스마트폰의 보안 위협요소 동향 및 향후 대응 전략

홍종우, 김희성, 윤희용
성균관대학교 컴퓨터공학과
e-mail: {coolskku, maxker, youn}@skku.edu

Smartphone Security Threat Trends and Future Strategy

Jong Woo Hong, Hee Seong Kim, Hee Yong Youn
Dept of Computer Engineering, Sungkyunkwan University

요 약

스마트폰의 이용자가 최근 급증하고 있다. 그에 반응하듯 많은 기업들은 기존의 서비스 외에도 스마트폰을 이용해 사용할 수 있는 서비스들을 시작하고 있고, 기존의 모바일로 불가능했던 작업들을 장소와 시간에 구애받지 않고 가능케 되었다. 이처럼 스마트폰의 이용인구가 급격히 증가하고 관련 컨텐츠들이 봇물 쏟아지듯 넘쳐나면서 개인정보 유출이나 악성코드로 인한 보안 사고도 급격히 늘고 있다. 본 논문에서는 스마트폰에 악영향을 미치는 악성코드에 대해 간단히 살펴보고, 악성코드가 쉽게 보안체계를 무너뜨릴 수 있게 만드는 스마트폰의 보안 위협요소 대하여 알아본다. 또 현재 사용되고 있는 대응 방안은 무엇이 있는지, 그리고 향후에 이러한 악성코드들과 위협요소를 줄이는 방법, 또는 대응 전략에 대하여 연구하였다. 이러한 연구는 스마트폰 보안 사고를 줄이거나 사전에 예방하고, 더 나은 스마트폰 사용 환경을 제공할 것이다.

1. 서론

모바일 네트워크의 발달과 하드웨어의 비약적인 발전은 '손안의 PC'라 불리는 새로운 형태의 모바일인 스마트폰을 탄생시켰다. 스마트폰은 휴대폰의 통화 기능 이외에도 컴퓨터와 유사한 기능 환경 구현이 가능한 범용 운영체제를 탑재하였고, 이는 다양한 App을 설치하여 실행할 수 있다. 이러한 편리성과 휴대성은 스마트폰 이용자가 급격히 증가하는 이유가 되고 있으며, 2009년 10월 80만 명에서 2011년 3월에는 1000만 명을 돌파하며, 국민 5명중 1명이 스마트폰을 사용하는 것으로 나타났다.

[표1] 스마트폰 가입자 현황[1] (단위: 만명, %)

구분	09.12	10.03	10.06	10.09	10.12	11.01	11.03
이동전화가입자	4.794	4.898	4.961	5.021	5.077	5.098	5.116
스마트폰가입자	80	152	247	442	722	826	1,002
비중	1.7	3.1	5.0	8.8	14.2	16.2	19.6

이처럼 스마트폰 이용자가 급격히 증가하고, 장소에 관계없이 24시간 통신망과 연결되어 있는 특성으로 인해, 악성코드의 공격에 의한 보안사고 또한 급증하고 있다.

따라서 본 논문에서는 스마트폰 보안에 위협이 되는 악성코드 및 악성코드에 취약한 위협요소들을 살펴보고, 향후 스마트폰에서의 보안 강화를 위한 전략을 제시해보고자 한다.

2. 본론

모바일 악성코드는 스마트폰을 포함한 모바일 단말을 대상으로 개인정보를 유출하거나 시스템을 파괴시키는 행동을 하는 프로그램이다. 악성코드는 유형에 따라 많은 종류가 있으며, 다음과 같이 이를 크게 5가지 형태로 분류할 수 있으며, 대응 방안은 다음과 같다..

