'는 2010년 12월에 유포된 '트로이목마'형 악성코드로써. 이용자의 개인정보를 훔쳐 원격지에 있는 서버로 보내는데 사용되었다. 그리고, 2011년 3월 집중 유포된 'DroidDreamLight'는 이용자의 개인정보 및 금융정보를 유출하는 악성코드이다.

2.2 스마트폰 악성 프로그램

2.2.1 악성 프로그램

악성 소프트웨어 또는 맬웨어(malware)는 컴퓨터에 악영향을 끼칠 수 있는 모든 소프트웨어를 의미한다. 예전에는 단순히 컴퓨터 바이러스만이 활동하였으나, 1990년대 말 들어서 감염 방법과 증상들이 다양해지면서 자세히 분류하게 되었다. 과거에는 디스크 복제 등 저장매체를 따라 전파되었으나 네트워크가 발달하면서 이메일이나 웹으로 감염되는 경우로 발전하였다.

악성코드는 크게 코드 정적 분석 (Static code analysis)과 코드 동적 분석 (Dynamic code analysis) 두 종류로 나뉜다. 코드 정적 분석은 프로그램을 디스어셈블하는 디버깅프로그램들을 이용하는 방법으로 Immunity Debugger, 올리 디버거, IDA pro, GDB 등의 프로그램을 사용하여 디스어셈블된 프로그램의 코드를 실행시키지 않고 분석한다. 코드 동적 분석 (Dynamic code analysis)은 런타임 디버깅기법을 이용하여 통제된 상황 하에서 악성코드를 직접 실행시키며 이후에 발생하는 변화들을 분석한다. 런타임 디버거로는 앞서 언급한 Immunity Debugger, 올리 디버거 등이 있으며 프로그램의 프로세스에 붙어서 제어하는 역할을 한다. 통제된 상황에서 변화를 살펴보는 툴로는 파일의 입출력을 감시하는 Filemon, 레지스트리 정보 변화를 감시하는 Regmon, TCP/UDP 통신에 대한 입출력을 감시하는 TDImon, 실행 중인 프로세스의 DLL 정보 등을 감시하는 프로세스 익스플로러 등이 있다.

2.2.2 안드로이드폰 내 악성 프로그램 점유율 변화

악성 프로그램은 최근 안드로이드 운영체제를 탑재한 스마트폰을 타깃으로 삼고 있다. 이 같은 이유는 안드로이드 스마트폰이 세계 시장에서 가장 큰 점유율을 점유하고 있고, 구글 플레이마켓(구 안드로이드마켓)에는 별다른 제약없이 앱을 올릴 수 있기 때문이다.

애플 앱스토어의 경우 애플이 직접 점검을 마친 앱만 등록될수 있어 구글 플레이마켓에 비해 비교적 안전하지만 아이폰의 보안 체제를 해제하는 이른바 '탈옥' 이용자의 경우 악성 프로그램에 노출될 위험이 높다. 탈옥시 아이폰의 보안체계가 정상 작동하지 않기 때문이다.

3. 스마트폰 보안 위협

3.1 스마트폰 보안 문제점

스마트폰에서는 사용자의 개인정보를 보호하기위해서 다양한 보안 기법을 제공하고 있지만 여전히 사용자의 중요 개인정보가 노출되고 있다.

3.1.1 루팅

루팅(rooting)은 모바일 기기에서 구동되는 안드로이드 운영체제 상에서 최상위 권한(루트 권한)을 얻음으로써 해당 기기의 생산자 또는 판매자 측에서 걸어 놓은 제약을 해제하는 행위를 의미한다.

스마트폰에서는 루팅을 통해 해당 기기의 버전보다 더 높은 버전의 안드로이드나 CyanogenMod처럼 사용자들이 임의로 개조한 안드로이드를 설치 및 구동 할 수 있어 사용자가 속한 지역의 안드로이드 사용자들에게 판매하지 않는 프로그램들을 구입하거나 일반 사용자 권한 이상의 권한 등을 필요로 하는 프로그램들을(백업 프로그램, 하드웨어 해킹 프로그램 등) 사용할 수 있다.

