情 報 保 護 學 會 誌
第19卷 第5號, 2009. 10

개방형 모바일 환경에서 스마트폰 보안기술

김 기 영*, 강 동 호*

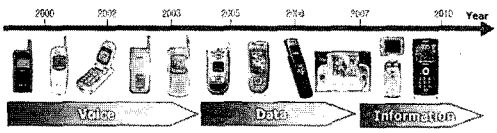
요 약

모바일 네트워크 고도화 및 단말기의 비약적인 발전으로 스마트폰 보급이 확산되고, 스마트폰 시장의 경쟁 본격화에 따른 개방형 플랫폼 증가와 애플리케이션 마켓플레이스의 활성화가 이뤄지고 있다. 개방형 모바일 환경에서는 표준화된 개발환경이 모든 개발자에게 공개되어 있어 누구나 애플리케이션의 제작 및 배포가 가능하기 때문에 질적으로나 양적으로 모바일 애플리케이션이 등장할 것으로 예상 된다. 하지만, 개방화된 개발환경의 등장과 더불어 범용 OS를 채택하고 있는 모바일 단말은 모바일 악성코드의 제작을 용이하게 만들고, 제작된 모바일 악성코드는 범용 OS로 인해 이식성이 높기 때문에 모바일 공격의 규모 및 피해가 증가할 것으로 예상된다. 본 논문에서는 개방형 모바일 환경에서 제공되는 스마트폰 기술 및 시장 전망, 모바일 위협의 종류 및 유형, 그리고 이러한 위협에 대응하기 위한 보안기술에 대하여 살펴보고자 한다.

1. 서 론

통신 속도 발전에 따라 휴대폰은 '88년 1세대 AMPS, '96년 2세대 CDMA, 그리고, '00년 2.5세대 CDMA 2000, '03년 3세대 W-CDMA, '06년 3.5세대 HSDPA가 시작되어 현재 4세대로 진화하고 있다. 이제 단순 통신 속도 발전 수준이 아니라 PC의 기능이 휴대폰과 같은 하나의 모바일기기에서 제공되어 주머니속의 인터넷 시대의 도래를 예측하고 있다. 지금까지 PC용 프로세서 개발에 주력해온 인텔이 2008년 스마트폰과 같은 모바일 디바이스용 프로세서로 아톰 프로세서를 출시하였고, 2009년 Acer와 ASUS와 같은 전형적인 PC 전용 프로세서 개발업체들이 단말시장에 참여하는 등 새로운 개념의 인터넷기기의 대중화시대를 알리는 시도들이 업체를 중심으로 진행되고 있다.

새로운 개념의 모바일 인터넷 환경의 변화와 사용자의 다양한 요구에 만족하기 위하여 All IP를 갖는 이동 단말이 출현하게 되었으며, 음성 중심의 단말이 데이터 중심으로 진화하고, 단순 데이터 중심의 단말이 고용량, 소형 및 저가격 저장장치, 풀 브라우저, 3D 그래픽을 강화한 멀티미디어 프로세서의 발전 및 아톰 프로세서와 같은 모바일 전용 CPU들의 제공으로 지능적인 정보 단말로 진화하게 되었다.



〔그림 1〕 스마트폰의 진화[1]

주니퍼 리서치 2009년 자료에 따르면 스마트폰 점유율이 지속적으로 증가하여 2013년까지 전체 모바일 시장의 23%를 점유할 것으로 예상하고 있다. 스마트폰의 다양한 인터페이스를 통하여 언제 어디서나 사용자가 원하는 모바일 서비스를 제공받게 되고, 그로 인하여 우리의 비즈니스 및 생활은 엄청난 기회를 갖게 되었다. 하지만, 이로 인하여 우리의 모바일 환경이 언제 어디서나 모바일 위협에 노출될 수 있다.

본고에서는 이러한 스마트폰 보안 위협의 급증에 따른 모바일 위협의 종류 및 유형 등을 분석하고, 대응을 위한 스마트폰 보안 동향을 살펴보고자 한다.

