情 報 保 護 學 會 誌
第21卷 第3號, 2011. 5

악성코드 동향으로 살펴본 스마트 기기의 보안 위협

최 은 혁*

요 약

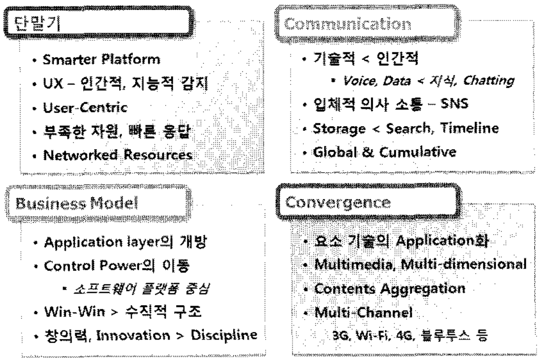
2009년 아이폰 출시로 시작된 국내 스마트폰은 트위터, 페이스북과 같은 SNS와 더불어 급속하게 보급되어 1,000만 사용자 시대를 맞이하고 있으며, 스마트폰의 경험을 그대로 활용할 수 있는 태블릿의 출연으로 인해 개인적인 활용에서 업무의 효율성과 형태에 대한 변화도 가져오고 있다. 모바일 오피스, 스마트워크 등 정부와 기업의 업무 효율화에 대한 관심과 녹색 성장 정책에 따라 스마트 기기의 확산과 활용은 더 급물살을 탈 것으로 보인다. 스마트 기기는 PC와 많은 부분이 닮아 있지만 이동성과 개인화된 기기라는 점에서 개인정보 유출이나 금전적인 피해에 노출되기 쉬워 이에 대한 대책 수립이 필요하다. 본 고에서는 스마트 기기로 인한 패러다임의 변화와 보안 위협과 보안 위협의 대표적인 모바일 악성코드의 트렌드를 알아보고자 한다.

Ⅰ. 패러다임 변화

스마트 기기를 통한 우리 생활의 변화는 정보를 소비하는 형태의 변화로부터 시작한다. 스마트 기기는 휴대성과 인터넷 연결로 인해 언제 어디서나(anywhere, anytime) 인터넷에 연결하고 활용할 수 있게 하는 연결매체(connected device)로, PC와 달리 하나의 장소에 고정되어 있지 않고 있으며, 하루 24시간 내내 늘 켜져 있고 휴대하고 있는 개인화된 기기이다 또한, 스마트 기기가 후각 기능을 제외하고 사람의 인지 기능을 대부분 가지므로 UX에 있어서도 편리한 인터페이스와 처리가 가능해 졌다. 매뉴얼을 통해 학습을 하지 않고도 쉽게 스마트 기기를 다룰 수 있게 되어 사용자 층이 넓어지고 있다.

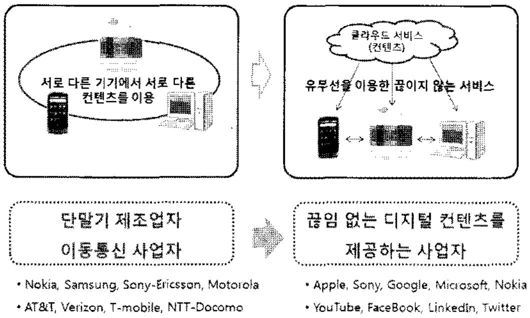
스마트 기기는 앱스토어(또는 마켓)를 통해 필요한 기능을 추가하고 변화시킬 수 있는 사용자 중심(user-centric)'의 장치로 인간적, 지능적 감지 기능을 통해 다양한 형태의 정보를 취득하고 소비할 수 있는 특성으로 인해 패러다임 변화를 주도하고 있다.

음성과 데이터 중심의 기술적인 소통 방식에서 스마트 기기를 통해 음성, 데이터 이외의 정보를 통한 소통이 가능해짐에 따라 사람과 사람간에 정보를 입체적으로 공유하고 의사 소통할 수 있는 SNS와 같은 커뮤니케이션 플랫폼이 등장하였다. 이와 같은 커뮤니케이션 플랫폼 사업자들은 애플, 구글과 같은 플랫폼 사업자와 함께 기존 모바일 시장을 장악하고 있던 이동통신사와 단말 제조사 중심의 공급자 위주 시장 (Supplier Driven Market)에서 사용자가 다양한 컨텐츠를 이용할 수 있는 플랫폼을 제공하는 사용자 중심 시장(Customer Oriented Market)으로 이동함에 따라 수직적 구조에서 상호 Win-Win하는 수평적 구조로 재편되고 있다.



