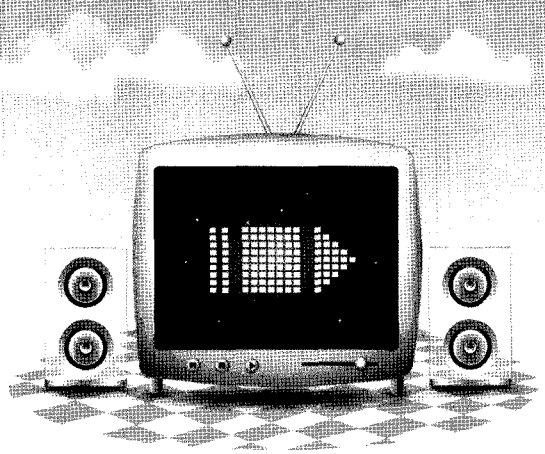
모바일 생태계의 보안 이슈 및 전망



김홍선 | 안철수연구소 대표이사
최은혁 | 안철수연구소 모바일개발팀장

1. 머리말

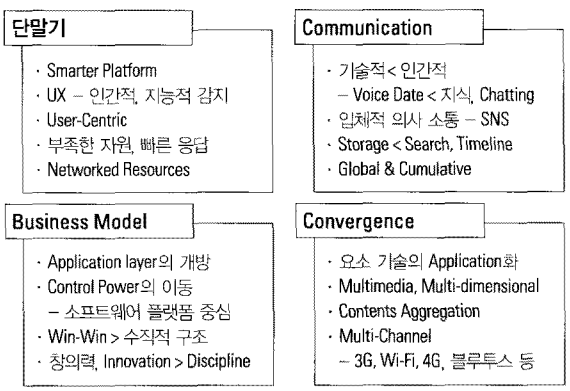
2010년 11월 현재 30여 종의 스마트폰이 출시되어 사용자가 500만 명을 넘겼으며, 연말이면 스마트폰 사용자가 전체 사용자의 15%에 이를 것으로 예상된다. 또한, 모바일 오피스, 스마트워크 등 정부와 기업의 업무 효율성 정책에 따라 스마트폰 열풍은 더 강해질 것으로 보인다. 스마트폰은 PC와 달리 이동성과 개인화된 기기로 개인정보 유출이나 금전적인 피해에 노출되어 있어 이에 대한 및 대책 수립이 필요하다.

본 고에서는 스마트폰으로 촉발된 패러다임의 변화, 모바일 생태계의 보안 이슈를 바탕으로 모바일 보안 산업의 미래와 시장을 전망해 보고자 한다.

2. 패러다임의 변화

스마트폰은 우리를 정보(인터넷)와 어느 곳에서나 연결해 주고 활용할 수 있게 하는 연결 매체(connected device)로, PC와 달리 하나의 장소에 고정되어 있지 않고, 하루 24시간 내내 곁에 있고 늘 켜져 있는 개인화 장치(personalized device)이다. 스마트폰은 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.

사람과 정보를 연결하면서 SNS(Social Networking Service)와 같은 입체적인 의사 소통이 이루어지고 있으며, 사업적으로 이동통신사와 단말제조사가 독점하던 시장에서 소프트웨어 플랫폼 중심으로 이동함에 따라 수직적 구조에서 상호 Win-Win하는 수평적 구조로 재편되고 있다.



[그림 1] 패러다임의 변화

스마트폰을 이해하는 몇 가지 키워드로 앱(Application), 앱스토어(AppStore), 위치정보 서비스(LBS), 소셜 네트워킹(SNS), 클라우드 컴퓨팅 그리고 융합(Convergence)과 매시업 등이 있다.