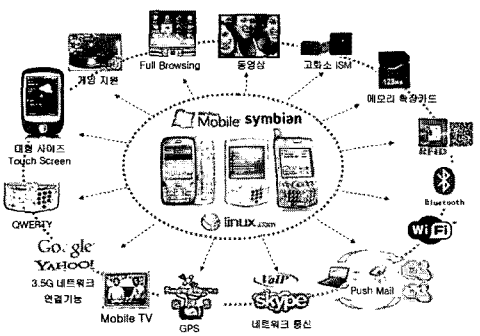
본 연구는 지식경제부/정보통신연구진흥원의 IT성장동력기술개발사업 연구개발 과제로 수행되었습니다.
* 한국전자통신연구원 인프라보호연구팀 ({kykim,dhkang}@etri.re.kr)

Ⅱ. 스마트폰 동향

2.1 스마트폰 개념 및 유형

최근 통신 인프라의 발전에 따른 휴대폰의 변화 및 사용자들의 다양한 요구에 의하여 스마트폰이 출현하게 되었으며, 이렇게 대두된 스마트폰의 다양한 인터페이스 및 기능이 하나의 모바일 기기에서 제공됨으로 인하여 모바일 컨버전스가 우리의 실생활에서 실현되게 되었다. 이러한 변화를 주도하는 스마트폰은 무엇이며, 통신 패러다임의 급격한 변화로 인한 모바일 환경 개방화와 오픈플랫폼 기반의 모바일 플랫폼의 등장으로 인하여 향후 어떠한 방향으로 발전할 것인지 살펴보도록 하자.

스마트폰은 일반폰보다 진보된 능력을 가진 PC와 유사한 기능의 모바일 단말로써 범용 운영체제가 탑재한 휴대폰으로 정의 할 수 있다. 주요 특징은 PDA 기능 및 Wi-Fi를 통한 무선 인터넷 서비스, QWERTY 자판 등을 탑재하고 있다.



〔그림 2〕 스마트폰의 기능[1]

스마트폰은 일반폰보다 뛰어난 CPU를 사용하여 멀티미디어 처리에 우수하다. 하지만 최근에는 일반폰의 사양이 스마트폰과 거의 차이가 없을 정도로 개선되어 이를 기준으로 스마트폰과 일반폰을 구분하기는 어렵다. 스마트폰을 일반폰과 구별 짓는 가장 큰 특성은 개방성이라 할 수 있다. 즉, 스마트폰은 범용 운영체제를 사용하고, 표준화된 개발 환경을 제공하여 개방화된 운영체제를 통해 개발자들이 자유롭게 애플리케이션을 개발할 수 있는 환경을 제공하고 있다. 따라서 일반 사용자들간에 개방형 운영체제를 기반으로 다양한 어플리케이션 의 공유가 가능하다. 스마트폰 사용자, 사업자, 제조사 측면에서 일반 휴대폰에 비해 다양한 이점을 제공하는데 이를 정리한 제조업체의 자료를 보면 다음과 같다[2].

〔표 1〕 스마트폰의 연관 플레이어별 장점 및 특징[2]

구분	특징
사용자	멀티태스킹, 멀티미디어, 통신 등 단말 기능 우수 다운로드 받아 사용할 수 있는 다양한 어플리케이션 및 서비스에 대한 요구 증가 타 단말과의 연동기능 우수
사업자	신규 서비스 런칭 기간 단축 사업자 테스트 위한 경비 절감 어플리케이션 다운로드 및 3'rd party 서비스 지원으로 ARPU 및 콘텐츠 사용료 증대(기출시 단말도 신규 서비스 제공.
제조사	플랫폼 사용으로 SW 재활용 극대화로 개발비 절감 3'rd party를 통한 어플리케이션 확보가 용이하고 다양한 어플리케이션 확보를 통한 단말 Value 증가 제조사 독자 서비스 적용 및 확산 용이

최근 스마트폰의 출현 및 활성화를 예측했던 CeBIT2008/MWC2008에서 "주머니속의 인터넷 시대" 및 "인터넷 머신의 해"를 키워드로 내세웠고, 이어 CES2009/MWC2009에서는 "휴대폰의 미래를 경험하라" 및 "Webciety" 등으로 이러한 변화의 시대를 이끌어낸 스마트폰의 개발자 및 대표기능이 확산되고 있음을 강조하고 있다. 특히 단말 제조업에 대한 진입 장벽이 낮아져 Acer 및 Asus와 같은 기존 PC 제조업체들이 모바일 기기개발에 참여함을 볼 수 있다.

