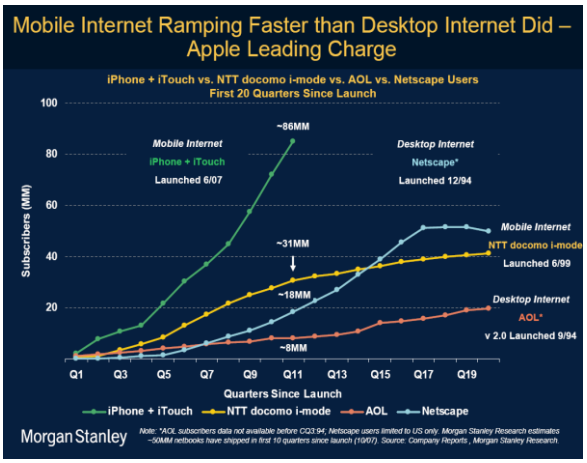
[정보보호] 모바일 에코시스템의 보안 위협과 안전화 방안

2009년 연말 국내에 아이폰의 출시로 시작된 스마트폰의 열풍은 2011년 3월에 1,000만 사용자에 이르고 연말에 2,000만 사용자가 될 것으로 예측되고 있다. 또한, 스마트폰의 경험이 재활용되면서 태블릿, 스마트TV, 스마트카까지 다양한 형태로 확대되고 있는 상황에서 스마트폰에 의한 패러다임의 변화와 그에 따르는 보안 위협요소 및 대응방안을 알아보고자 한다.

패러다임의 변화

이제는 누구나 익숙한 스마트폰에는 많은 새로운 개념과 단어들이 있는데 이 중에서 Touch, Apps, Internet이 가장 중요한 기능을 가리키는 단어가 될 것이다(<그림 1> 참조). Touch라는 가장 원초적이고 객관적인 Interface를 사용하고, 3G와 WiFi를 통해 인터넷에 쉽게 접근하여 다양한 정보를 취할 수 있고, 앱을 통해 피자에 토핑을 하듯 자기에게 맞는 스마트폰을 만드는 등 무궁무진한 새로운 경험을 우리에게 주고 있다.

<그림 1> 스마트폰 패러다임 키워드



<그림 2> 모바일 인터넷 사용자수 추이

현재 스마트폰의 시장은 애플의 아이폰과 구글의 안드로이드를 탑재한 안드로이드폰이 양분하고 있으며 국내의 경우 안드로이드폰이 60%정도의 마켓쉐어를 가지고 있는데 이는 중저가로 많이 뿌려졌고 홈쇼핑에서의 판매 영향도 있는 것으로 보이며 아무래도 갤럭시S의 판매호조 영향이 가장 클 것이며 스마트폰이 풀터치폰 시장을 빠르게 대체하고 있다.

모바일 인터넷은 기존의 인터넷보다 엄청나게 가파르게 성장하고 있으며 스마트폰의 확대와 비례하여 더욱 늘어나고 있다. 데스크톱 인터넷이 5년에 걸린 성장을 스마트폰은 2년 6개월 만에 넘어설 만큼 예측을 뛰어 넘어 급성장하고 있다(<그림 2> 참조). 모바일 인터넷이 활성화됨에 따라 노키아, 삼성 등의 단말기 제조업자와 AT&T, Verizon 등 이동통신 사업자에서 유무선을 통해 끊임없는 디지털 콘텐츠를 제공하는 사업자인 애플, 구글 등의 플랫폼 또는 콘텐츠 사업자 중심으

로 산업구조가 재편되었다. 이와 같은 산업 구조의 변화는 정보의 융합을 통해 새로운 사업모델과 기회를 만들어내고 있으나 안타깝게도 똑같이 보안위협도 함께 늘고 있다. 2011년 말까지 스마트폰이 2,000만대로 모바일 플랫폼에 30~40% 정도를 차지할 것으로 예측하고 있다. 스마트폰의 운영체제별 점유율을 보면 2010년 8월까지 아이폰이 25%를 유지하고 있고 안드로이드폰이 32%로 지속적 성장을 하고 있으며 기존의 강자였고 메일에 강한 블랙베리는 시장에서 완전히 밀려났다. 안드로이드는 디바이스의 영역을 가전과 FA까지 넓힐 것으로 보여 우리 생활에 더욱 가까워질 것으로 예상된다.

