디지털산업정보학회 논문지 제6권 제2호-2010년 6월

스마트폰 보안 기술 분석*

이 영 숙** · 김 지 연***

The Study on the security of Smartphone

Lee, Young Sook · Kim, Jee Yeon

〈Abstract〉

With the release Apple's iPhone, smartphone is enjoying a tremendous popularity. Security experts pointed the smartphone security risks and KCC(Korea Communications Commission) published safety rules for smartphone users. In this paper we surveyed market and product trends of smartphone and analyzed the security technology of smartphoen OS including Symbian, iPhone OS, Windows Mobile and Android.

Key Words : Smartphone, Smartphone OS, Security of Smartphone

Ⅰ. 서론

애플의 아이폰이 국내에 출시되면서 스마트폰에 대한 관심은 폭발적으로 대두되고 있다. 이에 따라 국내외 보안 전문가들이 스마트폰에 대한 해커의 공격을 경고하였고 방송통신위원회는 스마트폰 사용자들을 위한 해킹 방지 대책을 발표하는 등 스마트폰에 대한 보안 관심도 증대하고 있다. 본 논문에서 요즘 핫 아이템인 스마트폰에 대한 전반적인 시장 동향과 보안 제품 동향 그리고 주요 스마트폰 OS인 심비안 OS와 윈도우즈 모바일과 구글의 안드로이드와 아이폰 OS의 보안 기술을 분석하도록 한다.

* 이 논문은 2010년 호원대학교 연구비 지원을 받은 것임 .
** 호원대학교 사이버수사 경찰학부 전임강사(제1저자)
*** 성균관대학교 전기전자및컴퓨터공학부 박사(교신저자)

Ⅱ. 스마트폰 개요

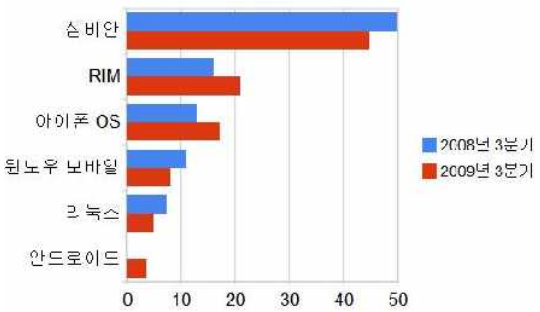
2.1 스마트폰의 정의

스마트폰(smartphone)은 PC와 같은 기능과 더불어 고급 기능을 제공하는 휴대전화이다[1]. 스마트폰의 산업 표준에 대한 정의는 없다. 어떤 사람들에게 스마트폰은 응용 프로그램 개발자를 위한 표준화된 인터페이스와 플랫폼을 제공하는 완전한 운영 체제 소프트웨어를 실행하는 전화로 볼 수도 있겠고 어떤 사람들에게 스마트폰은 전자 우편, 인터넷, 전자책 읽기 기능, 내장형 키보드나 외장 USB 키보드, VGA 단자를 갖춘 고급 기능이 있는 전화로 비칠 수 있다. 다시 말해 스마트폰은 전화 기능이 있는 소형 컴퓨터라 볼 수 있다.

고급 휴대 기기들의 수요가 늘면서 강력한 프로세서, 풍부한 메모리, 큰 화면, 개방형 운영 체제를 많이 쓰게

되자 여러 해 동안 휴대 전화 시장을 빠르게 채우고 있다.

2.2 스마트폰의 특징



<그림 1> 스마트폰 OS 시장 점유율(가트너)

GSM(Global System for Mobile Communications)과 GPRS(General Packet Radio Service) 네트워크 상의 음성 통신 외에도 스마트폰은 웹 브라우징, 이메일과 오거나이저 기능 및 고해상도의 칼라 스크린과 디지털 카메라, mp3 플레이어와 같은 개선된 멀티미디어 기능과 자바 어플리케이션을 제공한다.

또한 스마트폰에서 사용자는 블루투스, IrDA 또는 GPRS 상에서 SyncML, HotSync, Active Sync 또는 IntelliSync와 같은 프로토콜을 이용하여 PIM(Personal Information Management) 데이터(캘린더, 연락처, 업무 정리)와 이메일을 동기화할 수 있다. 스마트폰은 자원을 최적화하도록 설계된 완전한 전용 운영체제를 탑재한다.

Ⅲ. 시장 동향

3.1 세계 동향

시장조사업체 SA(Strategy Analytics)가 최근 발표한 보고서에 따르면, 2009년 4분기 전 세계 스마트폰 출하대수는 전년대비 30% 성장한 5300만대로 이에 힘입어 2009년 연간 규모는 1억 7380만대로 확대됐다. 전년 판매대수는 1억 5110만대였다.

업체별로는 노키아가 2,080만대(점유율 39.20%)로 여전히 1위를 가져갔다. 연중 기준으로도 노키아는 39% 점유율을 보였다. 노키아는 지난 2008년 1분기 이후 스마트폰에서 강한 입지를 다지고 있다고 SA는 설명했다. 다음 블랙베리 제조업체인 RIM(1,070만대, 20.20%), 아이폰으로 유명한 애플 1,280만대(16.40%) 순이었다[2].