전세계 스마트폰의 판매량을 살펴보면 2009년 2분기에 전년 동기 3,227만대보다 27% 증가한 4,096만대가

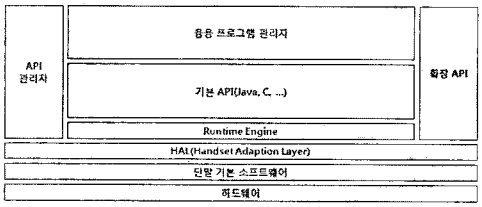
〔표 2〕 2009년 2분기 전세계 스마트폰 판매현황 (천대)[9]

Worldwide Smartphone Sales to End Users In 2Q 2009(Thousands of Units)				
Company	2Q09 Sales	2Q09 Market Share	2Q08 Sales	2Q08 Market Share
Nokia	18,441	45.0	15,297.9	47.4
Research in Motion	7,678.9	18.7	5,594.2	17.3
Apple	5,434.7	13.3	892.5	2.8
HTC	2,471.0	6.0	1,330.8	4.1
Fujitsu	1,249.0	3.0	1,071.5	3.3
Others	5,688.2	13.9	8,085.8	25.1
Total	40,962.8	100.0	32,272.7	100.0

판매되었으며 판매 순위는 1위는 노키아, 2위는 RIM사의 블래베리, 3위는 애플이 차지하고 있다.

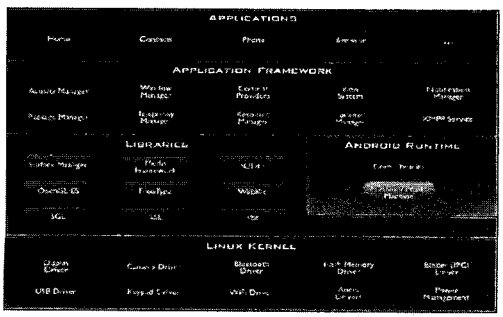
2.2 모바일 운영체제 및 단말의 발전방향

모바일 운영체제는 RTOS(Real Time OS)와 GPOS (General Purpose OS)로 구분할 수 있다.일반적으로 RTOS는 REX와 같이 음성위주 단말의 전용 운영체제로 분류하고 GPOS는 스마트폰과 같은 단말에 탑재되는 범용 운영체제 분류하고 있다. RTOS를 탑재한 모바일 단말은 다양한 미들웨어를 제공하고 있는데 대표적인 것으로 Java VM, BREW, WIPI, Mocha, infineon 등이 있다. 아래는 WIPI의 개념적 구조를 보이고 있다.



〔그림 3〕 WIPI 구조

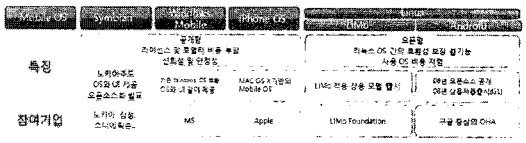
단말 기본 소프트웨어는 음성통화를 위한 통신기능 및 운영체제가 들어 있다. CDMA에서는 REX, GSM에서는 Nucleus, Kadak 등을 기본 운영체제로 사용하고 있다. 모바일 애플리케이션의 기능적 다양성과 함께 하드웨어의 성능 향상으로 인해 모바일 환경에서 다양한 멀티미디어 처리를 하기에는 RTOS가 한계에 이르게 됐다. 따라서 모바일 운영체제가 PC급의 운영체제 구조를 유지하면서 모바일에 최적화 하는 방향으로 전개되어 스마트폰의 등장이 이뤄졌다. 다음 [그림 4]는 구글



〔그림 4〕 구글 안드로이드 구조

의 안드로이드 플랫폼의 구조를 보이고 있다.

모바일 단말이 일반폰에서 스마트폰으로 발전되어감에 따라 모바일 플랫폼의 개발이 가속화되어 MS는 윈도우즈 모바일, 애플은 아이폰, 구글은 안드로이드 플랫폼을 상용화하여 모바일 단말에 적용하고 있다. 이들은 기본적으로 멀티태스킹을 지원하기 때문에 기존의 일반폰 보다 성능적으로 우수하고, 개방형 환경에 따라 자체적으로 애플리케이션을 개발하는 폐쇄형 구조에서 모든 개발자에게 표준화된 개발환경을 제공하는 공개형 구조로 발전하고 있다. [그림 5]는 공개형과 오픈형의 특징에 따른 분류, 대표적인 참여기업을 제시하고 있다.



〔그림 5〕 개방 및 오픈형 모바일 플랫폼의 종류 및 특징[13]

특히, 애플이나 구글 같은 모바일 플랫폼 제공업체들은 자사 모바일 운영체제를 기반으로 오픈 마켓을 통해 많은 애플리케이션의 개발 및 사용을 유도하고, 더 많은 사용자들로 인해 더 많은 애플리케이션 개발이 유도되는 선순환 구조 구축에 주력하고 있다.

