특집 08

# 스마트폰 보안 기술 동향

목 차



이형찬 · 정진혁 · 김선휘 · 이정현
(숭실대학교)

## 1. 서 론

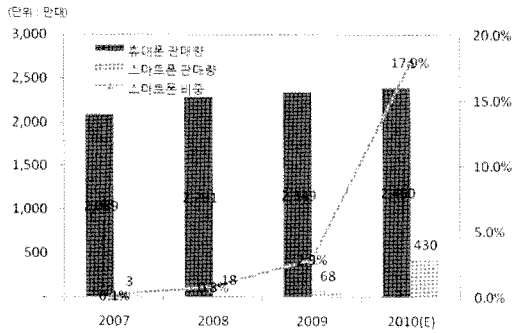
최근 휴대폰은 단순통화기능으로 출발하여 PDA기능, 모바일 결제(mCommerce), MP3, 카메라, DMB, 인터넷 및 E-mail 접속기능에 이르기까지 매우 빠른 속도로 진화하고 있다. 그 중에서도 기존 휴대폰의 통화 기능에 PC 환경에서 제공되던 다양한 인터넷 서비스 기능까지 하나의 단말기로 융복합화된 것이 스마트폰이다. 이와 같은 휴대단말 기능의 융/복합화 및 인터넷 연동의 가속화 추세는 제2세대(2G)에서 제3세대(3G)에 이어 3.5G, 4G의 흐름으로 진화중인 무선 이동통신 기술의 발전에 의해 더욱 촉진되고 있다. 2010년 이후의 스마트폰의 모습은 다음과 같은 기능을 지원하게 될 것으로 전망된다.

- 멀티(~100)코어CPU, Tera바이트급 메모리 등을 탑재한 고성능 휴대단말 출시
- 블루투스, 무선랜, 와이브로, DMB, 디지털TV 등의 다양한 네트워킹 기능 탑재
- 스마트폰용 소프트웨어의 多/高기능화
- 스마트폰 플랫폼의 오픈 플랫폼화
- 멀티미디어 컨텐츠의 범용화 및 개인화 증대
- 통신, 방송, 금융 등과 융복합화

스마트폰은 강력한 하드웨어를 기반으로 다양한 부가 서비스를 제공할 수 있는 계기가 되었고, 최근에는 증강현실(Augmented Reality), 소셜 네트워크 서비스(Social Network Service)와 위치 기반 서비스(Location-based Service)등의 서비스도 제공하기 시작하였다. 대표적인 사례로, 구글 버즈, 트위터, 페이스북 등을 들 수 있으며, 이러한 서비스들은 스마트폰 서비스의 새로운 이정표가 될 것으로 예상된다.

국내 스마트폰 시장은 2009년 3Q까지 미미하였으나, 2009년 4Q에 애플 아이폰(iPhone)의 국내 출시를 계기로 스마트폰 시장이 급변하는 상황이다. 2010년 4월말 현재, KT의 경우 iPhone 3GS 출시 후 60만 가입자를 돌파하였고, SKT는 옴니아2 등 다양한 스마트폰 대응으로 80만 가입자 수를 돌파한 것으로 보고되고 있다. 2010년말까지 국내 스마트폰 가입자수가 전체 430만에 달할 것으로 예상하고 있다. 하지만, (그림 1)에서 알 수 있듯이, 2009년말 현재, 전 세계 휴대폰 시장을 20%가까이 차지하고 있는 국내 제조사들이 스마트폰 시장 점유율에서는 3% 내외

밖에 기록하지 못할 정도로 고전하고 있는 실정이다.




(그림 1) 국내 휴대폰 시장 규모 및 스마트폰 비중
(출처: ROA Group Report, 2009.12. / 각 통신사 발표, 2010.01)

여기서 눈여겨 볼 점은 스마트폰의 비중 증대와 함께 데이터 서비스의 증가, 실행파일 공유 증가, 업무용 이용이 증가가 새로운 보안 취약점으로 이어질 수 있다는 점이다. (그림 2)에 제시된 바와 같이, 스마트폰의 지능화 및 네트워크 기능 탑재 추세에 발맞추어 이들 스마트폰을 공격하는 모바일 악성코드가 급증하고 있다. 스마트폰 보안 위협의 원인은 다음과 같이 크게 5가지로 분류할 수 있다.


(그림 2) 스마트폰 보안 위협 증가 원인

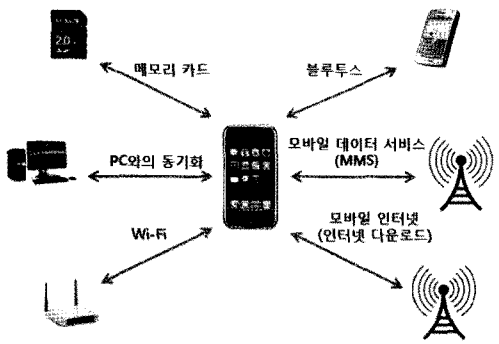
- 다양한 네트워크 접속: 스마트폰은 W-CDMA, CDMA-2000 등의 셀룰러 통신 방법을 기본적으로 제공하면서 근거리 통신을 위한 블루투스 및 인터넷 접속을 위한 Wi-Fi 또는 WiBro 등을 지원한다. 따라서 악성코드를 비롯한 위협이 시간이나 거리제한 없이 전파될 수 있는 환경을 제공한다. 휴대폰은 24시간 내내 켜져 있고 SMS 및 MMS전송 거리에는 제한이 없다. 또한, 폴브라우징 서비스를 사용하여 악성코드가 포함된 웹사이트에 접속할 경우 다운로드를 통하여 단말기를 직접 감염시킬 수 있다.
- 오픈 플랫폼: 휴대단말 플랫폼(OS 및 미들웨어)이 오픈 API 또는 오픈 소스화됨에 따라 보다 쉽게 악의적인 공격에 노출될 수 있다.
- 오픈 애플리케이션 마켓: 일반 개발자들이 자유롭게 애플리케이션을 등록할 수 있는 SW개발 및 수급 환경변화에 따라 악성코드의 전파 방식도 보다 편리해져 있다.
- 디바이스 컨버전스: 과거 PC 성능 수준의 다기능 및 고기능화된 모바일/IT/CE 환경에 인터넷과 결합되어 보다 강력한 악성코드가 활동할 수 있다.
- 다양한 개인정보 서비스: 주소록 정보 뿐만 아니라, 신용카드, 신분증, 멤버쉽 카드 등을 포함하는 모바일 지갑 서비스, 프로화일 정보를 활용한 개인 맞춤형 광고 서비스 등에 의한 개인정보 집중화 가중으로 인한 개인정보의 유출 가능성이 매우 높다.