2009년 12월 30일, 월스트리트저널(WSJ)이 가트너의 자료를 인용해 보도한 자료에 따르면 스마트폰 OS 시장에서 마이크로소프트의 윈도우 폰(구 윈도우 모바일)의 시장 점유율은 3분기를 기준으로 지난해 11.1%에서 올해 7.9%로 한 자리수로 떨어졌다[3].

블랙베리의 리서치 인 모션(RIM)과 애플은 각각 4.9%와 4.2% 상승로 상승해 20.8%와 17.1%를 기록했다. 노키아의 심비안은 시장 점유율이 하락했으나 여전히 1위를 지키고 있다. 그러나 MS의 경우는 시장 점유율 첫 한자리 수를 기록했다. 반면 구글의 안드로이드는 3.5%의 점유율을 기록했으나 안드로이드를 탑재한 모토롤라의 드로이드가 미국시장에서 선전하고 있는 만큼, 4분기 안드로이드의 점유율은 한층 높아질 것으로 예상된다.

시장 조사 기관인 ABI 리서치에 따르면 스마트폰 보안 시장은 5년 내에 급속하게 성장할 것이라고 한다[4]. ABI 리서치는 개선된 바이러스 보호 및 보안 소프트웨어를 탑재한 수많은 스마트폰이 2014년까지 5배로 급등할 것이라고 예측하였다. 2009년만 모바일 보안 솔루션으로 창출된 이익이 약 40%정도 증가했다.

3.2 국내 동향

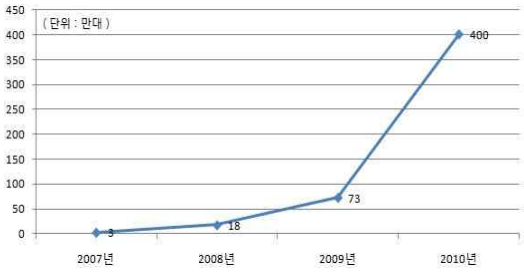
비즈니스 컨설팅 기관인 이노사이트그룹은 "The Future of Smartphone in Korea"라는 보고서를 통해 내년 스마트폰 이용자 수가 174만 명이 될 것으로 내다봤다. 이노사이트그룹은 올해 말 기준 스마트폰 이용자가

73만 명으로 점유율이 1.5%에 불과하지만, 내년에는 이용자 수와 점유율 모두 두 배 이상 급증해 174만 명에 3.7% 점유율을 전망하고 있다[5]. 보고서에서는 내년을 기점으로 스마트폰은 높은 성장률로 시장을 확대해 나갈 것이고 2013년 687만 명까지 증가하며 급성장세를 보이다가 휴대폰 시장 점유율 15%를 넘어서면서 정체를 보이며 상승세가 다소 둔화되는 양상을 보일 것이라고 예상했다.

2010년 국내 단말 출시는 총 30종으로 예정되어 있으며 13종밖에 되지 않았던 2009년에 비하면 2.3배나 증가할 것으로 보인다. 이통사별로는 SKT 15종, KT 10종, LGT 5종이다[6].

아이폰과 옴니아2의 경쟁 구도로 시작된 국내 스마트폰은 이렇게 다양한 단말이 출시되면서 본격적인 개화기를 만들어 낼 것으로 보인다. 하반기에는 본격적인 안드로이드 폰들이 출시될 것으로 보이며, 1Q에는 SKT의 모토로이와 LG전자의 210시리즈가 가세하면서 시장의 활기를 불어넣어 줄 것으로 기대된다[7].

로아그룹이 조사한 전문가 설문에 의하면 2010년 국내 스마트폰 판매량이 400만대에 이를 것으로 전망하고 있다. 아직까지 소비자의 요구(Needs)에 의하기 보다는 기술과 시장이 환경적 요인에 의해서지만, 다양한 서비스들과 스마트폰에 맞는 BM에 대해 시도가 많은 만큼 전체 시장이 풍성해질 수 있기를 기대하고 있다[8].



<그림 2>국내 스마트폰 판매량 추이(국내 이통 3사)

Ⅳ. 스마트폰 보안 이슈

스마트폰은 내재적인 특징 또는 사용(또는 악용) 또는 사용되는 기술로 인해 위험이 발생된다.

4.1 스마트폰의 내재적 특징과 관련된 위험

스마트폰은 전용 운영 체제를 갖는다. 이로 인해 보안 홀과 버그 출현과 같은 새로운 위험이 존재한다. 그 위험 원인은 주로 운영 체제의 복잡한 구조이다. 예를 들어 노키아 6600 내의 자바 MIDP 2.0 구현 내의 알려진 이슈가 문서화되어 있다[9]. 윈도우즈 기반의 스마트폰의 버그에 대한 사항도 있다[10]. 이러한 버그를 이용하여 장치를 고장나게 하고 리셋을 유발하도록 하는 것이 가능하다. 또한 이것은 장치 내에 저장된 데이터를 지우기도 한다.