루팅은 안드로이드 특성상 상 반드시 최고권한(관리자)이 필요한 동작(카메라무음, 파일접근, 시스템앱삭제 등)을 수행하고자 할 때 사용된다. 한 번 루팅된 안드로이드는 언루팅 하지 않는 이상 몇 번이고 supersu를 지웠다 설치했다 해도 루팅은 그대로 유지할 수 있다.

탈옥(Jailbreaking)과 루팅은 기기의 생산자 또는 판매자 측에서 걸어 놓은 제약을 해제한다는 면에서 iOS 관련 용어인 탈옥(Jailbreaking)과 비슷하다. 그러나, 루팅은 서드파티 프로그램 설치를 막아 놓은 AT&T 안드로이드 폰들을 제외하고는 루팅 없이도 구글 플레이에서 공하지 않는 프로그램을 따로 구할 필요가 없다는 차이점이 있다.

3.1.2 SE 사용제약

SE(Secure Element)는 스마트폰에서 전자 결제 서비스를 위해 사용되는 NFC(Near Field Communication)기능에서 사용된다. SE는 사용자의 카드 정보 등과 같은 중요한 정보를 저장할 때 사용한다. SE는 USIM(Universal Subscriber Identity Module)에 내장되어 사용되며 운영체제 차원에서 엄격하게 제어함으로써 사용자의 중요정보를 보호한다. 특히 SE가 USIM에 내장된 경우에는 통신사의 승인을 단말에 내장된 경우 단말 제조사의 승인을 받은 경우에만 사용 가능하다. 따라서, 임의의 앱에서 데이터를 SE에 저장하기란 사실상 불가능하다.

3.1.3 암호화 저장 기법 부재

스마트폰에서 실행되는 앱은 샌드박스에 의해 저장된 데이터를 안전하게 보호하지만 안드로이드 API에는 안전한 데이터 저장을 위한 별도의 기법을 제공하지 않는 문제점이 존재한다. 따라서, 루팅이 된 스마트폰의 경우 저장된 데이터를 보호하지 못하므로 스마트폰에 저장된 데이터가 암호화되지 않으면 데이터가 노출될 수 있다.

3.1.4 역공학

리버스 엔지니어링(Reverse Engineering, RE) 또는 역공학은 장치 또는 시스템의 기술적인 원리를 그 구조 분석을 통해 발견하는 과정을 의미한다. 역공학은 기계 장치, 전자 부품, 소프트웨어 프로그램 등을 조각내서 분석한다. 역공학은 유지 보수를 위해 같은 기능을 하는 새 장치를 원본의 일부를 이용하지 않고 만들기 위해 대상의 세부적인 작동을 분석한다.

역공학은 원본 생산의 절차에 관한 지식이 거의 없는 상태에서, 최종 제품을 가지고 디자인 결정과정을 추론하는 것을 목적으로 한다.

스마트폰에서는 사용되는 앱들이 보통 자바로 구현되고 있다. 자바는 다른 프로그래밍 언어에 비하여 역공학이 용이하다는 특징이 있다. 스마트폰은 스마트폰에 설치된 앱을 단말기 또는 컴퓨터를 통해 쉽게 추출할 수 있으며, 암호화된 키도 역공학을 통해 쉽게 노출될 수 있는 문제점이 존재한다.

3.2 스마트폰 소비자 피해 사례 및 관련 규정

3.2.1 스마트폰 소비자 피해

스마트폰 가입자가 빠르게 늘어나면서 소비자 불만도 급증하고 있다. 다음은 스마트폰 소비자 피해의 대표적인 예를 보여주고 있다.

[사례 1]
<30대 남성>
- 2011. 02월 스마트폰 구입
- 구입 후 화면이 멈추고 버튼 동작이 안되고 전원 꺼짐 증상으로 AS 요청
- 현재까지 AS센터 7번이나 방문 하였는데도 증상이 개선되지 않음
- 메인보드 교체까지 했는데도 동일증상 재발되어 환급 요청했지만 업그레이드만 해줌

[사례 2]
<40대, 남성>
- 스마트폰 6개월전 구입 동일하자 꺼지는 현상과 동영상 문제로 부품교체
- 5차례나 AS 받았지만 불량 개선되지 않음
- 더 이상 사용할 수 없는데 교환이나 환급처리를 해주지 않고 있음

[사례 3]
<30대, 남성>
- '홍콩폰사이트'에서 스마트폰 구입하려고 대금 입금했는데 물건도 오지 않고 판매자는 전화연락도 안됨

3.2.2 스마트폰 소비자 피해 관련 규정

스마트폰 소비자 피해 관련 규정은 <표 2>과 같다.