〔그림 1〕 패러다임의 변화

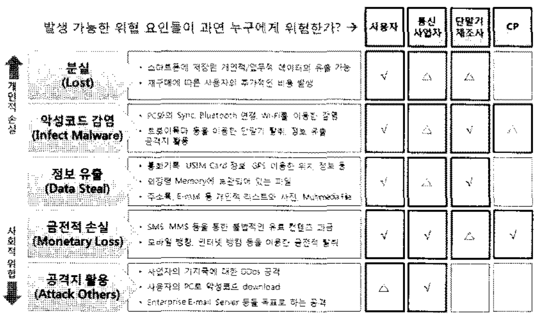
* 안철수연구소 플랫폼개발실 (caps@ahnlab.com)



〔그림 2〕 모바일 시장의 변화

Ⅱ. 모바일 보안 위협

빠르게 진화하고 있는 스마트 기기의 장점을 잘 살려서 활용한다면 어디서나 실시간으로 사람들과 소통하고 업무의 생산성을 높일 수 있다. 하지만 스마트폰의 편리함이라는 장점들은 자신의 위치 정보, 성별, 직업 등 개인정보의 '(사용자 동의라는 형태의) 적극적인 노출'을 통해서 이루어지고 있으며, 생산성 확대를 위해 정보를 집중하는 측면이 존재한다.



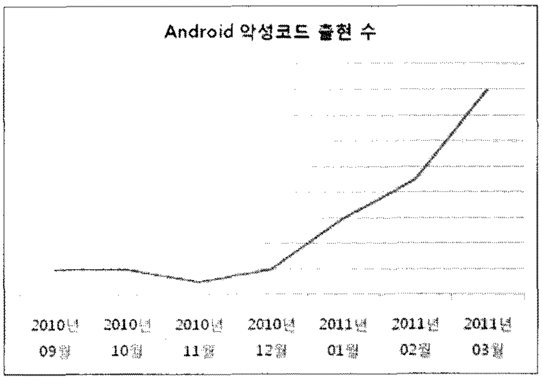
〔그림 3〕 스마트 기기의 5대 보안 위협

스마트폰의 위협은 크게 ①분실, ②악성코드 감염, ③정보유출, ④금전적 손실, ⑤공격지 활용으로 나누어 볼 수 있으며, [그림 2]에 나타나는 스마트폰의 5대 위협과 같이 사용자, 통신사업자, 단말기 제조사, 정보제공자에게 모두 위협 요인이 될 수 있지만, '개인정보의 유출과 금전적 손실을 가져오는 구조'로 되어 있어 사용자의 피해가 가장 크며, 이에 대한 대책이 필요하다.

특히, 스마트폰을 분실할 경우 돌이킬 수 없는 손실을 입을 수도 있다. 예로, 뱅킹 서비스나 증권 서비스와 같은 금융 거래 앱을 이용하여 계좌 이체, 증권 거래까지 가능하며, 해당 정보들이 스마트폰에 고스란히 보관될 경우 고정된 형태로 물리적인 보호를 받으며 이용할 수 있는 PC와 다르게 휴대의 편리성으로 인해 그 위협 수준이 높다.

2.1 모바일 악성코드 동향

2010년은 스마트 기기를 대상으로 하는 악성코드의 제작과 유포를 위한 실험적인 보안 위협들이 만들어진 해로, 중저가 스마트폰과 다양한 형태의 태블릿 출시로 사용자가 대폭 늘어난 2011년은 실제 스마트 기기에서의 다양한 개인정보들을 탈취하기 위한 악성코드가 본격 양산되기 시작할 것으로 예상된다.



〔그림 4〕 안드로이드 악성코드 출현 동향

안드로이드 플랫폼의 악성코드는 [그림 4]와 같이 2011년 들어서면서 악성코드와 변종들이 급격히 늘어나는 것을 볼 수 있다. 특히, 2월 감염된 안드로이드 플랫폼에서 개인정보를 탈취하기 위해 제작된 Android-Spyware/Adrd(이하 ADRD)와 Android-Spyware/Pjapps (이하 Pjapps)를 시작으로 3월에는 써드파티 마켓과 구글 마켓에서 통화명세까지 탈취할 수 있는 ADRD 변형이 발견되었다. 최근에서는 구글에서 배포하는 안드로이드 보안 앱 형태를 위장한 "BgService"가 써드파티 마켓을 통해 유포되었다.