<표 1> 스마트폰 사양 비교

구분	아이폰	옴니아	모토로이	LG 210 시리즈
통신사	KT	3사 모두 가능	SK 텔레콤	3사 모두 가능
DMB	X	O	O	O
두께	12.3㎜	12.3㎜	10.9㎜	12.9㎜
무게	135g	135g	140g	121g
카메라	320만 화소	500만 화소	820만 화소	500만 화소
디스플레이	3.5인치 LCD	3.7인치 AMOLED	3.7인치 LCD	3.0인치 LCD
운영체제	맥 OS X	윈도모바일 6.1 (오즈 옴니아는 6.5)	구글 안드로이드 2.0	윈도모바일 6.5
오픈마켓	앱스토어(11만종)	윈도마켓플레이스(800종)	안드로이드마켓(1만8000종)	윈도마켓플레이스(800종)

시스템 기반의 취약성은 컴퓨터에서와 마찬가지로 스마트폰에도 적용된다.

스마트폰의 내재적 특성과 관계된 또 다른 이슈는 접근 통제와 데이터 보안과 관련된다.

장치 내에 데이터를 보호하기 위한 암호화가 존재하지 않으면 정보는 그 장치에 물리적으로 접근할 수 있는 누구에게나 노출된다. PIN 코드 외에 개인 정보 및 비밀 정보를 저장하는 데 종종 이용되는 스마트에 대한 인증 수단이 존재하지 않는다. 이러한 위험은 스마트폰 제조자와 사용자가 고려해야 할 사항이다.

비록 PIN 코드가 전화 기능에의 접근을 보호하고 있다고 해도 때때로 데이터는 보호되지 않은 채 있게 된다. 게다가 대부분의 장치에서 데이터는 플래시 칩세트 또는 삭제 가능한 메모리 카드에 저장됨으로 칩세트에의 물리적 접근을 갖는 사람은 누구나 접근 통제를 우회하여 데이터를 훔칠 수 있다.

4.2 사용자와 관련된 위험

Pointsec Mobile Technologies에 의해 수행된 모바일 사용에 대한 조사에 따르면 장치의 75% 이상을 개인 이름과 주소, 비즈니스 대상 이름과 주소, 비즈니스 다이어리에 사용을 한다. 이러한 조사 결과는 사용자가 위험을 인식하지 못하고 자신이 장치에 비밀 정보를 저장하고 있음을 보여준다.

장치에 저장된 데이터는 불법적인 연결 또는 장치의 분실 또는 도난에 의해 쉽게 제3자에게 접근가능하게 되고 이로 인해 아이덴터티 도용에서부터 민감한 개인정보 또는 기업정보 또는 고객정보의 노출까지 다양한 위협에 취약하게 된다.

또한 사용자는 스마트폰을 쉽게 설정하여 기업 이메일과 데이터에 접근할 수 있다. 적외선 포트를 이용하는 동기화는 대부분의 경우 인증을 요구하지 않아 바이러스로 장치가 손상되었다면 정보 시스템에 대해 위협이 된다.

4.3 무선 네트워크와 관련된 위험

다양한 서로 다른 네트워크로의 스마트폰 연결은 무선 매체의 내재적 특성과 2.5G와 3G 네트워크에 의한 인터넷에 상시 접속성으로 인해 위험을 발생한다. 4G 네트워크에 의한 서로 다른 형태의 무선 네트워크의 상호 연결은 리바운드와 복잡도에서 여러 요인에 의해 위험을 증가시킬 것이다.

○ 블루투스 : 블루투스는 보안 기능을 제공하나 매우 자주 이러한 기능이 구현되지 않거나 스마트폰에서 구동되지 않는다. 대부분의 경우 스마트폰에서의 블루투스 보안의 구현은 메커니즘과 블루투스 모드를 “비인지(non-discoverable)”로 설정하는 것으로 제한된다. Redfang[11]과 BTscanner와 같은 툴은 블루투스 주소의 마지막 6 바이트를 무조건 공격하여 read_remote_name( ) 함수를 호출함으로써 “비인지” 모드를 우회한다. Redfang은 리눅스 플랫폼에서 동작한다. 노키아 6600과 소니에릭손 P900을 위해 개발된 BTbrowser와 같은 툴은 사용자가 주변 장치를 목록화하고 PIM 데이터와 파일을 탐색한다.
몇몇 블루투스는 노키아 폰이 잘못 구성된 OBEX 메시지에 의해 발생되는 버퍼 오버플로우에 취약하도록 할 수 있다[12]. 또 다른 취약성은 페이링 메커니즘을 통해 구축된 신뢰 관례를 포함한다. 이것은 관계가 더 이상 신뢰 장치 목록에 존재하지 않은 후에도 공격 대상 모르게 공격자가 장치 상의 파일에의 비인가된 접근을 얻도록 한다[13]. 프로토콜의 복잡도가 주어졌을 때 장치 상의 구현 오류는 장치 내의 보안 홀을 지속적으로 유발할 것이다.