위와 같은 이유로 스마트폰이 악성코드 제작자들의 새로운 표적이 될 전망이나 아직까지 스마트폰의 보안에 대한 기술적 대응이 미흡한 상태에서 스마트폰을 업무용으로 도입하거나 금융거래 서비스에 성급하게 도입할 경우 심각한 피해를 입을 우려가 높은 것이 현실이다. 더구나 스마트폰용 소프트웨어는 더욱 복잡해지는 반면 개발기간의 제약 등의 이유로 충분한 테스트가 어렵기에, 소프트웨어 버그 문제가 더욱 심각해지고 있다. 따라서 휴대단말용 보안기술, 특히 스마트폰에 적합한 악성코드/버그 검출과 분석 기술에 대한 연구와 이에 따른 대응 기술의 개발이 시급한 실정이다.

본 고에서는 날로 증대되는 스마트폰 악성코드의 동향, 스마트폰 플랫폼별 보안 특성을 살펴보고, 스마트폰 보안 취약점을 대응하기 위한 방안들에 대해 살펴보고자 한다.

## 2. 스마트폰 악성코드 동향

스마트폰 악성코드란 기존 PC 환경에서 발생하는 악성코드와 유사하게 스마트폰 단말기를 대상으로 개인정보유출, 시스템 파괴, 원격지 접속 등의 악의적인 행위를 수행하기 위해 제작된 악성 프로그램을 의미한다. 스마트 폰 환경에서 스마트폰 악성코드는 (그림 3)에서와 같이 PC와의 동기화, 메모리 카드, Wi-Fi, 스마트 폰 간의 통신, 스마트폰 데이터 서비스, 스마트폰 인터넷 등을 통해 전파될 수 있다[1, 2].



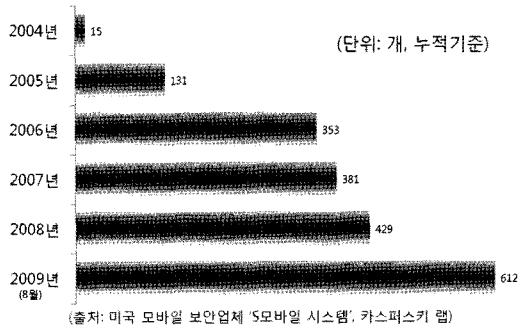

(그림 3) 스마트폰 악성코드 감염 경로

지금까지 등장했던 대표적인 스마트폰 악성코드들의 동작 유형은 〈표 1〉과 같다.

〈표 1〉 대표적인 스마트폰 악성코드 유형

| 유형 | 세부내용 |
|---|---|
| 파일 조작 | 응용 프로그램 및 시스템 프로그램에 특정 내용을 덮어 쓰거나 다른 파일로 교체하여 프로그램의 실행 및 단말기 사용이 불가 |
| 정보 유출 | 전화번호부나 주소록, 사진 등의 개인정보 및 스마트 폰 사용자의 수신 메시지 내용과 통화 내역이 외부로 유출 |
| 서비스 과금 | 감염된 스마트 폰을 통해 SMS와 MMS 메시지를 무단으로 발송하게 하여 금전적인 피해 유발 |
| 장치 사용 불가 | 서비스 거부 공격을 통해 스마트 폰의 배터리를 방전시키거나, 삽입된 메모리 카드의 패스워드를 임의로 변경함으로써 사용이 불가 |

국내에서 최근 발견된 '트레드다이얼(Tred Dial)'이란 스마트폰 악성코드는 윈도우즈 모바일(Windows Mobile) 플랫폼에서 동작하며 국제전화를 발신하는 서비스 과금 형태의 악성코드이다[3]. 해외 스마트폰 도입과 오픈 플랫폼 단말기 시장 확대로 인해 앞으로 더욱 더 많은 악성코드가 발견될 것이다. 특히, 최근에는 우리나라와 인접한 중국에서 중국어 버전 윈도우 스마트폰 및 심비안(Symbian) 상에서 동작하는 악성코드가 일부 발견되어 각별한 주의가 요망되고 있다.




(그림 4) 세계 스마트폰 악성코드 발견 추이

(그림 4)는 2004년부터 2009년 8월까지의 스마트폰 악성코드 수의 증가 추이를 나타낸다[4]. 2004년을 기점으로 악성코드의 수가 현저히 증가하고 있으며 2008년 6월까지 확인된 스마트폰 악성코드 수는 변종을 포함하여 총 400여개에 이르고 있다. 해외 백신업체 카스퍼스키에 의하면 2009년 8월 현재까지 612종의 스마트폰 악성코드가 발견되었다고 보고되었다.