2.3 스마트폰용 애플리케이션 보안관리 동향

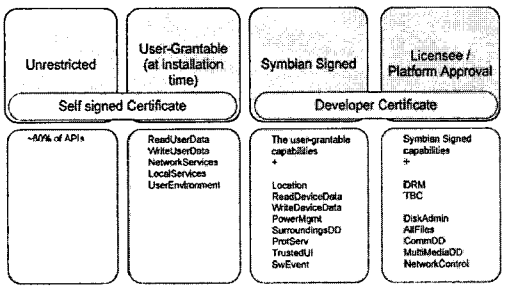
개방형 모바일 단말은 누구나 컨텐츠를 제작하거나 배포가 가능하기 때문에 다양한 컨텐츠 생성이 가능하다. 이는 장점이 될 수 있지만 악성코드가 포함된 애플리케이션의 제작 및 유포가 가능하기 때문에 모바일 환경에서의 보안위협은 증가할 것으로 예상된다. 개방형 모바일 환경에서 모바일 단말의 안전한 사용을 위해 제작된 애플리케이션의 보안적 측면을 단말내부에서 어떠한 처리하는지 심비안, 윈도우즈 모바일, 그리고 안드로이드를 중심으로 살펴보고자 한다.

2.3.1 노키아의 심비안[8]

심비안 OS v9는 애플리케이션이 모바일 단말에 존재하는 주요 데이터와 시스템 자원을 사용하기 위해 호출하는 API의 비정상적 접근을 제어하기 위해 플랫폼 보안(Platform Security)을 제공하고 있다. 플랫폼 보안

은 다음과 같은 3가지 주요 기능을 제공한다.

- Capability: 단말에서 실행중인 프로세스가 사용하는 네트워크, PIM, 그리고 카메라등과 같은 시스템 자원에 대한 접근 허용 리스트의 집합을 의미한다. 모든 개발 코드는 실행코드를 만들 때 Capability를 하고, 단말에 설치 시 Capability를 확인하는 과정을 거친다. 단말은 프로세스에게 자신에게 할당된 시스템 자원만을 허용한다. 서드 파트 애플리케이션은 기본적인 Capability만을 제공받는다.



〔그림 6〕 Capability 그룹

- 시큐어 소프트웨어 인스톨러: 전자 서명된 애플리케이션만 단말에 설치를 허용하고, Capability의 포함여부를 확인한다. Capability는 설치된 후 변경할 수 없기 때문에 애플리케이션은 할당된 시스템 자원만을 이용하고 다른 자원에 대한 접근은 허용하지 않는다. 따라서, 모바일 악성코드가 포함된 애플리케이션도 악성코드의 전파 및 단말에 위협을 가하기 위한 Capability를 가지고 있지 않으면 특정 시스템 자원을 이용할 수 없다.
- 데이터 케이징(Data Caging): 프로세스는 기본적으로 자신의 메모리 영역만 접근이 가능하고 다른 프로세스의 메모리 영역에 대한 접근만을 허용하지 않도록 제공한다.

2.3.2 MS의 윈도우즈 모바일

윈도우즈 모바일 6 의 보안 모델은 퍼미션 정책에 따라 애플리케이션의 접근권한이 결정된다. 윈도우즈 모바일 6 단말에 애플리케이션을 탑재하고자 하는 개발자들은 반드시 MS가 규정한 코드 인증을 거쳐야 한다. 애플리케이션의 퍼미션은 다음과 같이 Privileged, Normal, Block으로 나누어진다.

- Privileged: 시스템 자원에 접근하기 위한 모든 API 호출이 가능하고 레지스트리의 모든 영역에 대한 쓰기 및 모든 파일에 대한 접근권한을 가지는 "Trusted" 퍼미션
- Normal: 일부 API는 호출이 불가능하고, Protected 영역의 레지스트리나 파일에 대한 쓰기는 불가능한 "Untrusted" 퍼미션
- Blocked: 애플리케이션의 실행이 불가능한 "Locked" 퍼미션

코드 사이닝 때 인증서의 레벨에 따라 퍼미션이 결정된다.

2.3.3 구글의 안드로이드

안드로이드는 리눅스기반의 OS로써 리눅스의 보안 정책과 유사한 부분이 많다. 애플리케이션은 단말에 설치될 때 고유의 USER ID와 GROUP ID를 부여받는다. 사용자 ID를 할당받은 애플리케이션이 만든 파일은 기본적으로 사용자 ID가 다른 애플리케이션이 읽거나 쓸 수 없다. 애플리케이션이 사용하고자 하는 시스템 자원이 있다면 필요로 하는 퍼미션 선언을 위해 애플리케이션 개발단계에서 AndroidManifest. xml파일의 <uses-permission> 태그에 사용하고자 하는 시스템 자원을 입력해야 한다. 입력하지 않고 설치된 애플리케이션은 단말이 시스템 자원의 사용을 제한한다. 모든 안드로이드 애플리케이션은 개발자의 인증서를 이용하여 자신의 비밀키로 사이닝을 해야 한다.인증서는 애플리케이션 개발자의 신원 증명을 위해서만 사용되며 신뢰할 수 있는 인증국에 의해 발급된 것일 필요는 없고 자기 서명 인증서도 사용이 가능하다. 따라서 위에서 살펴본 심비안과 윈도우즈 모바일 보다는 보안 정책이 높지 않고, OS의 소스코드가 공개되었기 때문에 보안적 측면에서는 다른 상용 모바일 OS보다 취약할 것으로 예상된다.