○ GPRS : GPRS에 연결된 스마트폰은 GPRS IP 백본으로부터 발생되는 위험에 노출된다. GPRS 백폰에 대한 보안은 GGSN(Gateway GPRS Support Node)를 안전하게 하기 위해 운영자가 취하는 대책 수단에 달

려 있다. 만약 GGSN이 손상되면 GPRS 운영자의 가입자는 인터넷으로부터의 공격에 노출되게 된다. 또한 GPRS 네트워크의 NAT에 대한 공격이 제기되었다[14]. 이 공격은 구현이 간단하다. GPRS가 가능하게 하는 것은 스마트폰이 항상 인터넷에 연결되어 있도록 하여 이메일 Push, 동기화 또는 OTA 프로비저닝을 위한 것인데, 이로 인한 공격이 발생할 수 있다. 또한 다중의 활성화된 PDP(Packet Data Protocol) 컨텍스트를 지원하는 스마트폰은 위험이 있다. 공개 컨텍스트와 사설 컨텍스트를 동시에 가능하게 하는 것은 공개 컨텍스트에 사설 컨텍스트를 노출되게 할 수 있다. 이것은 공개 컨텍스트로부터의 공격에 사설 컨텍스트를 취약하게 한다. 심비안 OS 버전 8은 다중의 활성화된 PDP 컨텍스트를 지원한다. 스마트폰 사용자는 정보 시스템에 동시에 연결되어 웹 브라우징하거나 인스턴트 메시지를 이용하기 때문에 이것으로 인해 공격자는 정보 시스템에 접근을 획득하게 된다. 이런 위험은 모뎀으로 인터넷에 직접 연결하는 LAN에 연결하는 것과 같다.

4.4 어플리케이션과 관련된 위험

스마트폰 상의 어플리케이션 개발은 주로 게임과 모바일 상거래 어플리케이션에 대해 활성화되기 시작하고 있다. 이러한 어플리케이션은 독립형(stand-alone) 어플리케이션 또는 브라우저 기반의 형태를 갖는다.

○ 자바 MIDlets : MIDlets은 스마트폰에 대한 자바 독립형 어플리케이션이다. 스마트폰과 같이 자원이 제약되는 장치에 대해서는 J2ME 또는 자바 2 플랫폼, 마이크로 에디션 기술은 CLDC(Connected Limited Device Configuration)를 통해 기본적인 API와 MIDP(Mobile Information Device Profile)을 정의한다. 현재 MIDP에 대해 MIDP 1.0과 MIDP 2.0이 존재한다.

자바 MIDP 1.0 어플리케이션은 sandbox 모델에 따라 시스템 자원에 대해 제한된 접근만이 가능한 데 전체 바이트코드 검증이 스마트폰에 대해 너무 부담이 크므로 바이트코드 검증이 제한된다. 이것은 보안 매니저와 수많은 보안 패키지에 동일하게 적용된다. 또한 MIDP 1.0은 HTTPS를 포함하지 않아서 네트워크 프로토콜로 HTTP로 제한된다. 이러한 제약으로 인해 장치를 이용해서 네트워크 상의 데이터에 접근하는 것은 프라이버시 또는 기밀성 측면에서 실질적인 위험을 나타낸다.

MIDP 1.0 어플리케이션의 제한된 기능과 보안의 결함으로 인해 자바 MIDP 2.0 스펙은 MIDlets에 보다 나은 보안 특성과 기능을 제공하는 것을 목적으로 한다[15]. 자바 MIDP 2.0은 신뢰 MIDlets 개념을 도입한다. 만약 MIDlet이 신뢰되지 않으면 이것은 sandbox 환경에서 동작하게 된다. 만약 MIDlet이 신뢰되면 MIDP 2.0은 MIDlets가 PIM과 네트워크 접근과 전화 호출과 메시지 전송을 하기 위해 시스템 자원에 더 많이 접근하는 것을 허용한다.

○ 브라우저 이슈 : 만약 인터넷 익스플로러 또는 오페라의 취약한 버전이 스마트폰에서 실행되면 스마트폰은 일반적인 데스크톱과 동일한 방법으로 손상될 수 있다.

4.5 보안 고려 사항

○ 법적 이슈 및 보안 정책 : 고용인이 스마트폰을 사용함으로써 기업은 정보시스템을 기업 외부로 통제를 확장하여야 한다. 특히 스마트폰이 고용인 소유인 경우라면 통제는 법적으로 제한되도록 한다. 이 경우 기업은 다음과 같은 선택이 가능하다.

- 스마트폰의 개인 사용 금지 : 이것은 인터넷의 개인 사용을 금지하는 것과 동일하여 비현실적이고 물리적 통제와 시행이 불가능하다.

- 스마트폰의 개인 사용에 대한 제한 설정 : 이 경우 스마트폰과 정보 시스템 사이의 인가된 상호연동을 명확하게 정의하는데 이 역시 물리적 통제와 시행은 불가능하다.

비밀 정보의 노출되거나 스마트폰의 분실 또는 도난이 발생했을 때 비록 그 스마트폰이 고용인 소유라 할지라도 기업은 그 결과의 손실에 대해 책임을 갖는다.

기업 내에서 스마트폰에 의한 위험을 방지하는 데 있어서의 첫 번째 단계는 스마트폰의 존재를 인식하고 스마트폰 사용과 스마트폰 사용자에 대해 보안 정책을 채택하는 것이다. 이러한 보안 정책은 각 형태의 위험에 대해 권고 사항을 설명하고 위험과 해가 없는 행동 사이를 구분해야 한다.

보안 정책에서 정의되어야 하는 중요한 주 행동은 다음과 관련이 된다.