[표2] 모바일 악성코드 유형[2]

유형	설 명	악성코드 예
단말 장애 유발형	단말의 사용을 불가능하게 만들거나 장애를 유발	Skulls, Locknut, Gavno
베터리 소모형	단말의 전력을 지속적으로 소모시켜 배터리를 고갈	Cabir
정보 유출형	감연된 단말의 정보나 사용자의 정보를 외부로 유출	Infojack, Flexispy, PBStealer
과금 유발형	단말의 메시지, 전화 서비스를 계속적으로 시도하여 과금을 발생	RedBrowser, Kiazha
크로스 플랫폼형	모바일 단말을 통해서 PC를 감염	Cardtrap.A

[표3] 모바일 악성코드 대응 방안

대응 방안	설 명
사용자 및 모바일 기기 인증	모바일 오피스 App 은 허가된 사용자만 다운 가능 App 최초 실행 시 사용자 인증 과정 수행
입력정보 보호	가상 키패드 등을 이용한 암호화 및 무결성 보장 정보 전송 시 암호화시켜 전송
네트워크 보안	단말기 부터 서버까지 구간전체의 암호화 비 허가 및 통제되지 않는 네트워크 접속 차단
정보유출 방지	모바일 DLP(Data Linkage Protection)로 정보가 유출될 수 있는 각종 경로, App 차단
악성프로그램 방지	주기적인 백신 App을 통한 악성코드 검사

이러한 악성코드들에 노출되는 스마트폰의 위협요소들은 다음과 같다.

2.1. 위협요소

2.1.1. 개방성

스마트폰은 무선인터넷과 외부 인터페이스를 개방하여 사용자에게 다양한 네트워크 서비스를 지원하고 있다. 또, 개발자에게 편리한 개발환경을 제공하기 위해서 내부 API 인터페이스도 제공한다. 하지만, 무선인터넷과 외부 인터페이스의 개방은 악성코드의 공격 경로를 다양하게 만들고, 내부 API 인터페이스 제공은 악의적인 목적을 가진 개발자가 App을 통해서 보안체계를 쉽게 무너뜨리는 원인이 되고 있다.

2.1.2 통신환경

스마트폰의 통신환경은 3G 네트워크를 시작으로, Wi-Fi 및 블루투스 까지 다양하게 제공되고 있다. 특히 무료 무선 랜에 접근하다 보면 무작위로 검색되는 암호화가 적용되지 않은 AP(Access Point)에 접근하여 악성 코드에 감염된다.

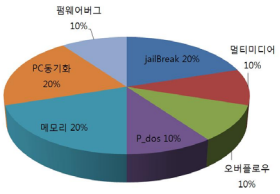
이렇게 감염된 악성코드들은 주변의 PC와 스마트폰에 유포되어 피해를 확산시킬 수도 있으며, 스마트폰의 다양한 보안 침해를 발생시킬 수 있다. 또, 시스템이나 개인정보가 유출되고, 금전적인 피해가 유발될 수 있으며, 심한경우에는 시스템 자체를 변경하거나 파괴하여 스마트폰을 사용이 불가능하게 만들 수도 있다.

2.1.3. 사용 환경

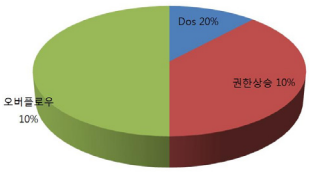
스마트폰이 기존의 휴대폰보다 기능과 성능이 매우 뛰어나지만, 공통된 점은 휴대성이다. 즉, 시간과 장소에 구애받지 않고 사용이 가능하다. 휴대성을 강조하다 보니 PC나 노트북 등의 다른 전자기기에 비해 도난 및 분실의 확률이 크고, 도난, 분실 시 개인정보, 업무에 관련된 정보 등이 유출되어 개인적 피해나 지적재산의 큰 손해를 불러올 수 있다.

2.1.4. 플랫폼

현재 스마트폰의 대표적인 두 플랫폼인 iOS와 안드로이드도 취약점을 가지고 있다. 주된 취약점은 바이러스/웜, 키보드해킹, 시스템 Unlock 등 이다. 여기서 시스템 Unlock 이란 사용자 임의로 펌웨어를 변조하여 사용하는 것을 말하며, iOs는 jailBreak(탈옥), 안드로이드는 Rooting이 있다. 이런 취약점들은 스마트폰 보안에 위협이 되고 있다.