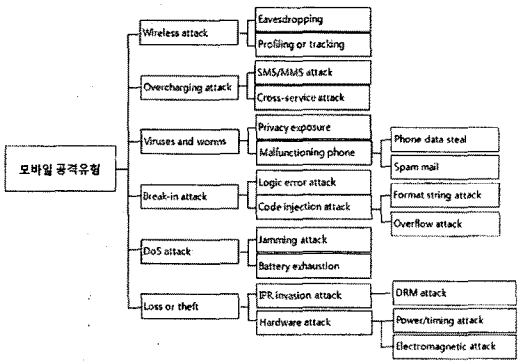
Ⅲ. 스마트폰 보안 위협 및 모바일 악성코드 동향

3.1 스마트폰 보안 위협

모바일 단말의 다양한 보안 위협에 대응하기 위해 모바일 보안 기술이 계속적으로 등장하고 있지만 단말기의 발전과 더불어 네트워킹 서비스의 활성화에 따라 모바일 악성코드로 인한 스마트폰의 보안 위협은 계속적으로 증

가하고 있다. 스마트폰의 확산과 더불어 스마트폰의 보안 위협에는 어떠한 유형들이 있는지 살펴보고자 한다.

[그림 7]은 모바일 환경에서 스마트폰과 같은 단말에 가해질 수 있는 다양한 공격들과 이들을 다시 공격방법 및 목표에 의해 공격의 유형을 분류하고 있다.



〔그림 7〕 모바일 공격 유형 분류

스마트폰을 공격하는 공격도구는 침해방법 과 목적이 다양하기 때문에 단순히 하나의 공격 유형으로 정의할 수 없지만 주요위협을 기반으로 분류하였다. 이러한 공격 유형은 대체적으로 단말의 기능을 마비시키거나 정보 유출 및 금전적 이득을 목적으로 이뤄지고 있다. 현재까지 국내에서 발생한 스마트폰의 보안 위협은 미비한 수준이다[10]. 스마트폰이 아직 국내에서 대중화 단계까지 성장하지 못했고, WIPI 장벽이 그 원인이라고 할 수 있다. 하지만, WIPI의 해제와 아이폰의 국내 시장진출은 모바일 환경에서의 개방화를 가속 시키는 역할을 할 것으로 예상되며 이에 따라 국내에서도 모바일 악성코드로 인한 피해가 현실화 될 것으로 예상된다.

3.2 모바일 악성코드

모바일 악성코드는 모바일 단말의 성장과 더불어 규모면에서 빠르게 증가하고 있고, 위협요인도 다양화되고 있다. 모바일 악성코드가 증가하는 원인은 악의적인 목적을 가진 악성코드의 제작 및 유통이 가능한 개방형 단말기의 증가와 함께 W-CDMA, CDMA-2000등의 셀루러 통신 방법을 기본으로 제공하면서 블루투스, Wi-Fi와 USB등 외부 접속의 다양화가 원인이라고 할 수 있다. 모바일 악성코드는 초기에 단순히 전파를 목적으로 하거나 단말의 기능적 동작을 마비시키는 형태에서 개인정보의 유출 및 금전적 이득을 목적으로 하는 형태로 변화되고 있다.

지금까지 존재한 모바일 악성코드의 주요 활동별 특성을 반영하여 분류하면 5가지 형태로 구분할 수 있다.

3.2.1 단말 장애 유발형 악성코드

단말의 사용을 불가능하게 만들거나 장애를 유발하는 공격 유형이다. 2004년에 발견된 Skulls가 단말의 기능을 마비시키는 단말 기능 마비형 악성코드 유형이다. 모든 메뉴 아이콘을 해골로 변경시키고 통화이외의 부가기능을 사용할 수 없게 만든다. 2005년에 발견된 Locknut는 단말의 일부 키 버튼을 고장 내는 특성을 가지고 있다. 이외에도 전화의 송수신을 기능을 마비시키는 Gavno가 등장하였다.