## 3. 스마트폰 플랫폼별 보안 기술

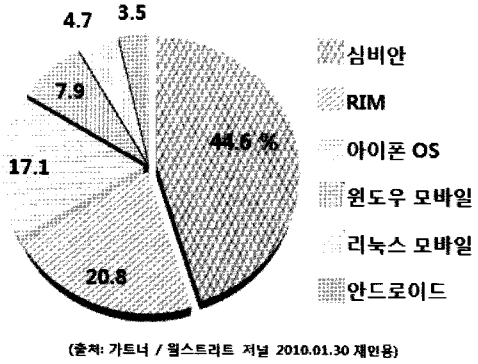
### 3.1 시장 동향

스마트폰 플랫폼[1]은 모바일 장치 (PDA, 휴대

1) 본래 스마트폰 플랫폼은 다양한 응용프로그램을 제공하기 위해 모바일 단말에 탑재된 OS 및 미들웨어를 포함한 소프트웨어 계층들을 총칭하는 용어이다.

폰, 스마트폰 등)을 제어하는 운영체제를 의미하며, 모바일 플랫폼, 모바일 OS, 핸드헬드(Handheld) OS 등으로 다양하게 표현되기도 한다.

과거 노키아(Nokia)의 스마트폰 플랫폼인 심비안은 일찍이 시장에 등장하여 선점을 하여, (그림 5)에서 보듯 2009년 3분기까지 세계적으로 가장 높은 점유율을 보여주고 있다. 차례로 블랙베리(BlackBerry) OS, 아이폰 OS, 윈도우즈 모바일, 리눅스 모바일, 그리고 안드로이드(Android)가 시장을 점유하고 있다. 최근에는 심비안을 사용하는 스마트폰은 점차 줄어들고 있고, 아이폰 OS, 안드로이드, 블랙베리 OS가 증가추세에 있으며, 특히 안드로이드 경우 구글폰을 앞세워 빠른 속도로 시장을 점유해 가고 있고, 2010년 하반기 국내 시장의 경우, 독자적인 플랫폼이 없는 국내 스마트폰 제조사들이 앞다퉈 안드로이드폰을 출시를 앞두고 있어 그 영향력이 더 커질 것으로 예상된다.




(그림 5) 스마트폰 플랫폼 시장 점유율 (2009.3Q 현재)

## 3.2 스마트폰 해킹 사례

최근 국내 스마트폰 플랫폼 시장은 아이폰, 안드로이드, 윈도우즈 모바일이 주도적으로 이끌어 나가고 있다고 해도 과언이 아니다. 현재까지 이들 3종의 스마트폰 플랫폼별로 보고된 대표적인 해킹사례들을 정리해 보면 〈표 2〉와 같다.

〈표 2〉 최신 스마트폰 해킹 대표 사례

| 플랫폼 | 악성행위 유형 | 버전 | 발표 |
|---|---|---|---|
| 아이폰 | 전화번호부, 파일시스템 목록 등 개인정보 탈취 | OS 3.1.3 | Black Hat DC 2010 |
| | 좀비 프로세스 활용한 DDOS공격 가능성 | OS 3.1.3 | A3 Security |
| | SMS, 전화번호부, 사진 등 탈취 | Safari | Pwn2Own 해킹대회 |
| 안드로이드 | ID, 패스워드 탈취 피싱 프로그램 | OS 2.1 | 쉬프트웍스 |
| 윈도우즈 모바일 | 프로세스 메모리 후킹을 통한 SMS 메시지 탈취 | CE 5.2 | 숭실대 모바일보안연구실 |
| | 리턴 오리엔티드 프로그래밍 기법 및 쉘코드 작성을 통한 공격 가능성 | CE 5.2 | Ruhr-University of Bochum |

아이폰에서는 다음 3가지 보안 이슈가 두드러지게 보고되었다. Black Hat DC 2010 컨퍼런스에서 Nicolas Seriot은 아이폰 OS 버전 3.1.3에서 전화번호 목록, 파일 시스템 목록보기, 인터넷 검색 목록, 키보드 캐쉬, GPS 위치정보와 같은 개인정보를 탈취할 수 있다고 발표하였고[14], 국내 보안업체 A3 Security가 최근 동일한 버전의 아이폰 OS에서 좀비 프로세스를 생성하고 개인정보 탈취, DDoS 공격 가능성 및 폐쇄망에 연결된 아이폰을 통해 폐쇄망을 침입할 수도 있다고 발표하였다[20]. 한편 Pwn2Own 해킹대회에서 Weinman, Iozzo는 아이폰의 사파리 브라우저의 취약점을 통해서 SMS 유출과 전화연결목록, 사진, 음악파일 등을 탈취하였다[19].

안드로이드 폰은 아직 많은 종류의 디바이스가 시장에 발매 되지 않아 활발한 조사가 이루어지지는 못했지만, 안드로이드 앱스토어의 경우, 등록된 소프트웨어가 악성코드로 판명될 시 악성코드 개발자 추적에 사용 가능한 코드사인 기능이 있으나, 앱스토어 자체적으로 소프트웨어의 보안성 및 기타 검증을 하는 시스템이 구축되지 않아있어, 자유롭게 악성코드가 등록될 수 있음이 알려져 있다. 또한, 소프트웨어 설치 단계에서 악성코드 판단을 모두 사용자에게 맡기며,

소프트웨어 실행에 필요한 권한에 대한 설명이 허술하다고 알려져 있다[5]. 또한, ID와 패스워드 및 개인정보를 절취하는 피싱 프로그램이 가능하다. 뿐만 아니라, 안드로이드 악성코드의 전파 경로를 6가지로 나누어서, 안드로이드 마켓, SMS, MMS, 웹브라우저, 파일전송 프로그램, USB를 통한 안성코드 전파가 가능하다고 보고된 바 있다[6].