3. 모바일 보안 이슈

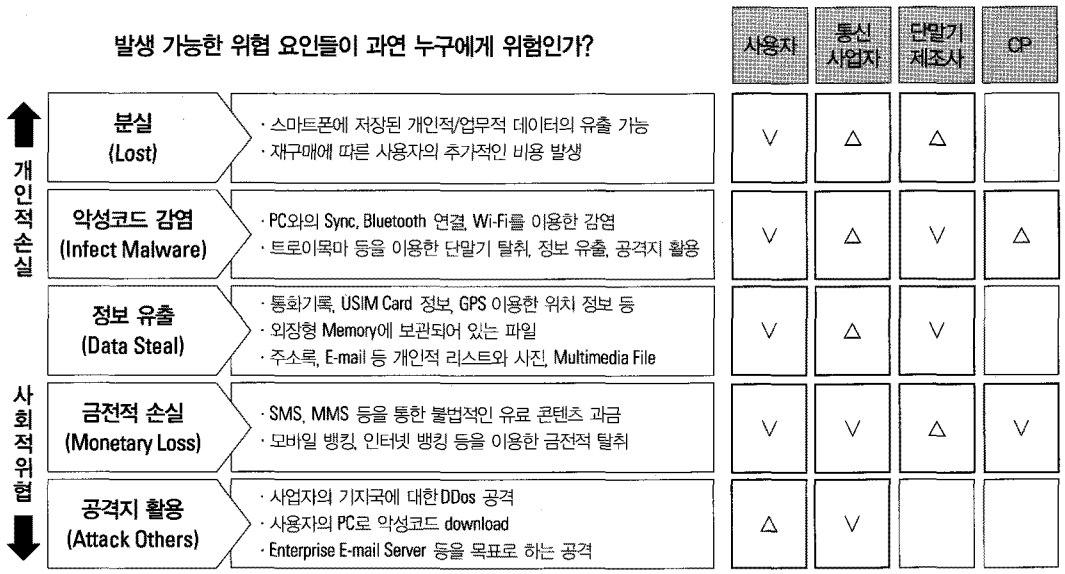
빠르게 진화하고 있는 스마트폰의 장점을 잘 살려서 활용한다면 어디서나 실시간으로 사람들과 소통하고 업무의 생산성을 높일 수 있다. 하지만 스마트폰의 편리함이라는 장점들은 자신의 위치 정보, 성별, 직업 등 개인정보의 '(사용자 동의라는 형태의) 적극적인 노출'을 통해서 이루어지고 있으며, 생산성 확대를 위해 정보를 집중하는 측면이 존재한다.

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.

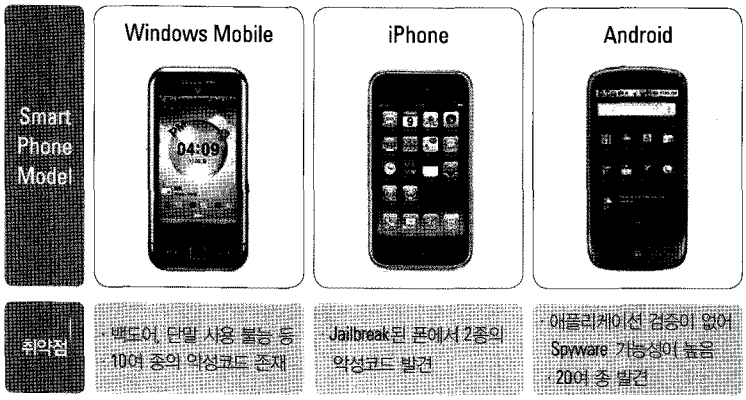
특히, 스마트폰을 분실할 경우 돌이킬 수 없는 손실을 입을 수도 있다. 예로, 뱅킹 서비스나 증권 서비스와 같은 금융 거래 앱을 이용하여 계좌 이체, 증권 거래까지 가능하며, 해당 정보들이 스마트폰에 고스란히 보관될 경우 고정된 형태로 물리적인 보호를 받으며 이용할 수 있는 PC와 다르게 휴대의 편리성으로 인해 그 위협 수준이 높다.