- 동기화(PIM, 첨부가 있는 이메일 또는 첨부가 없는 이메일)
- 공공 지역 내에서의 장치의 사용(핫스팟을 인식, 동작하지 않는 블루투스)
- 장치로부터 정보 시스템으로의 다운로딩 및 전송

○ 스마트폰 보안 프레임워크 : 스마트폰을 정보 시스템의 요소로 통합하는 것은 다음을 포함하는 보안 프레임워크를 의미한다.

- 중앙화된 관리 솔루션 : 중앙화된 관리 솔루션은 장치의 보다 나은 통제와 정보시스템과 스마트폰 사이의 상호 인증을 이용하여 정보 시스템과의 상호 연동을 허용한다.
- 장치와 서버 사이의 상호 인증
- 단대단 암호화 : 중앙 관리와 결합하여 통신과 스마트폰에 저장된 데이터 암호화는 비밀 정보의 노출 위험을 경감시킨다. 장치의 손실 또는 도난의 경우에 중앙 관리 솔루션은 원격으로 장치에 저장된 데이터를 삭제할 수 있다.
- 스마트카드의 하드닝 : 스마트폰은 랩탑과 동일한 방법으로 안티 바이러스와 개인 침입차단시스템과 함께 하드닝될 필요가 있다.

○ 보안 기술

<표 2> 스마트폰의 보안 기능

기능	설명
보안 OS 플랫폼	보안이 개선된 리눅스, 심비안 v9, OS 가상화
어플리케이션 인증	컨텐츠 다운로드 시 출처 및 악성코드 미감염 여부 검증
암호 및 사용자 인증	파일 시스템/데이터 암호화와 보안 로그인 기능
데이터 분실 및 도난 대비	원격 데이터 삭제 가능한 장치 삭제와 잠금 기능
스팸/바이러스 필터링	모바일 네트워크 상의 중앙서버/보안 게이트웨이와 연동하여 필터링, 단말 내 보안 S/W

V. 보안 제품 동향

5.1 국외

○ 시만택, 노턴 스마트폰 시큐리티[16] : 안티바이러스, 침입차단시스템, SMS 안티스팸 기술을 이용하여 다음과 같은 주요 특징을 갖는다.

- SMS 스팸의 최소화
- 스눕웨어 차단
- 바이러스와 다른 위협으로부터 보호
- SMS 안티스팸 보호
- 노턴 안티바이러스 기술이 개별 파일과 파일 아키브와 어플리케이션 내에 해가 되는 바이러스와 웜과 모바일 스파이웨어를 자동으로 스캔하고 탐지하고 검역

- 실시간 보호
- 심비안과 MS 윈도우즈 모바일 플랫폼 지원
- 사용자가 쉽게 안티바이러스 스캔과 업데이트를 관리하고 스케줄링하고 침입차단시스템 보호 수준을 설정하고 어떤 파일을 암호화할 것인지를 관리하는 것이 가능

○ 가디언에지, 스마트폰 프로텍션(Smartphone Protection)[17] : 보호되는 데이터 노출과 주요 지적 재산의 손실 등의 위험으로 조직을 보호한다.
- 원격 보안 관리 및 삭제 기능을 통해 폰 상의 데이터의 안전성을 보장
- 장치를 안전하게 하기 위해 어플리케이션 통제와 침입차단시스템 설정을 적용
- 스마트폰과 연결된 SD 카드 암호화를 이용하여 민감하고 법적으로 보호해야 하는 데이터와 거래 비밀 및 지적 재산 등의 손실과 연관됨 위험을 없앰
- 온디바이스 포트(USB, IR, WiFi, 블루투스, SD)의 통제를 통해 폰에게 인가된 지역 연결만을 허용하는 정책을 시행

○ F-Secure의 모바일 시큐리티(Mobile Security)[18] : 사용자의 폰이 손실되거나 도난당하거나 모바일 바이러스에 의해 감염된 경우 모바일 시큐리티는 개인 정보와 비밀 정보를 안전하게 보호한다. 새로운 원격 GPS 위치자 특성을 이용해서 사용자는 항상 자신의 폰의 위치를 알 수 있다.
- 해로운 사이트를 자동으로 차단함으로써 안전한 모바일 서핑 보장
- 스파이웨어 탐지 및 삭제
- 손실 또는 도난시 원격으로 스마트폰 잠금을 수행하거나 비밀 데이터 삭제 가능
- 모든 형태의 악의적인 소프트웨어로부터 사용자 스마트폰을 실시간 보호
- 개인침입차단시스템을 이용하여 해커로부터 사용자 컴퓨터 보호(침입차단시스템은 안드로이드 버전에는 포함되지 않음)
- 인스톨 및 사용 용이
- 자동 업데이트를 통해 새로운 모바일 위협에 대해 빠르게 대처

○ Fortinet, 포티모바일(FortiMobile)[19] : 윈도우즈 모바일 또는 심비안 플랫폼을 운영하는 스마트폰을 보호하는 다양한 보안 기능을 제공한다. 주요 특성은 안티 바이러스 스캐닝, 개인 침입차단시스템, 아웃룩 주소록 보호(윈도우즈 모바일용), IPSec VPN, SMS 안티스팸 및 필터링, 폰 보안 및 호출 필터링을 포함한다. 포티가드(FortiGuard) 가입자 서비스로부터의 자동화된 업데이트는 최신 위협에 대해 보호된다.