2010년 출시되기 시작한 아이패드, 갤럭시탭 등의 태블릿은 스마트워크, Enterprise Mobility 등이 활성화될 것으로 예측되기 때문에 2011년 이후에는 더 다양한 형태로 출시되고 시장을 이끌 것으로 보여지며 아이패드가 출시되고 100만대까지 판매되는 시간이 아이팟 1년, 아이폰 2개월에서 4주로 신기록 행진을 하고 있다. 아마도 아이팟과 아이폰으로 경험한 생태계에 대한 경험이 아이패드에 대한 구입장애를 없애버렸기 때문일 것이다. 태블릿 PC의 판매량 증가추세를 보면 2012년에 18%로 넷북의 판매량을 초과할 것으로 보이며 2013년에는 데스크톱 판매량을 넘어 21%로 노트북 다음으로 2번째가 될 것으로 예측하고 있다. 문제는 태블릿도 스마트폰과 같은 보안 이슈를 가지고 있다는 것이다.

패러다임을 변화시키는 3가지 축은 모바일 인터넷, 스마트 디바이스, 소셜 네트워크로 볼 수 있는데 2011년의 10대 IT 트렌드, SW 기술 이슈, 비즈니스 이슈 등에서 공통적인 키워드가 모바일, SNS, 클라우드 컴퓨팅인데 동일한 경향을 보이고 있다. 아쉽게도 보안업체들의 2011년 보안 이슈도 같은 키워드를 가지고 있다는 것에 주목할 필요가 있다.

보안 이슈

2010년 PC 보안 위협의 특징은 1) 악성코드를 이용한 공격이 대부분, 2) 악성코드 숫자의 엄청난 증가, 3) Target 공격으로 볼 수 있다. 여기서 APT(Advanced Persistent Threat)라는 위협이 현실이 되고 있으며 중국에서의 구글 해킹, 스턱스넷, 소니의 공격 등이 많이 알려진 예라고 할 수 있다. 그렇다면 모바일의 보안위협은 어떤가? 현 상태에서는 PC에서의 위협과 비슷한 동향을 보일 것이며 대신 POC(Proof of Concept) 형태가 많을 것으로 예측할 수 있다. 한국의 경우 2010년 8월부터 모바일 악성코드가 나타나기 시작하더니 2011년 3월에는 벌써 40~50건이 발견되고 있으며 하루에 100건 이상의 모바일 관련 파일의 문의가 접수되고 있을 정도로 예측을 넘은 동향을 보이고 있다. 2010년 하반기에 총 16개가 국내에서 발견되었는데 2011년 6월 전까지 74개의 악성코드가 발견되고 있다. 모바일 악성코드의 증상은 복합된 형태를 보이고 있으며 위치정보, 단말기 정보 등 정보 유출하는 형태와 통화 및 SMS발송 등의 무단 과금 형태, 그리고 강제 루팅 기능 등이 주를 이루고 있다.

단말기 및 통신서비스를 위한 공급자 위주의 시장에서 사용자가 다양한 애플리케이션을 직접 개발/설치하여 사용하는 사용자 중심 시장으로 이동하고 있다. 과거 공급자 위주였을 때 보안 이슈가 적었던 이유는 1) 단말기사이의 호환성 문제, 2) 단말기 외에는 정보가 제한되어 사용자가 마음대로 할 수가 없다, 3) 공급자의 Control이 가능한 상황이었기 때문이다. 사용자 중심으로 변화되면서 호환성이 해결되었고 Open된 환경으로 개발이 가능하며 공급자의 Control이 무너진 상황이기 때문에 단말기에서 플랫폼/애플리케이션 중심으로 전환되면서 보안 이슈가 부각되고 있는 중이다.