3.2.2 배터리 소모형 악성코드

단말의 전력을 지속적으로 소모시켜 배터리를 고갈시키는 공격 유형이다. 2004년에 블루투스를 통해 전파되는 최초의 모바일 악성코드인 Cabir가 대표적이다. Cabir는 단말의 침해를 유발하지 않는 대신 지속적으로 인근 단말의 블루투스를 스캐닝하고, 블루투스를 통해 악성코드를 전파하는 특징을 가지고 있다. 감염된 단말은 지속적인 스캐닝을 통해 배터리의 고갈 피해를 입게 된다.

3.2.3 과금 유발형 악성코드

단말의 메시징 서비스 나 전화 시도를 지속적으로 시도하여 과금을 발생시키는 공격 유형이다. 2006년 러시아에서 제작된 J2ME 플랫폼용 RedBrowser가 대표적인 사례로써 감염된 단말은 사용자도 모르게 불특정 다수에게 SMS를 전송시켜 사용자에게 금전적 피해를 입히는 악성코드이다. 또한 중국에서 2008년에 발견된 Kiazha 악성코드는 감염된 단말 화면에 사용자에게 돈을 요구하는 경고 메시지와 함께 단말에 저장된 문자메시지를 삭제하는 악성코드가 등장했다.

3.2.4 정보유출형 악성코드

감염된 단말의 정보나 사용자 정보를 외부로 유출시키는 공격 유형이다. 2008년 발견된 Infojack은 합법적

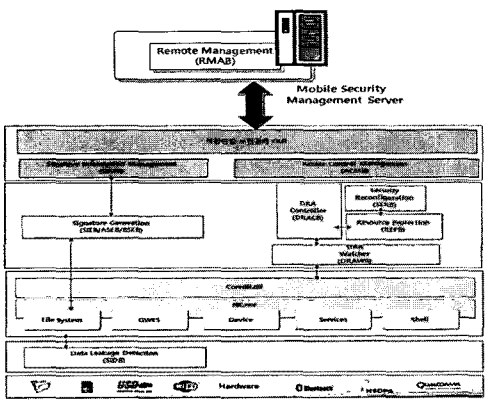
인 애플리케이션이 단말에 다운로드 될 때 .cab 설치파일과 함께 포함되어 설치되고, 설치된 후, 특정 웹서버에 접속하여 Infojack의 나머지 부분을 다운로드하여 재 설치한다. 설치가 완료되면 단말의 보안 설정을 변경하고 단말의 시리얼 번호, OS, 설치된 애플리케이션 등 단말의 정보를 외부로 전송하여 2차 공격을 용이하게 한다. 사용자의 정보를 외부로 유출시키는 악성코드로는 Flexispy, PBStealer가 있다. Flexispy는 스파이웨어형태의 상용 악성코드로써 스마트폰의 전화기록, 문자메시지 내용을 특정 웹서버로 전송하는 기능을 가지고 있다.

3.2.5 크로스 플랫폼형 악성코드

모바일 단말을 통해 PC를 감염시키는 공격 유형이다. 2005년에 발생된 Cardtrap.A가 최초의 크로스 플랫폼형 악성코드로써 폰의 메모리 카드에 윈도우 웜을 복사하여, 감염된 폰 메모리 카드를 PC에 장착했을 때 autorun를 통해 PC를 자동으로 감염시켜 데이터를 삭제하거나 성능을 저하시키게 만든다. 모바일 기기간의 확산이 아닌 모바일 기기에서 PC를 감염시킨다는 점에서 새로운 형태의 공격 유형을 가지고 있다.

Ⅳ. 복합단말용(스마트폰) 침해방지기술

복합단말용 침해방지기술은 '07년부터 ETRI에서 개발하고 있는 보안기술로써 스마트폰과 같은 복합단말에 대한 침해시도를 사전에 탐지, 차단하고 저장된 민감 데이터의 보호를 목적으로 한다. [그림 8]은 현재 개발이 진행 중인 Windows Mobile용 침해방지 기술의 구조도를 보이고 있다.

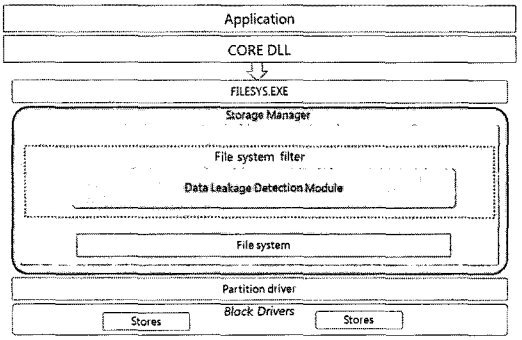


〔그림 8〕 복합단말 침해방지 기술

복합단말용 침해방지기술은 민감정보 유출방지 기술, 모바일 접근제어 기술, 원격 모바일 관리 기술, 그리고 모바일 보안 서비스 재구성 기술로 나뉜다.