[그림1] iOS[5]



[그림2] 안드로이드[5]

2.2. 대응 전략

스마트폰을 악성코드로부터 보호하고, 보안 위협요소들을 줄이기 위해서 현재 사용되고 있는 방안들은 단말용 백신 프로그램과 각 OS의 대응 방안 등이 있다. 먼저 국내외 백신프로그램에 대해서 알아보자.

2.2.1. 백신

국내외 주요 스마트폰 백신프로그램의 동향은 다음과 같다.

[표4] 국외 동향[4]

구 분	기 능
노턴 스마트폰 시큐리티(시만택)	안티 바이러스, 침입 차단시스템, SMS 안티스팸 기능
스마트폰 프로텍션(가이언에이지)	지적재산권 보호, 데이터 보호, 장치 보안 기능

[표5] 국내 동향[4]

구 분	기 능
Touchnsafe(소프트시큐리티)	통신채널인 탭에 대한 보안, 사용자 인증정보의 편리한 사용 환경 제공, 저부하 악성코드 탐지
Ahnlab Mobile Security(안철수 연구소)	악성코드 실시간 차단, 모바일 디바이스 보호

2.2.2. 스마트폰 OS 보안

주요 스마트폰 OS로는 안드로이드, iOS 등이 있다. 그리고 각 OS 마다의 보안 위협에 대응하기 위한 방안은 다음과 같다.

[표6] 주요 스마트폰 OS별 보안 방안[4]

구 분	기 능
안드로이드[6]	·보안 샌드박스(외부로부터 들어온 프로그램이 부정하게 조작되는 것은 막는 보안 형태) ·모든 App은 코드서명이 되어 있음 ·사용자 ID와 파일 접근
iOS[7]	·인가된 사용자만이 저장된 데이터에 접근 ·스마트폰 도난, 분실시 원격으로 데이터를 삭제하도록 지원 ·보안 플랫폼(의무적인 서명, 런타임 보호 등)

2.3. 새로운 전략 제시

현재의 대응 전략을 강화해 가는 것은 매우 중요하다. 하지만, 앞으로 더 많은 위협요소와 악성코드의 공격에 대응하기 위해서는 기존의 전략뿐만 아니라 새로운 방안을 찾는 것 또한 중요할 것이다.

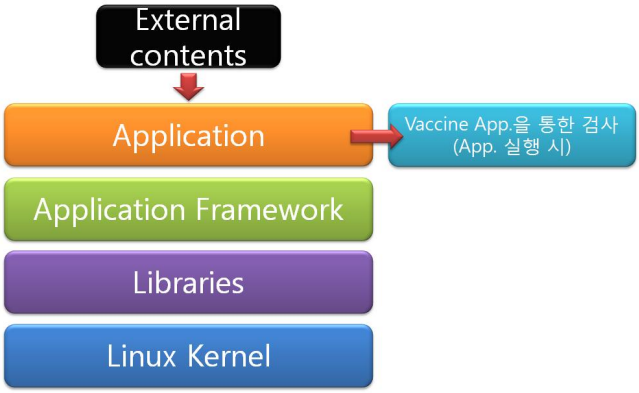
2.3.1. 정책적인 측면

정부는 악의적으로 악성코드를 유포하거나 제작하는 개발자들을 강력하게 규제해야 한다. 이를 위해서는 관련 법규를 엄격하게 만들고, 시행해야 할 것이다. 또, 전문가들로 구성된 조직을 구성하여 사고를 사전에 예방하고, 백신프로그램이나 연관된 신기술개발에 힘써야 한다.