○ 트렌드 마이크로 모바일 시큐리티(TMMS 6.5, Trend Micro Mobile Security 6.5)[20] : TMMS 6.5의 주요 기능은 휴대폰을 도난 혹은 분실했을 경우에도 정보 유출을 방지하도록 원격으로 내부 데이터 포맷할 수 있는 다양한 운영환경과 최신형 터치스크린 스마트폰을 보호한다. 그리고 바이러스 및 각종 스팸으로 위협받는 소중한 개인정보 및 전화 커넥션을 보호한다. TMMS 6.5에서 새로이 추가된 기능은 휴대폰 분실 시 정보 도난을 방지하도록 권한 없는 사람이 SIM 카드를 제거할 경우 기밀 데이터를 보호하며 원격에서 데이터를 포맷하는 것도 가능하다. 6.5버전은 심비안과 윈도우 모바일 두 가지 플랫폼을 동시 지원한다.

○ Aiko Solutions, SecuBox for Smartphone[21] : SecuBox는 암호화 소프트웨어로 윈도우즈 모바일 스마트폰과 메모리 카드에 저장된 비밀 정보를 암호화한다. SecuBox는 AES 256비트의 암호 알고리즘을 이용하여 모든 비밀 파일과 문서에 대해 안전한 “금고”를 생성한다. 즉, 이 안전한 “금고”에 기록되는 데이터는 자동적으로 그리고 투명하게 암호화된다. 또한

SecuBox는 손쉬운 예외 처리를 제공하고 사용자 장치의 성능을 유지한다.

5.2 국내

○ 소프트시큐리티, 터치앤세이프(TouchnSafe)[22] : 터치앤세이프는 2009년 7월부터 6개월 동안 정보통신산업진흥원(NIPA)의 과제로 소프트씨큐리티(주)를 중심으로 루멘소프트(주), 쉬프트웍스(주) 3사가 공동 개발한 스마트폰에 대한 통합보안솔루션이다. 스마트폰 사용자에게 '보안 브라우저' 형태로 제공되며, 스마트폰에 대한 편리한 보안 환경을 제공한다. 터치앤세이프는 외부와의 주된 통신채널인 웹에 대한 집중적인 보안 관리를 수행하며, 보안 저장소를 이용하여 개인정보를 안전하게 관리한다. 또한 스마트폰 성능에 영향을 주지 않는 저부하 악성코드 탐지기법을 적용해 효율적 보안관리 기능을 수행한다.
각각의 기능 모듈들은 API/SDK 형태로 제공되어져 다양한 응용 서비스 개발을 지원한다. 라이브러리 형태의 각 모듈들은 다양한 제품에서 호출되어 사용될 수 있으며 위젯에서 스크립트를 통해 대부분 모듈의 기능들을 호출하여 사용할 수 있다.

○ 소프트씨큐리티, 터치앤세이프 M. 트랜스키(TouchnSafe M. TransKey)[23] : 스마트폰 입력보안 솔루션으로 터치앤세이프 M. 트랜스키는 가상 키보드를 이용해 입력되는 모든 정보를 암호화함으로써 스마트폰을 통한 정보유출 가능성을 차단한다. 또한 사용 시점에 따라 가상 키보드가 무작위로 생성되며, 입력되는 모든 정보도 암호화하여 전달돼 메모리 해킹 등을 통해 스마트폰 비밀번호, 신용카드 정보, 계좌번호 등의 노출을 방지할 수 있다.

○ 안철수 연구소, AhnLab Mobile Security(AMS)[24] : 안철수 연구소는 2001년부터 모바일 보안 솔루션 AMS를 개발하여 판매하고 있다. AMS는 윈도우즈 모바일이나 심비안 운영체제를 이용한 스마트폰과 같은 휴대전화에 설치되어 웜, 트로이목마, 바이러스 등 악성코드를 실시간으로 차단하여, 모바일 디바이스를 안전하게 보호하는 보안 솔루션이다.

Ⅵ. 스마트폰 OS 분석

6.1 심비안 OS

심비안 OS는 심비안 재단에서 개발한 모바일 기기용 운영체제로, 라이브러리, 사용자 인터페이스, 프레임워크, 다양한 도구를 포함한다. 심비안 OS는 원래 EPOC 운영체제를 기반으로 하고 주로 Psion가 개발한 PDA에 사용되었다. 심비안 OS는 EPOC 버전 5.0 이후 버전 6.0부터 시작된다. 가장 최신 버전은 9.5로 버전 9부터 보안 플랫폼이 도입되었다. 심비안 OS는 서로 다른 모바일 장치를 수용하기 위해 몇 개의 UI 참조 모델 플랫폼을 정의한다. 심비안 OS는 2G와 2.5G와 3G 셀룰러 시스템 내 광범위한 음성과 데이터 서비스뿐만 아니라 멀티미디어와 데이터 동기화를 지원하도록 설계되었다. 최초에는 폐쇄형 소스였으나 2010년 2월 4일 오픈 소스로 전환되었다.

심비안 OS의 주요 특징은 다음과 같다.