3.3 스마트폰 피해 예방 방법

스마트폰 피해를 예방하기 위한 방법은 여러 가지가 있다. 그 중에서 스마트폰을 사용하는 사용자의 피해를 최소화하기 위한 가장 대표적인 피해 예방 방법을 정리하면 대표적으로 다음과 같은 5가지 방법이 있다.

① 스마트폰 사용 시간을 미리 정해 둔다. 수업 시간이나 업무 시간에는 스마트폰을 아예 사용하지 않는 습관을 들이도록 한다.
② 꼭 필요한 앱만 사용하도록 하고 불필요한 앱은 삭제한다.
③ 걸어다닐 땐 되도록 스마트폰을 손에 들지 않는다.
④ 스마트폰을 대체할 수 있는 물건을 사용해본다. 메모를 위한 수첩이나 스케줄 관리를 위한 다이어리를 사용해 보는 것도 좋다.
⑤ 자기 관리 어플 (MOMO, 넌얼마나쓰니 등)을 이용하여 스마트폰 사용을 제한한다.
⑥ 밤늦게 까지 하지 않는다.

4. 결론

스마트폰의 기능이 다양화됨에 따라 스마트폰을 사용하는 사용자의 개인정보의 보안위협이 증가하고 있다.

Table 2. Smartphones based on consumer dispute resolution

분쟁유형	해결기준	비고
1) 정상적인 사용상태에서 발생한 성능기능상의 하자로 중요한 수리를 요하는 사항을 구입 후 10일 이내에 문제 제기	- 신품 교환 또는 구입가 환급	* 단, 품질보증기간 이내에 동일하자에 대해 2회까지 수리하였으나 하자가 재발하는 경우 또는 여러 부위 하자에 대해 4회가지 수리하였으나 하자가 재발하는 경우는 수리가 불가능한 경우로 본다.
2) 정상적인 사용상태에서 발생한 성능기능상의 하자로 중요한 수리를 요하는 사항을 구입 후 1개월 이내에 문제 제기	- 신품 교환 또는 무상수리	* 리퍼폰 교환은 무상수리로 본다.
3) 정상적인 사용상태에서 발생한 성능기능상의 하자에 대하여 구입 1개월이 경과한 이후부터 품질보증기간 이내에 문제 제기		* 품질보증기간 이내에 발생한 정상사용에 따른 하자로 인해 동일인이 4회까지 리퍼폰으로 교환하였으나 또다시 수리 또는 리퍼폰 교환이 불가능한 경우로 본다.
- 하자발생시 - 수리 불가능시 - 교환불가능시 - 교환된 신제품이 교환 후 1개월 이내에 중요한 수리를 요할 때	- 무상수리 - 신품교환 또는 구입가 환급	* 이동통신사업자는 이용자가 이동통신사업자의 유통망에서 구매한 단말기 AS 등의 요청을 하는 경우에 이를 접수한 후 신속히 AS등에 필요한 조치를 취한다.
4) 부품보유기간 이내에 수리용 부품을 보유하고 있지 않거나, 이 문제를 리퍼폰 교환으로 해결할 수도 없어 발생한 피해 -품빌보증기간이내 · 정상적인 사용상태에서 발생한 성능기능상의 하자인 경우 · 소비자의 고의과실로 인한 고장인 경우 - 품질보증기간 경과 후	- 구입가 환급 -신품교환 또는 구입가 환급 -유상수리에 해당하는 금액 징수 후 신품 교환	* 감가상각방법 -정액법에 의하되 내용연수는 3년(월할계산)적용 -감가상각비 계산은 (사용연수/내용연수)×구입가 -감가상각 잔여금의 계산은 구입가-감가상각비 -품질보증기간 : 1년 -내용연수 : 3년 -부품보유기간 : 4년
5) 제품구입시 운송과정에서 제품 훼손	-정각한 잔여급에 구입가의 5%를 가산하여 환급(감가상각한 잔여금액 <0이면 0으로 계산 -신품교환(단, 전문운송기관에 위탁한 경우는 운송시에 대한 구상권 행사)	