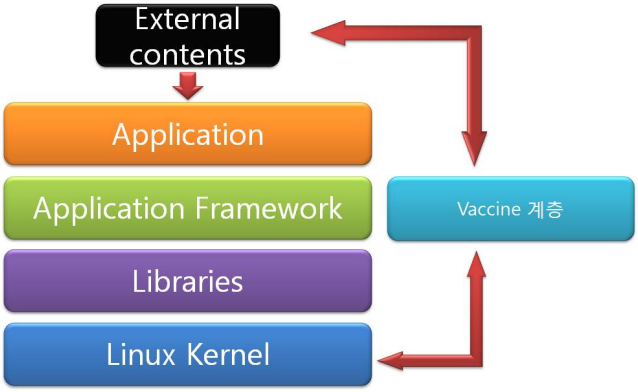
2.3.2. 플랫폼 측면

현재 스마트폰의 백신은 하나의 App으로 사용자가 실행했을 때에만 검사가 되는 형태이다. 즉, 외부 컨텐츠(App, 통신 등)가 새로이 스마트폰에 유입되어도 사용자가 백신프로그램을 실행시키지 않으면, 대부분은 그 컨텐츠를 검사하지 않는다. 이런 점은 컨텐츠 자체가 안전한 것인지, 또는 정상적인지 판단할 수 없게 만든다.

따라서 커널 자체가 관리하는 새로운 계층을 추가하여 새로운 외부 컨텐츠가 유입될 때마다 검사를 실시하게 한다면 보안 사고를 줄일 수 있다. 또, 실시간으로 계속적인 감지를 하는 기능을 계층에 추가하면 좀 더 강력한 보안체계를 형성할 수 있을 것이다.



[그림3] 기존의 백신 체계

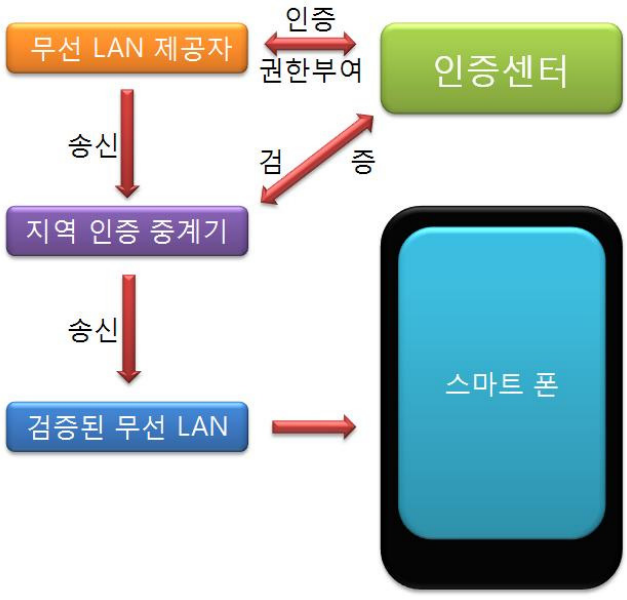


[그림4] 새로운 백신 체계

2.3.3. 네트워크 측면

네트워크 측면에서 가장 큰 위협요소는 무료 무선 랜을 통해서 유포되는 악성코드이다. 무작위로 검색되는 무선 랜은 아무런 제한 없이 스마트폰에 연결되고, 통신을 할 수 있다. 이것은 정보를 유출의 원인이 되기도 하고, 악의적인 프로그램의 침투 경로가 되기도 한다. 그럼에도 불구하고 사용자들이 무료 무선 랜을 선호하는 이유는 비싼 데이터 요금 때문이다. 그렇기 때문에, 사용자들은 무료 무선 랜에 매력을 느끼는 것이다.