스마트폰에 의한 패러다임을 이해하기 위해서는 1) 지능화되고 개인화되어 가는 기기, 2) 애플리케이션 마켓, 3) Seamless한 Networking과 사람간의 관계를 중심으로 새로운 정보와 지식을 만들어가는 소셜 네트워킹이 이루고 있는 “생태계”에 대한 이해가 우선되어야 한다. 또한 “개방성”과 “연결성”에 따른 보안 위협이 존재한다는 것도 인정해야 할 것이다. 항상 연결되어 있다는 것은 공격자들에게는 매우 매력적인 점이기 때문이다. “개방성”에는 2가지 측면이 있는데 1) 공격 방법을 찾기 쉽다, 2) 대신 방어도 쉽거나 빠를 수 있다라는 점이다. 공격과 방어의 2가지 특성 중 어느 것이 빠르게 실행되고 지속성이 있느냐에 따라 개방성이 갖는 특징이 보안에서는 최선과 최악으로 평가될 수 있을 것이다.

모바일 보안 위협은 1) 개인정보 유출, 2) 계좌정보 유출, 3) 결재 도용, 4) 불법 과금, 5) ID도용, 6) SNS피싱, 7) 악성코드 감염, 8) 불법 위치 추적 등이며 SNS피싱과 불법위치 추적과 관련된 악성코드는 국내에서도 보고되어 있고 이런 위협의 가능성이 점점 높아지고 있다. 스마트폰의 시장 확대에 따라 모바일 악성코드와 보안 위협은 더욱 빠르게 증가하고 있고 사회 혼란이나 사이버 전쟁까지도 도구로 사용될 수 있다. 모바일 악성코드의 특징은 1) “More Phone, More Target”으로 스마트폰이 악성코드 제작자들의 목표가 될 것이며, 2) “잠재 위협 요소의 증가”로 자료 유출이나 금전적 목적으로 공격 동기가 다양화되고 더 많은 서비스가 나타남에 따라 그 서비스를 대상으로 하는 악성코드의 출현 가능성이 증가할 것이며, 3) “악성코드의 발전”은 동작 기반의 다변화와 오픈 소스를 이용한 지능화된 취약점 공격이 가능해질 것이며, 4) “해킹의 목적=금전적 이익”으로 스마트폰이 가지고 있는 다양한 정보는 공격자에게 매력적이며 스마트폰이 해킹에 편리한 환경이기 때문이다. 모바일 보안 위협 요소 중 가장 큰 것은 개인 정보 유출로 인한 개인적 손실이며 이통사와 사회적인 위협으로 확대가 될 것으로 예측할 수 있다. 모바일의 피해는 PC 보다는 그 피해의 강도가 더욱 큰 것이 문제로 다양한 단말기/플랫폼에 대한 보안 대책 및 애플리케이션 보안이 필요하게 되며 단말기 분실에서 단말기가 공격지로의 활용까지 모두 악성코드와 연관되어 있을 것이다.

대응 방안 및 기술

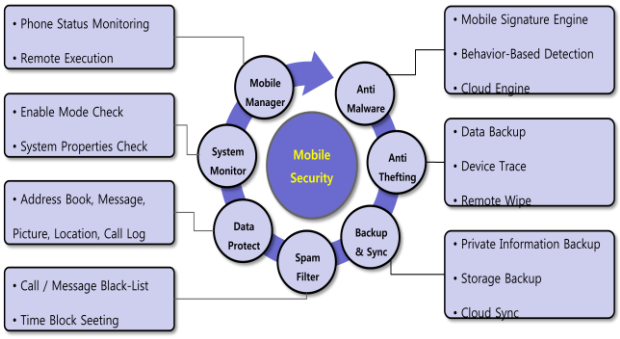
“앱”은 단말기 출시 전에 프리로드하는 경우와 출시 후에 마켓을 통해 다운로드하여 설치하는 형

태가 존재한다. 각 경우에 단말기제조사, 솔루션 개발자, 이동통신사의 단말기 출시 전의 앱 검증 업무는 일반적으로 플랫폼 및 프리로드 앱에 대한 취합 및 검증이 주이며 단말기 출시 후에는 이동통신사의 주관하에 다운로드 앱의 사업 정책에 따른 평가 및 검증이 주를 이루고 있다. 아직은 보안에 대한 검증은 못하거나 기초적인 것에만 국한되어 있다.