○ WCDMA와 GSM/GPRS 및 cdma2000 1x RTT를 지원하는 모바일 기술
○ SMS, EMS, MMS를 지원하는 메시지 서비스
○ 인터넷 이메일 서버, 멀티미디어 기록, 플레이백, 스트리밍
○ 블루투스, USB, TCP/IP의 통신 프로토콜 지원
○ 암호화(예, 3DES, RC5, AES, RSA, SHA1, HMAC) 및 전자 인증서 보안

○ TLS/SSL, WTLS, IPSec을 포함하는 보안 프로토콜
○ 메모리 관리와 프로세스와 쓰레드 스케줄링 및 프로세스간 통신, 프로세스 및 쓰레드 관련 자원 관리, 하드웨어 추상화 및 에러 핸들링을 수행하는 실시간, 멀티쓰레드, 선점적 커널
○ 개발 언어 : C++, Java, Flash Lite, Python, Ruby, OPL, PIPS

6.2 아이폰 OS

애플사가 개발한 아이폰은 2007년 6월 29일에 출시된 이후 가장 빠르게 성장하고 있는 스마트폰이다. OS 계열은 Mac OS X/유닉스 계열로 일부 소스만 오픈되어 있다. 최신 버전은 2010년 2월에 출시된 3.1.3으로 ARMv6, ARMv7-A, Apple A4(아이폰, 아이터치, 아이패드)의 플랫폼을 지원한다.

아이폰과 아이포드 터치에는 앱 스토어를 통한 프로그램만을 공식적으로 인스톨할 수 있다[25]. 그러나 버전 1.0부터 비인가된 써드파티 내부 어플리케이션이 작동 가능해졌다[26]. 비록 애플이 SIM 잠금 해제를 수행하는 어플리케이션 이외의 내부 어플리케이션이 손상되도록 소프트웨어 업데이트를 설계하지 않을 것이라고 발표했지만 그러한 어플리케이션은 아이폰 OS 업데이트로 인해 동작하지 않을 가능성이 존재한다. 이러한 어플리케이션을 배포하는 방법은 Cydia, Icy, Rock 및 인스톨러 유틸리티이다. 이러한 프로그램은 탈옥(jailbreaking) 이후에 아이폰에 인스톨될 수 있다.

아이폰에서 사용되는 보안 기술은 다음과 같다.

○ 장치 통제 및 보호
- 패스코드 정책 : 장치 패스코드는 비인가된 사용자가 아이폰에 저장된 데이터에 접근하거나 다른 방법을 통해 장치에 접근하는 것을 방지한다. 아이폰 OS를 이용하여 사용자는 자신의 보안 요구(타임아웃 기간, 패스코드 강도, 변경 주기 등)에 맞는 패스코드 요구사항을 선택할 수 있다.
- 정책 시행 : 정책은 아이폰에서 두가지 방법으로 설정될 수 있다. 만약 장치가 MS 익스체인지 계정에 접근하도록 설정되었다면 익스체인지 액티브싱크(ActiveSync) 정책이 OTA를 통해 장치에 삽입된다. 이것은 사용자와 연동 없이 시행되고 갱신되게 된다. 정책은 또한 사용자에 대한 설정 프로파일의 부분으로 배포되어 인스톨된다. 프로파일을 삭제하는 것은 관리자 패스워드를 이용해야만 가능하도록 프로파일을 정의하거나 사용자는 프로파일이 장치에 대해 잠겨져 장치의 모든 컨텐츠를 완전히 삭제하지 않고는 제거될 수 없도록 정의할 수 있다.
- 안전한 장치 설정 : 설정 프로파일은 장치 보안 정책과 제약사항, VPN 설정 정보, Wi-Fi 설정, 이메일과 캘린더 계정, 인증 크리덴셜을 포함하는 XML 파일이다. 설정 프로파일에 장치 설정과 함께 패스코드 정책을 구축하는 기능은 기업 내 장치가 올바르고 조직의 보안 표준에 따라 설정되었음을 보장한다. 설정 프로파일은 암호화되고 잠기므로 설정은 삭제되거나 변경되거나 공유될 수 없다. 설정 프로파일은 서명되고 암호화된다. 설정 프로파일은 CMS(Cryptographic Message Syntax, RFC 3852)를 이용하여 암호화된다. CMS는 3DES와 AES 128을 지원한다.
- 장치 제약 : 장치 제약은 사용자가 장치 내의 어떤 아이폰 특성을 접근할 수 있는 지를 결정한다.

○ 데이터 보호
- 암호화 : 아이폰 3GS는 하드웨어 기반의 암호화를 제공한다. 아이폰 3GS 하드웨어 암호화는 AES 256 비트 암호화를 이용하여 장치 내의 모든 데이터를 보호한다. 암호화는 항상 동작되며 사용자가 비활성화할 수 없다. 또한 어플리케이션 데이터를 보호하기 위해 개발자는 어플리케이션 데이터 저장 내

의 데이터를 암호화하기 위해 API에 접근한다.
- 원격 삭제 : 아이폰은 원격 삭제를 지원한다. 만약 장치가 손상 또는 도난당했다면 관리자 또는 장치 소유자는 모든 데이터를 삭제하고 장치를 비활성화하는 원격 삭제 명령어를 발행할 수 있다.
- 로컬 삭제 : 장치는 패스코드 입력이 여러 번 실패한 경우에 로컬 삭제를 자동적으로 개시하도록 설정될 수 있다. 이것은 장치에의 접근을 획득하기 위해 소모적 공격에 대한 주요한 제지 방법이다. 기본적으로 아이폰은 10개의 패스코드 시도 실패 후에 자동적으로 장치를 삭제한다.