무료 무선 랜 때문에 발생하는 보안 위협요소에 대응할 수 있는 전략으로는 스마트폰 사용자가 인증된 무선 랜만을 이용하게 하는 것이다. 즉, 무선 랜 제공자는 인증센터에 자신들의 확실한 신원정보, 무선 랜 정보, 서비스 목적을 제공하고 인증센터는 자체적인 검증을 통해서 안전한 무선 랜을 서비스할 수 있는 제공자에게만 권한을 부여하는 것이다. 그 다음, 무선 랜 제공자가 서비스를 제공하게 되면 1차적으로 각 지역별 중계기로 서비스가 도착하게 되고, 중계기에서는 인증센터와의 통신을 통해서 지금 제공되고 있는 무선 랜이 인증된 안전한 서비스인지 검증을 받은 뒤, 안전한 무선 랜만을 스마트폰 사용자에게 제공하게 하는 것이다. 이러한 인증센터와 지역별 인증 중계기를 통한 네트워크는 사전에 악의적인 목적을 가진 서비스 제공자의 무선 랜을 차단하여, 안전한 무선 랜만을 통신망에 서비스 할 수 있다. 따라서 무분별한 무선 랜으로 인한 보안 사고를 예방할 수 있을 것이다. 물론 인증센터를 설립하고 지역별 중계기를 설치하려면 정부와 기업 모두 힘을 합쳐야 하고, 정책과 규제를 잘 정립해야 하지만, 보안 사고를 줄일 수 있다면 분명 매력적인 전략 중 하나임에 틀림없다.



[그림5] 인증센터를 통한 안전한 무선 랜 서비스

2.3.4. 사용자 측면

스마트폰 사용자들은 백신 App 사용을 의무화해야 한다. 현재 스마트폰은 수동적으로 App을 통한 검사가 대부분이다. 따라서 정기적인 검사를 통해 악성코드의 감염을 예방해야 한다. 또한, 중요한 정보는 되도록 스마트폰에 저장하지 않아야 하고, 부득이한 경우는 분실이나 도난에 각별히 신경 쓰며, 개인 암호 설정을 생활화해야 한다. 그리고, 사용자들은 불법적인 마켓을 통한 무료 App을 사용하는 것보다는 공식 사이트를 통한 안전하고 검증된 App을 사용하여야 한다. 또, 항상 보안사고가 자신에게도 일어날 수 있다는 것을 인지하고, 보안의식을 개선하는데 힘써야 한다.

3. 결론

본 논문에서는 스마트폰에 악영향을 주는 악성코드의 종류에 대해서 알아보고, 보안 취약점을 제공하는 위협 요소인 개방성, 통신환경, 사용 환경 및 플랫폼에 대해서 분석하였다. 그리고 현재 국내외에서 사용되고 있는 백신 프로그램에 의한 대응방안과 주요 스마트폰 OS별 대응방안을 소개하고, 앞으로의 스마트폰 위협요소에 대한 대응 전략에 대해서 작성하였다.

스마트폰이 더 발전하게 되는 미래에는 더욱더 다양한 보안 사고가 발생할 것이다. 이는 현재의 정보 유출, 기기의 오작동 등의 문제와는 달리 인명피해, 금전손해 및 지적 재산권 침해와 같은 더 큰 문제들을 야기 시킬 것이다. 앞으로는 스마트폰 사용자들의 보안의식 개선이 필요하고, 보안에 관련된 교육프로그램들을 많이 시행하여 보안사고 대처 능력을 배양해야 하겠다. 또 정부와 기업 및 업체 등에서 규격화된 보안기술 및 여러 가지 대응전략이 필요할 것이며, 기술뿐만 아니라 규제, 정책등도 함께 병행되어야 할 것이다.

참고문헌

[1] 방송통신위원회

[2] 강동호, 한진희, 윤경, 조영섭, 한승완, 김정녀, 조현숙, “스마트폰 보안 위협 및 대응 기술”, 전자통신동향분석, 제25권 3호, 2010. 6.

[3] 김기영, 강동호, “개방형 모바일 환경에서 스마트폰 보안기술”, 정보 보호 학회 논문지, 제19권, 제5호, 2009. 10

[4] 최은영, 김미주, 정현철, “스마트폰 보안 강화를 위한 방안 연구”, 한국인터넷정보학회, 2010년도 학술발표대회, 2010

[5] 김기연, 조성제, “스마트폰 보안 취약점 동향”, 한국정보과학회, 2010 한국컴퓨터 학술발표논문집, 제37권, 제2호 (B), 2010

[6] 서승현, 전길수, “스마트폰 보안 위협 및 대응 전략”, TTA 저널, 132, 44-48, 2010