최근 윈도우즈 모바일 플랫폼은 버전 6.1과 버전 6.5 모두 Windows CE 5.2 커널을 사용하는 것으로 알려져 있는데, 해당 플랫폼에서 리턴 오리엔티드 프로그래밍 기법을 사용하여 쉘코드를 작성하고 이를 통한 공격이 알려져 있다[7]. 또한 숭실대학교 모바일 보안 연구실에서 악성코드를 윈도우즈 모바일에 설치 한 후, 프로세스 메모리 후킹 기법을 이용하여 SMS 메세지 탈취가 가능하다고 최근 보고되었다 [8,9,10]. 이를 통해 윈도우즈 모바일의 경우, 사용자가 무의식적으로 설치한 악성코드가 다른 프로세스의 실행코드가 기록된 메모리영역은 물론, OS 영역까지 메모리를 직접 읽을 수 있고, 커널레벨의 쓰레드도 임의로 생성가능하고, 심지어 다른 프로세스의 실행코드가 기록된 메모리영역에 쓰기 접근까지 가능할 정도로 심각한 보안 취약점을 안고 있음이 실험을 통해 제시된 바 있다.

이렇듯 스마트폰 플랫폼에서는 많은 취약점들이 존재하고 있고, 현재까지 발견된 취약점이 스마트폰 플랫폼에 잠재된 모든 취약점이라 볼 수 없는 만큼, 아직 보고되지 않은 무수한 취약점들이 존재할 것으로 예상되므로, 앞으로 스마트폰 플랫폼 보안 특성에 따른 더욱 체계적인 연구가 필요하다.

### 3.3 플랫폼별 보안 특성

각각의 스마트폰 플랫폼은 독자적인 보안 정책을 가지고 있다. 스마트폰 플랫폼의 보안정책은 악성코드의 발발의 중요한 역할을 하는데, 그 대표적인 사례로 심비안의 경우, OS 버전 8.x에서 9.x로 버전업이 되면서 보안정책이 대폭 변경되었고 그로 인해 악성코드의 출현빈도가 급감하게 되었다. 심비안이 9.x로 OS 버전업이 되면서 크게 변경된 보안정책으로는 신뢰되지 않는 소프트웨어[2] 설치를 방지하며, 설령 사용자가 신뢰되지 않는 소프트웨어를 설치하더라도 실행시 스마트폰 플랫폼의 중요기능 사용을 제한하는 것이다. 이러한 보안 정책 때문에 악성코드가 심비안 OS 9.x 에서는 설령 설치되었다 하더라도, 악의적 행위가 극히 제한되고, 실질적인 악성코드로써의 의미를 크게 가지지 못하게 되었다. 현재까지 알려진 스마트폰 플랫폼들의 보안 특징을 살펴보면 〈표 3〉과 같다.

〈표 3〉 스마트폰 플랫폼 별 보안 특성

| 구분 | 아이폰 OS | 심비안 | 블랙베리 OS | 안드로이드 | 윈도우즈 모바일 |
|---|---|---|---|---|---|
| 개방형 플랫폼 | X | O | X | O | O |
| 오픈 소스 | X | O | X | O | X |
| 신뢰되지 않은 SW 설치 방지 | O | X | X | X (self-signed) | X |
| 신뢰되지 않은 SW 실행 방지 | N/A | O (limited access) | O (limited access) | X | X |
| 샌드박스 기능 제공 유무 | O | O | O | O | X |
| 멀티태스킹 기능 제한 | O | X | X | X | X |

아이폰 OS는 폐쇄형 플랫폼이고, 플랫폼의 소스가 공개되어 있지 않아 상대적으로 플랫폼 분석이 힘들다. 또한, 신뢰할 수 없는 소프트웨어는 설치될 수 없다. 즉, 모든 응용 소트프웨어는 앱스토어를 통해 배포되는데, 소프트웨어 등록 및 검증을 위한 제반 절차를 통과하지 못한 소프트웨어는 앱스토어에 등록되지 못하므로, 신뢰

2) 코드사이닝 절차에 의한 노키아의 서명을 받지 못한 소프트웨어를 의미함

할 수 없는 소프트웨어가 설치되거나 실행될 수 없는 구조이다. 또한, 사용자 프로그램이 시스템 프로그램의 자원 접근을 제한하도록 하는 샌드박스(SandBox)[3] 기능을 제공한다. 다른 OS와는 달리, 아이폰 OS는 멀티태스킹 기능[4]을 제공하지 않는 않아 백그라운드에서 동작하는 트로이 목마 형태의 바이러스의 동작을 제한하고 배터리 소모를 줄일 수 있는 장점을 지니지만, 다양한 소프트웨어를 동시에 사용할 수 없는 단점을 지닌다.

심비안은 플랫폼이 개방되어 있어 플랫폼 개발용 툴의 활용이 용이하고 소스코드도 최근 공개하였다. 앞서 언급하였듯이, 검증되지 않은 코드가 설치는 될 수 있지만, 커널에서 실행을 시켜주지 않거나, 혹은 가장 낮은 수준의 권한을 주어 스마트폰 시스템 자원의 접근을 제한하므로 플랫폼 차원에서 안전한 코드 실행 기능을 제공하고 있다고 할 수 있다. 그 외에 스마트폰 보안을 위한 필수 기능이라고 할 수 있는 샌드박스 기능을 제공하며, 멀티태스킹도 가능하다.

블랙베리 OS는 플랫폼과 소스가 비공개인 점을 제외하고는 플랫폼 아키텍처 상에서 제공하는 보안특성들은 심비안 OS와 대부분 유사하다.

안드로이드는 모바일 기기를 위한 소프트웨어 스택으로 개방형 플랫폼에 속하며 소스도 공개되어 있다. 신뢰되지 않은 소프트웨어의 설치 및 실행을 허용하여 보안에 대한 우려가 있지만, 샌드박스 기능을 통해 많은 위협요소들을 방어하고 있고, 멀티태스킹 기능을 제공한다.

윈도우즈 모바일은 개방형 플랫폼이며, 소스는 공개되어 있지 않다. 확인되지 않은 코드를 사용자가 강제로 설치할 수 있고, 그 이후로는 실행에 아무런 제약을 받지 않으며, 샌드박스 기능도 제공하지 않아 사용자 프로그램이 시스템 자원에 접근을 하는 것이 허용되는 취약점을 지니고 있다. 다른 플랫폼과 마찬가지로 멀티태스킹을 지원한다.