특히 안드로이드 플랫폼은 마켓을 통하지 않고 ADB를 이용하여 설치할 수 있는 사이드 로딩 지원과 앱 설치시 마켓과 연동하여 앱의 무결성을 검증하지 않는 취약점을 악용하여 정상적인 앱에 악성코드를 삽입하는 형태로 변조한 후 리패키징(re-packaging)하는 방식으

로 악성코드 배포가 증가할 것으로 예상된다.

〔그림 5〕 보안 도구로 위장한 악성 앱(BgServce)

iOS의 경우 애플이 앱스토어를 통해 사전 검증된 앱에 대해서만 유통하고 있어 안드로이드 플랫폼에 비해 상대적으로 안전하지만, Cydia 등 블랙 마켓이 존재하며 다양한 제공자(Repo)가 존재한다. 탈옥(JailBreak)이 된 경우 손쉽게 Cydia를 통해 검증되지 않은 앱을 설치할 수 있으므로 안드로이드 플랫폼과 동일한 이슈가 발생할 수 있으나 애플의 정책에 의해 백신과 같은 보안 제품의 등록이 제한되어 있다.

그동안 애플이 앱을 검증하고 유통 관리를 해서 상대적으로 보안 위협으로부터 안전한 것으로 여겨졌던 아이폰도 Cydia와 같은 블랙 마켓을 통한 앱의 유통과 웹브라우저(사파리)의 취약점을 이용한 악성코드의 출연으로 안드로이드 플랫폼과 동일한 이슈가 발생할 수 있다. 특히, 한 번의 실행만으로 아이폰을 탈옥(JailBreak)시킬 수 있는 탈옥 툴이 있어 국내 아이폰 사용자의 30~40% 정도가 탈옥된 아이폰을 사용하고 있으며, Cydia를 통해 검증되지 않은 앱을 설치해 사용하고 있다. 또한, 작년 웹브라우저의 취약점을 이용한 탈옥 사이트(JailBreakMe.com)가 등장하였고, 최근에는 가짜 탈옥 사이트 “UNLOCK NOW FREE"가 등장해 iOS가 탑재된 기기(아이폰, 아이팟, 아이패드 등)로 접속할 경우 10~15초간 "DOWNLOAD UNLOCK 2 NOW FREE"라는 메시지와 함께 SIM 카드와 기기의 정보 일부를 파괴하는 위협이 보고 [그림 6]되었다.

스마트 기기의 확산과 모바일 악성코드가 양산되면서, 트위터, 페이스북과 같은 SNS가 악성코드를 포함한 보안 위협의 새로운 전파 경로로 활용되기 시작했다. 단축 URL(URL Shortening)의 악용으로 사전에 유해성을 검사해 주는 보안 단축 URL이 개발되자 1월에는 이러한 보안 단축 URL을 악용하여 허위 백신을 설치함으로써 악성코드의 감염을 시도하는 트위터 메시지들이 유포되었다. 2월에는 페이스북 담벼락으로 이용자들의 개인 정보를 탈취하기 위한 목적의 악성코드를 내려받도록 유도하는 게시물이 유포되었고, 페이스북 사용자 간의 채팅 메시지를 악용하여 허위 페이스 북 웹 페이지로 접속을 유도하여 악성코드를 내려 받도록 유도하는 기법도 발견되었다. SNS를 제공하는 플랫폼과 외부 환경을 악용하는 보안 위협들은 앞으로도 지속적으로 증가할 것으로 예상된다.

〔그림 6〕 웹브라우저의 취약점을 이용한 위협 (iOS)

2.2 모바일 생태계와 보안

모바일 시장은 노키아, 삼성전자, LG전자 등 단말 사업자와 KT, SKT, LGT 등 이동통신 서비스 사업자의 공급자 위주 시장에서 사용자 중심 시장으로 이동하고 있다. 이에 따라 모바일 플랫폼, 모바일 마켓, 모바일 앱으로 이루어진 모바일 에코시스템이 중요하게 부각되고 있다.