본 논문에서는 현재까지 발견된 스마트폰의 다양한 취약점에 대해서 분석하고 스마트폰 보안 공격 방법에 대한 대응방법에 대해서 조사 및 분석하였다. 특히, 스마트폰에서는 루팅을 고려한 대응 방안 즉, 스마트폰에서 발생하는 보안 위협 중 네트워크, 악성코드, 훔쳐보기 공격 등의 위협들이 개인정보 유출이나 금전적 손실과 같은 직접적인 피해를 최소화하기 위한 방법들이 요구되고 있다. 향후 연구에서는 데이터 보호 프레임워크에 따라 앱의 알고리즘 및 데이터를 안전하게 보호하는 방법에 대해서 연구할 계획이다.

REFERENCES

[1] Gartner, “Market Share Analysis: Mobile Phones, Worldwide, 2Q13,” http://www.gartner.com/newsroom/id/2573415, Aug. 2013.

[2] Gartner, Market Share: Mobile Communication Devices by Region and Country, 3Q11, http://www.gartner.com/newsroom/id/1848514, Nov. 2011.

[3] icrossing, 2013 Mobile Market Share, http://connect.icrossing.co.uk/2013-mobile-market-share-infographic_10062, Jan 2013.

[4] Wikepedia, Bring Your Own Device, http://en.wikipedia.org/wiki/ Bring_your_own_device

[5] News1, From 15th, blocking smartphone features in the building of Ministry of National Defense, http://news1.kr/articles/1239175

[6] BlackBerry, Balance technology, http://us.blackberry.com/business/software/blackberry-balance.html

[7] Jason Foy, “Understanding BlackBerry Balance,” BlackBerryLive, 2013.

[8] Samsung, KNOX, https://www.samsungknox. com/en/

[9] SELinux Wiki, SEforAndroid, http://selinuxproject.org/page/SEAndroid

[10] Centrify, Samsung to OEM Centrify for Single Sign-On and Mobile Management, http://www.centrify.com/blogs/tomkemp/samsung_oems_centrify_for_sso_and_mdm.asp

[11] Samsung, Samsung KNOX available for use by consumers, http://www.samsung. com/us/news/21651

[12]http://www.anti-spyware-101.com/threats/rogue-antispy

ware-program.
[13] Hyongshick Kim, Jun Ho Huh, Ross Anderson, "On the Security of Internet Banking in South Korea," Oxford University Technical Report CSRR-10-01, Mar. 2010.
[14] Lucas Adamski, "Securing Browser Interactions," Security Issues of Online Banking & Payment in Korea, COEX Conference Hall, Seoul, Korea, Apr. 2010.
[15] Yunho Chung, "Korea's Smartphone Market: Late Start, Fast Growth," Korean Insight, Apr. 2010.
[16] Kilmo Kang, "Korea's smartphone market is emerging, all thanks to Apple, but the e-book market is not," CNET Asia, May 2010. (http://asia.cnet.com/blogs/digihunter/post.htm?id=63018568)
[17] Choi, Hwi-Min;Jang, Chang-Bok;Kim, Joo-Man, "Efficient Security Method Using Mobile Virtualization Technology And Trustzone of ARM," Journal of Digital Convergence, vol. 12, no. 10, pp. 299-308, October 2014
[18] Sunghyuck Hong, "Vulnerability of Directory List and Countermeasures," Journal of Digital Convergence, vol. 12, no. 10, pp. 259-264, October. 2014.

저 자 소 개

정 윤 수(Yoon-Su Jeong) [정회원]

- 1998년 2월: 충북대학교 전자계산학과 학사
- 2000년 2월 : 충북대학교 전자계산학과 석사
- 2008년 2월 : 충북대학교 전자계산학과 박사
- 2012년 3월 ~ 현재 : 목원대학교 정보통신융합공학부 조교수

<관심분야> : 유·무선 보안, 암호이론, 정보보호, Network Security, 이동통신보안