## 4. 스마트폰 취약점 대응 방안

### 4.1 사용자 대응방안

스마트폰 악성코드 사고에 대한 책임은 전적으로 시스템에만 존재할 수 없고, 사용자들에게도 일정부분 책임이 존재한다. 기존 피쳐폰에서 스마트폰으로의 급속한 전환이 일어나는 시점에서 사용자들은 스마트폰 보안에 대한 이해가 부족한 실정이다. 이에 방송통신위원회는 국내 스마트폰 사용자들에게 보안의식을 고양시키기 위하여, 스마트폰 '이용자 10대 안전수칙'을 아래와 같이 발표한 바 있다.

① 의심스러운 애플리케이션 다운로드하지 않기
② 신뢰할 수 없는 사이트 방문하지 않기
③ 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제하기
④ 비밀번호 설정 기능을 이용하고 정기적으로 비밀번호 변경하기
⑤ 블루투스 기능 등 무선 인터페이스는 사용시에만 켜놓기
⑥ 이상증상이 지속될 경우 악성코드 감염여부 확인하기
⑦ 다운로드한 파일은 바이러스 유무를 검사한 후 사용하기
⑧ PC에도 백신프로그램을 설치하고 정기적으로 바이러스 검사하기
⑨ 스마트폰 플랫폼의 구조를 임의로 변경하지 않기
⑩ 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트하기

3) 샌드박스(SandBox)는 보호된 영역 안에서만 사용자 응용프로그램이 동작될 수 있도록 하는 보안 소프트웨어로서, 네트워크를 통해 전송받은 응용프로그램의 시스템 자원에 대한 접근을 제한하는 기능을 제공한다.

4) 아이폰 4G에서는 멀티태스킹 기능을 제공할 것이라고 2010년 4월에 애플에서 발표한 바 있다.

이외에도 최근 스마트폰의 편리함과 다양한 기능에서 비롯된 서비스가 사회공학적인 기법을 활용한 범죄에 악용되는 사례도 발생하였다. 즉, 스마트폰을 이용해 트위터와 페이스북 등 소셜 네트워크 서비스를 이용할 때, 스마트폰의 GPS 혹은 기지국 망을 사용한 위치기반 서비스로 인해 사용자의 위치 정보와 서비스에 남긴 글을 통해 생활패턴을 파악한 후, 이를 악용한 범죄자들이 실제 빈집털이를 한 사례가 발생한 바 있다.

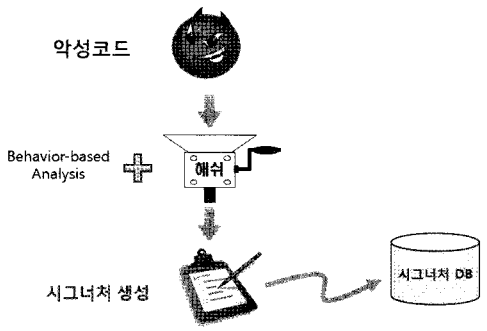
따라서, 사용자들은 단순히 수동적인 자세에서 벗어나 새로운 문명의 이기인 스마트폰 활용에 있어서 자발적이고 적극적인 자세로 '이용자 10대 안전수칙'을 지키며, 더 나아가 사생활 노출 및 개인 금융 정보보호에 각별한 노력이 요구된다.

## 4.2 기술적 대응방안

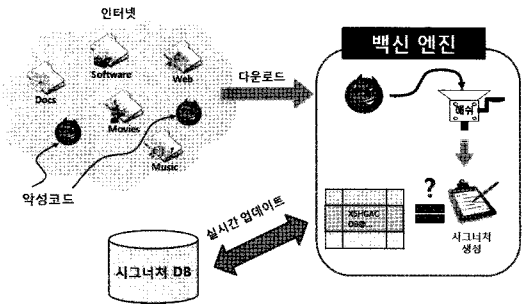
### 4.2.1 백신 소프트웨어의 한계

PC환경에서 악성코드 검출 및 제거 방법으로 백신 프로그램의 설치를 최우선적으로 고려해 왔던 것이 사실이다. 하지만, 스마트폰이 손안의 PC 개념이라고 해서 기존 PC에서와 동일한 접근방법이 스마트폰 환경에서도 그대로 적용할 수 있을 지에 대해서는 다시 한 번 검토해 볼 필요가 있다. 이를 위해 백신의 원리에 대해 간략하게 살펴보고자 한다.

악성코드 발견시 (그림 6)에서처럼 백신업체 또는 관련기관에서는 해쉬, 압축, 패턴추출 알고리즘 등을 통해 해당 악성코드에 대한 시그너처를 생성하여 이를 DB화 한다. 이를 사용자들에게 통보하여 개별 사용자가 각각 백신 업데이트 절차를 통해 이 업데이트된 시그너처 DB를 다운로드하게 된다. 그런 후, 악성코드로 의심되는 프로그램이 발견될 시 (그림 7)에서처럼 백신 프로그램 엔진은 시그너처 DB의 조회를 통해 사전 등록된 악성코드의 시그너처와 동일할 경우 해당 프로그램을 블록하거나 삭제하는 조치를 취하고, 그렇지 않을 경우 정상코드로 판단하는 원리를 따른다.