플랫폼별로 앱을 검증하는 방식은 안드로이드의 경우 검증도구나 인증 체계 등이 없거나 미약한 상태로 개발 가이드만 제공하는 형태로 그 만큼 보안에 있어서 취약한 상태이며 최근 발견되는 악성코드도 거의 안드로이드폰을 대상으로 하는 것이 많기 때문에 앱 검증에 대한 연구가 많은 상태이다. 아이폰인 애플은 검증 체계는 잘 갖추고 있다. 다만 애플의 가이드에 따라 개발되었고 해당 국가의 Regulation 준수 여부 등이지 개인 정보, 보안성에 대한 검증은 미약한 편이다. 윈도우 모바일도 늦게 나옴에 따라 검증 체계는 잘 갖추어져 있으나 보안성에 대한 검증은 역시 미흡한 편이다. 아이폰에서의 악성코드가 적은 이유는 이런 검증 체계의 영향도 있겠지만 그보다는 1) 폐쇄성, 2) SandBox 형태로 다른 리소스 접근 불가, 3) 제한된 멀티 태스크 기능 등이 악성코드에서는 더 큰 제약이 되고 있다. 아이폰을 탈옥(JailBreak)하면 악성코드 제작이 가능하다는 것은 이미 발견된 악성코드로 증명이 된 셈이다.

모바일 "생태계"에서의 앱 검증은 앱 유통경로 접점에서의 검증이 필요하다(<그림 3> 참조). 앱 스토어에서 폰 영역으로의 보안은 정적(Static)/동적(Dynamic) 앱 분석 또는 사람을 통해서 앱을 검증하고 백신이나 보안 API 등으로 보안이 필요하며 PC 영역에서의 검증은 백신을 이용한 단말기 스캔, 비허가된 앱 스토어 검증 등이 가능하다. 앱 검증 방식의 발전 방향은 1) 사용자 정보보호를 목적으로 해야 하며, 2) 검증 대상은 사용자 정보에 해가 될 수 있는 앱이 대상이어야 하며, 3) 검증 방식은 Binary Level 분석 및 Dynamic 실행 검증 방식이 될 것이며, 4) 검증 시점도 유통 전 검증으로 다운로드되기 전까지 유통경로에서 검증하여 사용자 보호 안정성 측면에서 앱을 검증해야 할 것이다.

<그림 3> 모바일 에코 시스템에서의 앱 검증



<그림 4> 모바일 오피스 보안

단말에서의 보안 위협에 대한 대응은 모바일 백신으로 관리가 가능하나 현재는 단말기에서 모든

동작을 하고 있다. 하지만 모바일의 제한된 환경으로 인해 곧 한계에 봉착할 것이다. 그 이유는 아직은 숫자가 적지만 악성코드가 많아질 경우 업데이트 문제가 발생하여 트래픽 문제가 예상되며 트래픽으로 인한 비용문제, 용량 문제가 발생하여 모바일의 성능까지 영향을 미칠 것이다. 이에 대한 대비책으로 요즘 뜨고 있는 클라우드 컴퓨팅 개념을 도입하여 Security Cloud Service를 이용해 업데이트가 필요없는 클라우드 환경으로 서비스가 제공될 것이다. 즉, 현재처럼 단말에서 판단하는 것이 아니라 클라우드에서 검사를 한 후 그 결과를 받는 개념으로 최근 악성코드의 추세로 보면 적절한 대책으로 보인다. 또 다른 장점은 하나의 단말, 하나의 파일과 행위에서 판단하던 기존 방법을 여러 개의 단말, 여러 개의 파일, 여러가지 행위 및 특징을 종합하여 판단하여 빠르고, 정확하게 대응할 수 있다는 것이다. 모바일에서의 클라우드 보안 환경은 PC나 클라우드로 백업하여 검사를 수행하고 악성코드 의심 파일 발견 시 알려주며 분실 대책으로 백업, 추적, 원격지 잠금 및 삭제 등의 기능을 제공할 수 있다.

마지막으로 모바일 오피스를 구축할 때는 여러 기능이 필요한데 Anti-Malware부터 단말기 관리까지 구축이 되어야 한다(<그림 4> 참조). 특히 Management에 대한 대안 및 솔루션 확보가 필수이며 단말기 정책에서 관리까지 mDM(Mobile Device Management)이 가장 중요해질 것이다.

조시행 (안철수연구소 연구소장, shcho@ahnlab.com)