4.1 민감정보 유출 방지 기술

민감정보 유출방지 기술은 단말 내부 파일들로부터 민감정보가 포함된 파일을 분류 및 선정하여 외부 유출 시도 시 탐지 및 차단을 위한 시그니쳐 생성한다. 시그니쳐를 기반으로 파일 시스템 필터를 이용하여 파일의 Open, Read, Write, 그리고 Modify 등 파일에 관련된 모든 동작을 체크하여 민감정보 유출을 사전에 방지하는 기능을 담당한다.

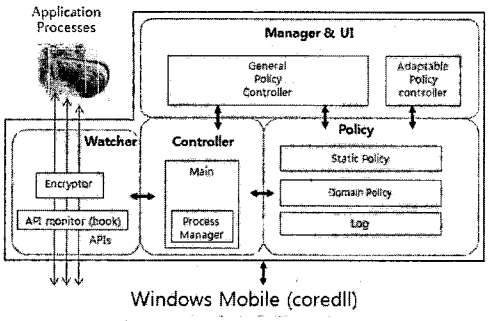


〔그림 9〕 민감정보 유출 방지 기술

민감정보로 지정된 파일이 변조되거나 다른 파일 이름으로 생성되었을 경우도 이를 확인하여 민감정보 파일로 지정하고 지정된 파일에 대한 탐지 정책을 생성한다.

4.2 모바일 접근제어 기술

모바일 접근제어 기술은 사용자의 데이터를 안전하게 보호하고, 외부로부터 침해를 방지하는 기능을 제공한다. 이를 위해서 단말의 애플리케이션들이 시스템 API를 통하여 시스템 자원에 접근하는 것을 모니터링한다. 기존 접근제어 기술과의 차이는 모바일 환경의 특성상 기존의 대형시스템용 접근제어 기술에 비하여 사용자가 미리 지정해야 하는 정책의 양을 최소화하였고, 사용자 대상의 접근제어가 아닌 애플리케이션과 데이터를 대상으로 접근제어 기능을 제공하고 있다.



〔그림 10〕 모바일 접근제어 기술

모바일 접근제어 관리기술은 다음 3가지 모듈을 제공하고 있다.

- Watcher : Coredll의 관련 API를 후킹하여 단말자원의 접근 감시 및 제어기능을 담당한다. 모든 프로세스들이 단말의 정보 자원과 인터페이스에 접근할 때마다 Controller 에게 보고하고, Controller의 정책에 따라서 단말자원접근을 허용 또는 불허한다. 또한 Controller의 제어에 따라 특정 파일에 대해서는 암복호화 기능을 수행한다.
- Controller : Watcher로부터 수집한 정보와 Policy에 구축된 정책을 바탕으로 모든 제어 결정을 수행한다. 또한 처리결과에 대한 리포팅, 모니터링 및 로깅 기능도 담당한다.
- Manager & UI : 주로 사용자 인터페이스 기능을 담당하여 Controller로부터 입출력되는 정보를 사용자와 인터페이스 할 수 있는 기능을 제공한다.

4.3 원격 모바일 보안 관리 기술

원격 모바일 보안관리 기술은 모바일 단말의 보안정책 적용, 단말의 분실 및 도난 시 단말내부의 중요 정보 삭제 기능을 담당한다. 모바일 단말과 원격 모바일 보안관리 서버는 OMA DM 프로토콜을 통해 통신하며 OMA DM 규격은 서버와 단말간의 통신 프로토콜, 단말 관리 객체 정의, 단말 관리 메시지의 보안 방법 등의 단말 관리에 대한 기본 규격과 그 외의 단말 관리 서비스를 위한 부가 규격으로 구성된다.

4.4 모바일 보안서비스 재구성 기술

모바일 보안서비스 재구성 기술은 단말의 환경변화 즉, 복합단말이 접속한 네트워크의 보안상태, 배터리 상태 등 보안 상황 정보를 수집하여 현재의 보안상황에 가장 최적화된 보안 서비스를 자동으로 구성하는 기능을 담당한다. 보안 상황정보은 모바일 단말의 용도(예, 게임용, 비즈니스용 등), 위치한 장소 (예, 회사, 집, 음식점), 접속한 네트워크에 설치된 보안기능(예, IDS, Firewall 등), 그리고 모바일 단말의 배터리 상태 등의 정보를 의미한다. 보안 상황정보는 사용자의 입력에 따른 정적 구성과 단말에서 시스템 자원정보를 통해 얻거나 원격 모바일 보안 관리 서버에서 전달받아 적용하는 동적 구성으로 이뤄져 있다. 이러한 재구성 기술을 통해 단말의 보안수준을 유지하면서 단말 자원 효율성과 사용자의 편의성을 제공하게 된다.