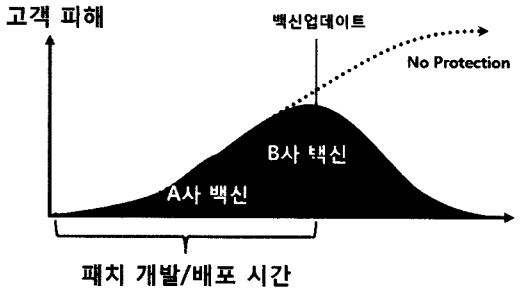



(그림 6) 악성코드 사전등록




(그림 7) 악성코드 탐지

여기서 백신의 허점을 파악할 수 있다. 즉, 백신은 시그너처가 등록된 악성코드에만 한하여 제 기능을 발휘하지만, 신종 악성코드의 경우 시그너처가 사전 등록되어 있지 않으므로, 문제의 악성코드가 시그너처 DB에 업데이트될 기간까지에 아무런 대처를 할 수 없는 기술적인 맹점이 있다. 이러한 허점이 기존의 PC환경에서는 백신 업데이트가 신속하게 대처하고, 피해수준이 일부 데이터 또는 이메일 손상 정도에 머물 경우 일반 사용자들이 큰 거부감 없이 이 허점을 용인해 주는 관습을 따라왔었다. 하지만, 스마트폰 환경에서는 기존의 PC와는 달리 그 데이터의 성격이 개인 프라이버시와 밀접하고, 요금청구 기능에 맞물려서 금전적 손실을 유발할 수 있는 데이터 손실이기 때문에 PC에서와 같은 방식으로 대응할 수 없는 측면이 있다.



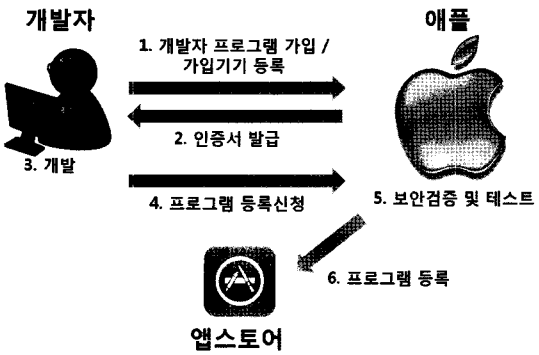

(그림 8) 기존 백신기술의 한계점

스마트폰뱅킹, 개인일정관리, 주소록관리, 통합메일관리 등을 간편하게 제공하는 바쁜 현대인의 비서인 스마트폰은 GPS, 카메라, 휴대전화, SMS의 기능도 관리하기 때문에, 개인정보의 총체라 할 수 있다. 이러한 스마트폰에서 악성코드로 인해 개인정보가 유출되고, 주소록을 절취당하고, 심지어 신용카드 정보가 유출될 경우 백신 업데이트를 아무리 신속하게 (예를 들어, 30초 이내로) 처리하여도 (그림 8)과 같이 패치개발/배포 시간 동안의 고객의 금전적 피해를 막을 수 없다는 맹점이 생기는 것이다.

### 4.2.2 소프트웨어 등록 및 검증

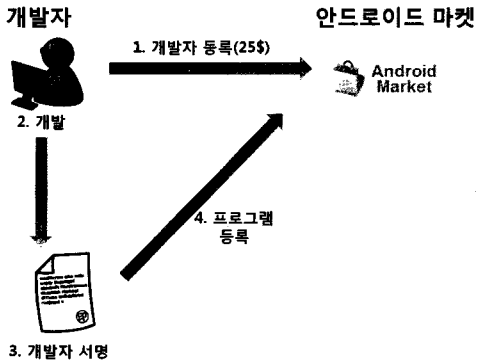
알려진 악성코드에 대한 탐지 및 치료를 위해서는 백신 소프트웨어만큼 현실적인 기술적 대안은 아직 없어 보인다. 앞서 언급했듯이, 알려지지 않은 악성코드의 확산으로 인한 피해를 줄일 수 있는 방법 중의 하나가 사용자 애플리케이션인 앱(App)의 등록시 이의 검증 메커니즘의 도입을 들 수 있다. 이를 위해 아이폰, 안드로이드, 심비안의 경우 각각 다른 앱 등록 프로세스를 가지고 있는데, 이에 대해 살펴보면 다음과 같다.

아이폰 앱스토어는 (그림 9)과 같은 절차로 소프트웨어 등록이 이루어지며, 개발자가 프로그램 등록시 이에 대한 보안성 검증 및 테스트가 이루어진다. 이 테스트를 통과하면 사용자 앱이 앱스토어에 등록되어진다. 하지만, 앱 검증과정




(그림 9) 아이폰 앱스토어 등록절차

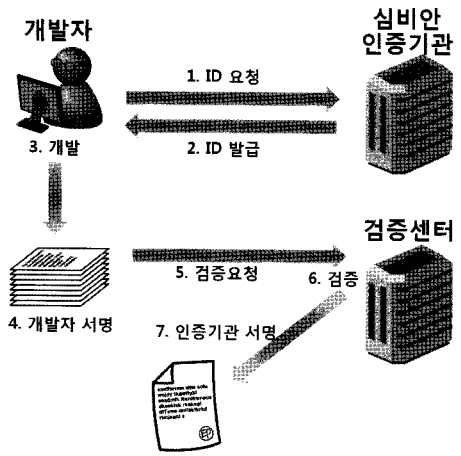
에 대해서는 폐쇄적으로 진행되어 어떤 검증과 테스트가 이루어지는지 알 수 없으며, 완벽한 보안성 검사를 하는 것은 아닌 것으로 알려져 있다. 스위스의 소프트웨어 엔지니어 Nicolas Seriot은 앱스토어 검증을 우회해서 악성코드를 등록하는 것이 가능하다고 Black Hat 2010에서 발표한 바 있다[14].




(그림 10) 안드로이드 마켓 등록절차

안드로이드 마켓의 경우, (그림 10)처럼 소프트웨어에 대한 어떠한 보안성 및 기타 검증 절차를 거치지 않는 완전개방형 정책을 사용한다. 따라서, 개발자가 자유롭게 마켓에 앱을 자체서명(self-sign)하여 등록할 수 있다. 또한, 자체서명을 하지 않은 채로 등록할 수도 있는데 이 경우에는 서명되지 않은 소프트웨어라는 경고 메시

지를 알려준다. 상대적으로 안드로이드 마켓에는 악성코드가 좀 더 수월하게 등록될 소지가 확률이 높아 보인다.