모바일 마켓은 모바일 앱과 콘텐츠를 개발자가 공급

하고, 사용자가 구매할 수 있는 형태로 새로운 유통 구조를 만들어내 스마트폰을 통한 새로운 사업 기회를 제공하고 있다. 대표적인 모바일 마켓으로는 애플의 앱스토어와 구글의 안드로이드 마켓이 있으며, 국내 통신사에서 제공하고 있는 T-Store, 올레 스토어가 있다. 애플 앱스토어는 애플의 관리 하에 운영되는 스토어로 애플리케이션은 애플이 제공하는 심사 기준에 따라야 하며, 이 기준에 어긋날 경우 앱을 등록할 수 없도록 하는 '폐쇄형' 운영 구조를 갖고 있다. 애플 앱스토어의 애플리케이션이 자체적인 결제 시스템이나 애플 사업과의 잠재적인 경쟁 등이 있을 경우 등록이 거절되는 경우가 있어 이슈화되기도 한다. 구글의 안드로이드 마켓은 애플 앱스토어와 달리 마켓을 열어 놓고 개입하지 않는 '개방형' 정책을 펴고 있다. 안드로이드 마켓에는 애플리케이션 개발자 누구나 등록 가능하지만 최소한의 검증도 이루어지지 않아 마켓 자체가 악의적인 앱을 유포할 수 있는 곳으로 활용될 수 있다. 약 10만여 개의 앱이 등록되어 있으며, 최근에 국내에서도 유료 결제가 가능해져 안드로이드 마켓이 활성화 될 것으로 예상된다.

(그림 7) 루팅 관련 코드가 삽입된 악성 앱(Android-Exploit/Zft)

애플이 앱에 대한 검증을 수행하는 애플의 앱스토어가 안드로이드 마켓에 대해 보안성은 우수하지만, 이 부분도 앱의 전체적인 기능이나 사용성 검증 보다는 자신들이 제공한 가이드에 따라 사용 API를 준수하였는지, 앱이 유통되는 국가의 법적인 저해 요소가 없는지 수준에 머물기 때문에 실제 사용자의 개인 정보 보호에 대한 부분에 대한 이슈가 있다. 애플의 검증을 통해 앱스토어를 통해 배포된 국내 앱 하나가 지난 3월 말 2~30분 사이에 3G망을 통해 2~300M를 사용하는 현상과 같이 사용성을 검증하지 못한 경우가 있었다. 해당 내용은 웹이 악성보다는 앱의 버그로 인해 과다 트래픽을 사용하게 된 경우로 애플의 검증이 완벽하지 않다는 반증으로 볼 수 있다.

모바일 애플리케이션을 개발할 때는 PC에서의 개발과 달리 전력 소모를 최소화 할 수 있도록 해야 하며, 설치본 크기도 최소화해야 한다. 또한, 사용자의 요청에 몇 초 내에 반응을 하거나 시간이 걸릴 경우 진행에 대해 진행 상태 등을 알려주는 형태로 UI에 보다 많은 신경을 써야 한다. 이외에도 모바일 단말의 특성을 고려하여 많은 계산이 필요하거나 웹과의 매쉬업(mash-up) 등 복잡한 로직이 들어간 경우 클라우드 서비스를 이용하는 방법을 검토해야 하며, 이 때 통신을 안전하게 할 수 있는 방안도 같이 검토 되어야 한다.

악성코드 대응 입장에서 보면 모바일 에코시스템의 보안을 위해서는 기존 PC 방식의 시그니처 기반의 악성코드 대응을 기본으로 앱의 비정상 행위를 탐지하는 행위기반 탐지 기술이 필요하다. 앱의 행위로는 앱 설치 시 요청하는 권한, 접근하는 정보, API 호출 순서, 주기적인 외부 서버(IP)와의 통신 등을 다양한 형태의 규칙으로 정의할 수 있다. 참고로, [그림 7]은 정상적인 안드로이드 폰에서 비정상적인 권한(루트 권한)을 요청하는 악성 앱의 예이다. 이외에 악성코드로 의심되는 앱을 수집 및 분석할 수 있는 인프라의 구축도 필요하다.