V. 결 론

지금까지 스마트폰 기술, 모바일 플랫폼 동향 및 위협, 그리고 시장성장과 함께 요구되는 스마트폰의 보안 위협 및 대응방안에 대하여 살펴보았다. 또한, ETRI에서 개발 중인 복합단말용 침해방지 및 민감정보 유출방지 기술에 대해서 살펴보았다.

국내는 현재 개방형 모바일 환경의 변화 및 개방형 플랫폼 도입으로 스마트폰 기술 및 시장에 많은 변화가 이루어지고 있다. 더불어 '09년 4월에 지금까지 국내 휴대폰 시장의 보호 역할을 해주고, 외산 스마트폰의 진출의 차단막이었던 WIPI 의무화가 폐지되어 다양한 개방형 모바일 단말이 국내에 진출하거나 진출이 예상되고 있다. 개방형 모바일 단말은 누구나 컨텐츠를 제작하거나 배포가 가능하기 때문에 다양한 컨텐츠 생성이 가능하다는 장점이 있지만 일부 악의적인 개발자가 이를 이용해 악의적인 프로그램을 제작 및 유포해서 단말에 침해를 가하거나 개인정보를 습득할 수 있는 가능성도 높아졌다.

따라서 외국에서의 사례처럼 국내에도 모바일 악성코드 뿐 아니라 모바일 취약점, 오픈마켓과 같은 새로운 비즈니스 모델을 기반으로 전파되는 모바일 위협에 따른 철저한 대비가 필요하다. 자칫 모바일 보안위협 등을 무시하고, 오픈마켓의 성장 및 스마트폰의 가시적인 성장에만 치중하게 된다면 현재 근본적으로 해결가능 할 수 있는 많은 기술적.정책적 접근 부분을 추후 엄청난 노력으로 대비하게 될 것임을 명심해야한다. 개방형 모바일 보안기술분야는 향후 전개될 건전하고 안전한 모

바일 생태계구축을 위하여 지속적으로 대비하고 발전시켜야할 기술이다 .

참고문헌

[1] KIEI, "휴대폰(스마트포) 및 부품/소재 기술.시장 분석 세미나", 2009년 3월 10일~12일.

[2] 와이즈인포, "스마트폰 시장/기술 및 연관산업 동향 리포트", 2009년 3월.

[3] 배근태, 김기영, "모바일 단말 보안 운영체제 기술 동향", 전자통신동향분석 제23권 제4호, 2008.

[4] Mikko Hypponen, "Malware goes Mobile", Technical Report, Scientifical American, INC, 2006.

[5] C. Mulliner, "Security of Smart Phones," Master's Thesis, Department of Computer Science, University of California Santa Barbara, CA, June 2006.

[6] 유지은, "스마트폰의 Key Enabler: 소프트웨어", SW Insight 2009년 4월.

[7] Ken Dunham, "Mobile Malware attacks and Defense", SYNGRESS 2009.

[8] Ben Morris, "Platform Security and Symbian Signed: Foundation for a Secure Platform", Symbian Developer Network Report, Jan 2008

[9] Gartner, "Worldwide Smartphone Sales to End Users in 2Q2009", AUG 2009.

[10] http://kr.ahnlab.com/info/security info/.

[11] http://www.f-secure.com/.

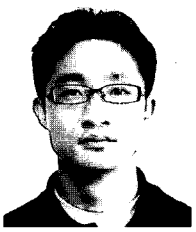
[12] http://www.android.com/.

[13] http://www.kandroid.org/.

〈著者紹介〉

김 기 영 (Kiyoung Kim)
정회원

1988년 2월: 전남대학교 전산통계학과 졸업
1993년 2월: 전남대학교 전산통계학과 석사
2002년 2월: 충북대학교 전자계산학과 박사
1988년 2월~현재: 한국전자통신연구원 인프라보호연구팀 책임연구원
<관심분야> 네트워크보안, 임베디드 보안 OS 및 복합단말용 보안기술 등



강 동 호 (DongHo Kang)

1999년 2월: 한남대학교 컴퓨터공학과 졸업
2001년 2월: 한남대학교 컴퓨터공학과 석사
2001년 2월~현재: 한국전자통신연구원 인프라보호연구팀 선임연구원
<관심분야> 네트워크보안, 임베디드 보안 OS 등