4. 모바일 악성코드의 특성

최근에 스마트폰의 개인정보와 금전적인 이득을 노리는 악성코드들의 출연 빈도가 급증하고 있는데, 윈도우 모바일이나 안드로이드 기반의 스마트폰들은 검증되지 않은 앱을 위장하여 사용자의 주소록, 통화기록, 문자 메시지 등을 빼돌리기도 하며, 금융거래 앱을 위



[그림 2] 스마트폰의 5대 위협



[그림 3] 플랫폼별 악성코드 및 위약점

장하여 사용자 정보의 계좌 정보를 빼내기도 한다. 아이폰의 경우 애플이 앱스토어를 통해 사전 검증이라는 제도를 두고 있지만 Cydia 등 블랙 마켓이 존재을 통해 앱의 유통도 이루어지고 있고, 탈옥(JailBreak)이 된 경우 검증되지 않은 앱을 설치할 수 있으므로 동일한 이슈가 발생할 수 있으나 애플의 정책에 따라 백신 등의 제품 등록이 제한되어 있다.

현재까지 알려진 모바일 플랫폼별 악성코드 및 취약점은 유럽에서 유통되고 있는 심비안 계열이 가장 많으며, 국내에서 확인된 것은 [그림 3]과 같이 윈도우 모바일은 백도어, 단말 기능을 제한하는 형태의 악성코드 10여 종, 아이폰은 '탈옥' 된 상태에서의 2종의 악성코드가 발견되었다. 안드로이드는 무단 SMS 발송이나 개인정보를 빼가는 스파이웨어 형태의 앱이 10여 종 발견되었고 현재 증가 추세에 있다.

국내에서 2010년 4월 윈도우 모바일 계열의 스마트폰에 게임을 실행할 때 국제전화를 몰래 걸어서 과금을 시도하는 사례가 발생했으며, 2010년 8월에는 동영상 재생기 앱으로 설치가 되어 무단 SMS를 발송하는 사례와 위치정보를 지속적으로 특정 서버로 전송하는 게임 앱이 보고되었다.

모바일 악성코드의 형태를 보면 초기 바이러스나 웜으로 제작을 시도하고, 대부분이 개인 사용자 대상의 정보 탈취가 목적이었으나 현재는 특정한 목적을 갖고 트로이 목마 형태로 제작되는 경우가 증가하고 있다. 전체 모바일 악성코드의 80% 이상의 트로이 목마이므로 앱을 설치할 때 다운로드 수와 사용자의 평가 등을 살펴보고 설치하는 것이 바람직하다.

5. 모바일 생태계와 보안

모바일 시장은 노키아, 삼성전자, LG전자 등 단말 사업자와 KT, SKT, LGT 등 이동통신 서비스 사업자의 공급자 위주 시장(Supplier Driven Market)에서 사용자가 다양한 콘텐츠를 이용할 수 있는 플랫폼을 제공하는 '사용자 중심 시장(Customer Oriented Market)' 으로 이동하고 있다. 이에 따라 모바일 플랫폼, 모바일 마켓, 모바일 앱으로 이루어진 모바일 에코시스템이 중요하게 부각되고 있다.

모바일 마켓은 모바일 앱과 콘텐츠를 개발자가 공급하고, 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 통신사

에서 제공하고 있는 T-Store, 쇼스토어가 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 있으며, 2010년 7월 현재 21만여 개의 앱이 등록 되어 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. 2010년 7월 현재 5만여 개의 앱이 등록되어 있으며, 최근에 국내에서도 유로 결제가 가능해져 안드로이드 마켓이 활성화 될 것으로 예상된다.

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 매시업 등 복잡한 로직이 들어갈 경우 클라우드를 이용하는 방법을 검토해야 한다. 이 때 클라우드와의 통신은 웹에서와 같이 안전하게 할 수 있는 보안 방안이 검토되어야 한다.

모바일 에코시스템의 보안을 고민하기 위해서는 시그니처 기반 악성코드 대응을 기본으로 애플리케이션의 행위를 기반으로 한 악성코드 탐지가 이루어져야 한다. 애플리케이션의 행위로는 애플리케이션 설치 시 갖는 접근 권한, 접근하는 정보, API 호출 순서, 주기적인 외부 IP 접속 및 데이터 전송 등을 다양한 규칙으로 정의할 수 있다. 이 외에도 악성코드로 의심되는 해당 파일을 수집 및 분석할 수 있는 인프라의 구축이 필요하며, 3G, Wi-Fi, WiBro 등 다양한 네트워크 환경에서의 실시간 업데이트에 대한 기능 제공도 필요하다.