(그림 11) 심비안 소프트웨어 서명절차

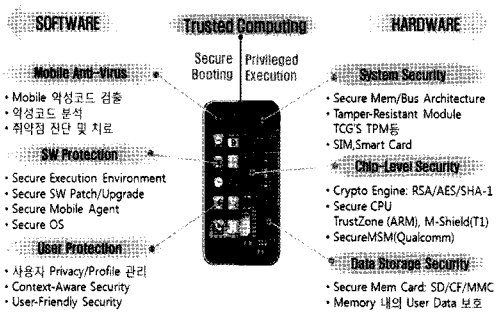
심비안의 경우, 아직 소프트웨어 마켓이 존재하지 않고, 노키아는 오는 5월초에 스마트 스토어 (Ovi-store)를 개장 할 예정이다. 비록 아직까지 소프트웨어 마켓이 존재하지 않지만, 심비안의 경우 (그림 11)과 같은 소프트웨어 등록 및 검증 프로세스를 가지고 있다. 일반 소프트웨어에 대해 자동화된 테스트를 수행하며, 일반 소프트웨어가 아닌, 즉 심비안 시스템에 중요 API를 사용하는 소프트웨어의 경우 2차 테스트를 거치게 된다. 2차 테스트의 경우, 소프트웨어 검토원에 의해 테스트가 이루어진다. 그러나 심비안의 검증 시스템도 역시 완벽하진 못하다. 실제로 이러한 등록 및 검증 테스트를 통과한 악성코드가 심비안 인증을 받은 사례가 2009년에 보고된 바 있다.

윈도우 스마트폰의 경우, 윈도우즈 마켓 플레이스 (Market Place)라는 소프트웨어 마켓이 2009년 후반기에 개장하였으며, 품질 검증, 컨텐츠 검증, 상용 검증의 3가지 기준에 따라서 검증한다. 자세한 프로세스는 알려져 있지 않으며, 국내 출시한 윈도우즈 스마트폰의 경우 현재 마켓플레이스를 지원하지 않으며, 아직 활성화되지 않아, 온라인 커뮤니티를 통해 소프트웨어가 주로 배포 되며, 이러한 소프트웨어들은 악성코드로부터 안전하지 못하다. 하지만, 2010년말 출시 예정인 윈도폰7에서는 이러한 문제들이 모두 해결될 것으로 전망된다.

이러한 사례로 볼 때, 신종 악성코드의 설치를 사전에 예방하기 위한 대책으로 코드 사이닝에 기반한 소프트웨어 등록 및 검증 절차는 백신 소프트웨어의 부족한 점을 상당부분 메울 수 있을 것으로 기대된다. 특히, 국내 모바일 소프트웨어 시장 활성화를 위해서는 애플 앱스토어와 심비안 소프트웨어 마켓의 검증 시스템을 벤치마킹하여 보다 체계적인 소프트웨어 등록 메카니즘을 강구해 나가야 할 것으로 사료된다.

### 4.2.3 스마트폰 단말 보안

사후 약방문 형태의 백신 프로그램과 사전 예방을 위한 코드사이닝 기술만으로는 스마트폰 보안을 근본적으로 해결하지 못하며, 스마트폰 소프트웨어뿐만 아니라 하드웨어 전반에 걸친 보안 대책 마련이 절실하게 요구되고 있다.




(그림 12) 스마트폰 보안 기술 분류

스마트폰 소프트웨어 보안 기술로는 다음 세부 기술들을 포함한다.

- 백신 소프트웨어: 악성코드/버그검출, 악성코드 분석, 취약점 진단 및 치료 기능을 담당한다.

- 소프트웨어 검증: 안전한 소프트웨어 실행환경 구축, 안전한 소프트웨어 패치 및 업그레이드 기술, 안전한 모바일 에이전트 및 OS 기술 등을 포함한다.
- 사용자 정보 보호: 사용자 프라이버시 및 프로화일 관리 기술, 상황인지 및 사용자 편의성을 고려한 보안 기술 등을 포함한다.

스마트폰 하드웨어 보안 기술은 다음과 같이 분류된다.

- 시스템 보안: 안전한 메모리 및 버스 구조 설계, 차세대 tamper-resistant 모듈, TPM (trusted platform module), SIM, 스마트카드 보안 등을 포함한다.
- 칩레벨 보안: RSA, AES, SHA-1 등을 포함한 암호 엔진, ARM사의 TrustZone, TI사의 M-Shield 등 안전한 CPU, Qualcomm사의 Secure MSM 모뎀 칩 등의 기술을 포함한다.
- 스토리지 보안: 보안 메모리 카드(SD, Compact Flash, MMC 등) 관련기술 및 메모리 내의 사용자 데이터 보호 기술들을 포함한다.

또한 보안 부팅 및 보안실행(privileged execution) 환경의 제공을 위해, Trusted Computing 기술을 하드웨어와 소프트웨어의 조합 형태로 스마트폰에 탑재할 필요가 있다.

## 5. 결 론

본 고에서는 국내 스마트폰 악성코드의 등장과 이로 인한 피해가 예상되는 현 시점에서, 그 심각성을 알리고자 스마트폰 악성코드 동향 및 스마트폰 플랫폼 보안동향을 소개하였다. 기존 PC와는 달리 스마트폰에는 개인정보가 집중화되어 있고 통신과금 체계를 악용한 금전적 피해를 입힐 수 있어, 보안에 대한 필요성이 증대 되고 있다.