2.3 모바일 앱 검증의 필요성

앱은 기기이 출시될 때 탑재되는 탑재(preload) 형태와 사용자가 마켓을 통해 설치하는 설치(download) 형태가 있다, 탑재형 앱은 기기 출시 전 단말제조사에서 기능 모듈, 플랫폼에 대한 영향, 플랫폼이 호환성 등에 대한 절차에 따라 검증되며, 설치형 앱은 기기 출시 후 제공되는 마켓의 정책에 따라 평가 및 검증이 이루어진다. 스마트 기기는 마켓을 통해 앱을 설치하는 형태로 플랫폼별로 제공하는 검증 절차가 다르다.

안드로이드 플랫폼은 구글에서 개발 가이드와 CTS (Compliance Test Suite)를 제공하여 플랫폼에 대한 호환성을 검증할 수 있도록 하고 있지만 앱 자체의 사용성, 보안성에 대한 검증을 할 수 있는 가이드나 도구가

제공되고 있지 않다. 안드로이드 플랫폼의 경우 안드로이드 마켓, 웹을 통한 다운로드 설치, ADB를 통한 설치가 가능하여, 앱의 검증 여부를 확인할 수 있는 방법이 존재하지 않아 이에 대한 대책 수립이 절실하다.

MS의 윈도우 모바일은 PC의 윈도우 환경과 유사한 형태의 디지털 인증서 기반의 인증 제도를 갖고 있지만 검증에 소요되는 비용이 1회에 \$250~\$400로 다른 플랫폼에 비해 비싼 편이나, 국내에서 윈도우 모바일의 시장 점유율이 크지 않고 WinPhone 7의 경우 자체적인 마켓을 통해서만 앱을 유통할 예정이어서 현재보다 보안성이 강화될 것으로 예상된다.

앞서 살펴본 바와 같이 모바일 플랫폼에서 제공하는 검증 방식의 목표는 단말 또는 망의 안정성에 중점을 두고 있어 플랫폼 호환성 검증, 망 호환성 검증, 정적 소스 분석(소스 코드가 있을 경우) 등 애플리케이션이 시스템에 해가 되는지를 검증하고 있다. 이와 같은 검증 방식은' 사용자'를 고려하지 않은 방식으로 개인정보를 많이 갖고 있고 금전적인 피해를 입을 수 있는 모바일 단말의 특성을 고려할 때 사용자 정보 보호를 중심으로 하는 애플리케이션의 바이너리 단위 분석, 동적 실행 검증, 악성코드 검증 과정을 추가적으로 할 필요가 있으며,' 설치형 앱'의 경우도 마켓을 통해 유통되기 전에 검증할 수 있는 제도적인 장치가 필요하다.

Ⅲ. 맺음말

스마트 기기의 보안 이슈는 개인 정보의 유출과 금전적인 피해와 관련이 깊어 PC의 보안과는 다른 형태의 접근이 필요하다. 자칫 PC의 보안 기술을 그대로 스마트 기기에 적용하여 사용성과 효율성을 중요시하는 스마트 기기의 사상을 훼손할 수 있으므로 스마트 사상에 부합되는 보안 기술의 개발과 적용이 필요하다. 특히, 모바일 에코시스템 전반적인 보안을 위해서는 이동통신사, 단말제조사, 마켓 운영자, 개발사, 보안업체의 협업과 협조가 필요하며, 제도적인 뒷받침도 있어야 한다.

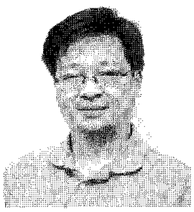
참고문헌

[1] 김홍선, "스마트폰 보안과 패더다임 변화", 安 2010 특별판, pp.3-5, 2010

[2] Peter Gilbert, Byung-Gon Chun, Landon Cox, and Jaeyoen Jung, "Automating Privacy Testing of Smartphone Applications", Duke University, Technical Report CS-2011-02, 2011

[3] 방송통신위원회, "신규 모바일 단말 보안 강화", 스마트 모바일 시큐리티 종합계획, pp.24-30, 2010

〈著者紹介〉



최 은 혁 (Eunhyeog Choi)
정회원
1993년 2월 : 동국대학교 전자계산학과 졸업
1995년 8월 : 동국대학교 컴퓨터공학과 석사
2007년 4월 ~ 현재 : 안철수연구소 플랫폼개발실 실장
관심분야 : 정보보호, 스마트폰 보안, mHealth