6. 모바일 앱 검증

모바일 애플리케이션은 단말이 출시될 때 탑재되어 출시되는 '탑재형 앱(Preload App)'과 사용자가 마켓을 통해 설치할 수 있는 '설치형 앱(Download App)'이 있다. 탑재형 앱은 단말 출시 전 단말 제조사에서 각 기능 모듈 검증, 앱의 취합 및 검증을 수행하고, 솔루션 제공사에서 플랫폼 기능 검증, 플랫폼 호환성 검증 등이 이루어진다. 설치형 앱은 단말 출시 후 서비스사업자(이동통신사)의 주관 하에 사업정책에 의한 평가 및 검증, 배포가 이루어진다.

반면, 구글은 개발 가이드만을 제공하고 있고 안드로이드의 앱을 설치할 때 안드로이드 마켓, 웹을 통한 다운로드 설치, ADB(Anroid Debug Bridge)를 통한 설치 등 다양한 방법을 제공하고 있어 앱에 대한

검증이 거의 되고 있지 않다. 구글에서 플랫폼의 분산화(Fragmentation)로 인한 위험을 제어하기 위해 CTS(Compliance Test Suite)를 제공할 예정이지만 플랫폼에 대한 검증 또는 인증만 가능하고 애플리케이션에 대한 대안은 준비되지 않은 상태이다.

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 편이다.

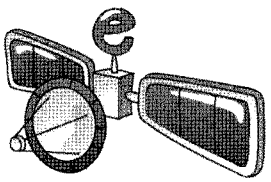
앞서 살펴본 바와 같이 모바일 플랫폼에서 제공하는 검증 방식의 목표는 단말 또는 망의 안정성에 중점을 두고 있어 플랫폼 호환성 검증, 망 호환성 검증, 정적 소스 분석(소스 코드가 있을 경우) 등 애플리케이션이 시스템에 해가 되는지를 검증하고 있다. 이와 같은 검증 방식은 '사용자'를 고려하지 않은 방식으로 개인정보를 많이 갖고 있고 금전적인 피해를 입을 수 있는 모바일 단말의 특성을 고려할 때 사용자 정보 보호를 중심으로 하는 애플리케이션의 바이너리 단위 분석, 동적 실행 검증, 악성코드 검증 과정을 추가적으로 할 필요가 있으며,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

특히, 앱스토어나 마켓을 통해 유통될 때 기능성과 더불어 사용성에 대한 정보를 제공할 필요가 있고, 평판 시스템 등의 도입도 검토되어야 한다. 이러한 모바일 에코시스템 전반적인 보안을 위해서는 단말제조사, 이동통신사, 마켓 운영자, 개발사 등 에코시스템의 모든 구성원의 협업과 협조가 필요하다.

7. 맺음말

스마트폰 보안을 위해서는 앱스토어나 마켓을 통해 유통될 때 기능성과 더불어 사용성에 대한 정보를 제공할 필요가 있으며, 평판 시스템 등의 도입도 검토되어야 한다. 이러한 모바일 에코시스템 전반적인 보안을 위해서는 단말제조사, 이동통신사, 마켓 운영자, 개발사 등 에코시스템의 모든 구성원의 협업 및 협조가 필요하며 제도적인 뒷받침도 있어야 한다. TTA

정보통신용어해설



콜드 부트 공격

Cold Boot Attack, -攻撃 [정보보호]

컴퓨터에 저장된 암호 키 정보 획득 공격.
온도를 낮추면 수 분 이상 정보가 유지되는 사실에 기반한 공격기법으로 컴퓨터 전원을 차단하고 장착 메모리를 저온 상태로 유지한 뒤 해당 메모리를 다른 플랫폼에 장착하여 아직 지워지지 않은 암호 키 정보를 분석하는 공격기법이다.