현재의 스마트폰 시장은 앱스토어 중심의 소프트웨어 및 콘텐츠 경쟁에 치중하고 있다. 안드로이드 마켓, 삼성 앱스토어, 아이폰 앱스토어, 마이크로소프트의 마켓플레이스 등 스마트폰 관련 기업들은 앞다투어 스마트폰 소프트웨어 마켓용 컨텐츠를 제공하고 있다. 뿐만 아니라 보다 많은 개발자들을 확보하고, 편리하고 강력한 소프트웨어 개발툴 개발에 온 힘을 다하고 있는데, 이를 1차 스마트폰 전쟁이라고 한다면, 다가올 2차 스마트폰 전쟁의 키워드는 보안이 될 것이다.

향후, 스마트폰 소프트웨어 시장에서 한 플랫폼에서 성공한 소프트웨어 또는 콘텐츠는 반드시 다른 플랫폼에도 출시할 것으로 전망된다. 즉, 개발자 입장에서 특정 플랫폼에 제한하지 않고 보다 많은 사용자 확보를 통한 수익성 증대를 위해 동일 소프트웨어의 멀티 플랫폼화 전략을 구사하게 될 것은 자명한 사실일 것이다. 따라서, 머지않아 모바일 소프트웨어 마켓 시장은 플랫폼에 따라 이용자수의 차이는 있을 수 있지만, 제공되는 소프트웨어 수와 기능은 균형을 이루게 될 것으로 예상된다. 고로, 사용자들은 같은 기능을 제공하는 스마트폰이라면 보다 안전한 스마트폰을 찾게 될 것이다.

결론적으로 2차 스마트폰 전쟁에서 우위를 점하려면, 스마트폰 백신 개발 뿐만 아니라, 플랫폼차원, 하드웨어 차원, 서비스 차원 등 다양한 각도에서 스마트폰 생태계 전반에 걸친 안정성 제공을 위한 보안 기술 개발에 박차를 가하여야 할 것이다.

## 참고문헌

[1] W. Jansen and K. Scarfone, "Guidelines on Cell Phone and PDA Security", NIST, 2008.

[2] A. Schmidt and S. Albayrak, "Malicious Software for Smartphones", Tech. Rep., DAI-Labor, 2008.

[3] "스마트폰 악성코드 국내감염 첫 발견",

http://article.joins.com/article/article.asp?Total_ID=4127310

[4] K. Dunham, S. Abu-Nimeh, M. Becher, S. Fogie, B. Hernacki, J. A. Morales, and C. Wright, "Mobile Malware Attacks and Defense", Syngress, 2008.

[5] 김재중, "앱스토어 보안과 코드사인", 정보통신망 정보보호 워크샵(NETSEC-KR'10), pp.527-549, 2010.

[6] 홍동철, "스마트폰에서의 악성코드 대응방안", 정보통신망 정보보호 워크샵(NET SEC-KR'10), pp.550-562, 2010.

[7] Tim Kornau, "Return Oriented Programming for the ARM Architecture", Ruhr-University of Bochum, 2009.

[8] 김익수, 정진혁, 이형찬, 이정현, "모바일 악성코드 분석 방법과 대응방안", 한국통신학회논문지, 제 35권 제 4호, 2010.

[9] "스마트폰 개인정보 유출", http://news.kbs.co.kr/society/2010/02/01/2038943.html, KBS 뉴스9

[10] "스마트폰 해킹에 취약", http://imnews.imbc.com/replay/nwtoday/article/2556091_5782.html, MBC 뉴스데스크

[11] K. Scarfone and J. Padgette, "Guide to Bluetooth Security", NIST, 2008.

[12] "Policy and Guidance for the Use of BlackBerry by the Australian Government", Australian Government, 2006.

[13] Nicolas Economou and Alfredo Ortega, "Smartphone (in) Security", Core Security Technologies, 2009.

[14] Nicolas Seriot, "iPhone Privacy", Black Hat, 2010.

[15] Troy Vennon, "A Study of Known and Potential Malware Threats", SMobile Systems, 2010.

[16] Troy Vennon and Mayank Aggarwal, "Spyware in the Android Market", SMobile Systems, 2010.

[17] Daniel V. Hoffman, "A demonstration of current threats to mobile devices", Hacker Halted, 2009.

[18] Tim Hurman, "Exploring Widnows CE Shellcode", Pentest Limited, 2005

[19] "iPhone hacked, SMS database hijacked", http://www.zdnet.com/blog/security/pwn2own-2010-iphone-hacked-sms-database-hijacked/5836

[20] "스마트폰 악성코드 위협 고찰", http://teamcrak.tistory.com/270

## 저자약력

**이 형 찬**

2010년 2월 숭실대학교 컴퓨터학부 학사
2010년 3월~현재 숭실대학교 컴퓨터학과 석사과정
관심분야 : 모바일 시스템 보안, 모바일 서비스 보안
이 메 일 : lee.hyeongchan@ssu.ac.kr

**정 진 혁**

2004년 3월~현재 숭실대학교 컴퓨터학부 학사과정
관심분야 : 모바일 시스템 보안, 모바일 서비스 보안
이 메 일 : nemojjh@gmail.com

**김 선 휘**

2005년 3월~현재 숭실대학교 미디어학부 학사과정
관심분야 : 모바일 서비스 보안, 모바일 컨텐츠 보안
이 메 일 : ksungnl@paran.com

**이 정 현**

1993년 2월 숭실대학교 전자계산학과 학사
1995년 2월 숭실대학교 전자계산학과 석사
2005년 8월 University of California at Irvine, Computer Science 박사
1995년 2월~2001년 8월 한국전자통신연구원 연구원
2000년 4월~2001년 3월 미국 표준기술연구원(NIST) 객원연구원
2005년 10월~2008년 8월 삼성종합기술원 수석연구원
2008년 9월~현재 숭실대학교 컴퓨터학부 조교수
관심분야 : 모바일 보안, 네트워크 보안, 클라우드 보안
이 메 일 : jhyi@ssu.ac.kr