○ 보안 네트워크 통신 : VPN, SSl/TLS, WPA/WPA2

○ 보안 플랫폼 : 아이폰 OS는 보안을 가지고 설계된 플랫폼이다. 이것은 어플리케이션 런타임 보호를 위해 “샌드박스(sandboxed)” 기법을 포함하며 어플리케이션이 변경되지 않았음을 보증하는 의무적 어플리케이션 서명을 요구한다. 아이폰 OS 또한 어플리케이션의 안전한 저장과 암호화된 키체인 내에 네트워크 서비스 크리덴셜을 가능하게 하는 보안 프레임워크이다. 개발자를 위해 어플리케이션 데이터 저장을 암호화하는 데 이용될 수 있는 공통 크립토 구조를 제공한다.
- 런타임 보호 : 장치 내의 어플리케이션은 다른 어플리케이션에서 저장한 데이터에 접근할 수 없도록 샌드박스로 보호된다. 또한 시스템 파일, 자원 및 커널은 사용자 어플리케이션으로부터 보호된다. 만약 어플리케이션이 다른 어플리케이션으로부터 데이터에 접근할 필요가 있다면 아이폰 OS에 의해 제공되는 API와 서비스를 이용해서만 접근이 가능하다. 코드 생성은 금지된다.
- 의무적 코드 서명 : 모든 아이폰 어플리케이션은 서명되어야 한다. 장치와 함께 제공되는 어플리케이션은 애플이 서명한다. 써드 파티 어플리케이션은 애플이 발급한 인증서를 이용하여 개발자가 서명한다. 이것은 어플리케이션이 변경되지 않았음을 보장하며 런타임 체크는 어플리케이션이 마지막으로 사용된 이후 비신뢰된 상태로 되지 않았음을 보장하기 위해 수행된다.
- 안전한 인증 프레임워크 : 아이폰은 디지털 아이덴터티, 사용자 이름 및 패스워드를 저장하기 위해 안전하고 암호화된 키체인을 제공한다. 키체인 데이터는 분리되어 써드 파티 어플리케이션에서 저장되는 크리덴셜이 다른 아이덴터티를 갖는 어플리케이션에 의해 접근될 수 없도록 한다. 이것은 아이폰 상의 인증 크리덴셜을 안전하게 하는 메커니즘을 제공한다.
- 공통 암호 구조 : 어플리케이션 개발자는 암호화 API에 접근할 수 있다. 데이터는 AES, RC4 또는 3DES와 같이 안전성이 증명된 알고리즘으로 암호화된다. 또한 아이폰은 AES와 SHA-1 암호를 위한 하드웨어 가속기를 제공한다.

아이폰에 대해 다음과 같은 보안 이슈가 논의되고 있다.

○ 탈옥(jailbreaking) : 아이폰에서 공식적으로 지원하지 않는 어플리케이션이나 기능들을 사용하기 위해 아이폰의 OS를 조작하기 위한 해킹이 발생하는데, 이를 탈옥이라 한다. 이렇게 탈옥된 아이폰에 대한 위협 사례가 존재한다. 실제로 네델란드의 한 해커는 최근에 포트스캐닝을 통해 넷에 탈옥된 아이폰을 찾아내, 무방비상태에 놓인 해당 아이폰 사용자에게 무시무시한 협박 문자(SMS)를 날렸다.

○ 킬 스위치(kill switch) : 아이폰 사용자들은 애플의 앱스토어를 통해 애플로부터 승인을 받은 어플리케이션을 다운받을 수 있다. 이 때 악의적인 어플리케이션이 존재하면 아이폰의 킬 스위치를 통해 해당 어플리케이션을 삭제할 수 있게 된다. 이 킬 스위치의 비활성화가 해커들의 표적이 되었으나 이를 위해서는 OS

의 Core Location을 비활성화해야 한다는 것이 증명되면서 이에 대한 공격은 중단되었다.

○ 아이폰 해킹툴
- Redsn0w : 가장 보편적으로 모든 기기에서 사용되고 있는 탈옥 툴 (QuickPwn 소스를 기반으로 iPhone Dev Team 및 Chronic Dev Team에서 함께 개발)
- Ultrasn0w : 가장 보편적으로 사용되고 있는 3G/3GS 아이폰을 위한 소프트웨어 잠금해제 툴
- PwnageTool : 커펌을 생성시켜 주는 탈옥 툴
- Yellowsn0w : 3G 아이폰을 위한 소프트웨어 잠금 해제 툴 (펌웨어 2.2 및 베이스밴드 02.28을 유지한 펌웨어 2.2.1)
- QuickPwn : 펌웨어 2. x 지원하는 탈옥 툴
- BootNeuter : 가장 보편적으로 사용되고 있는 2G 아이폰을 위한 소프트웨어 잠금해제 툴

6.3 윈도우 모바일

윈도우즈 모바일(Windows Mobile, WM)은 PDA 및 스마트폰에 사용하는 운영 체제이다. 이전에는 포켓 PC라고 불렸다. 이 운영체제는 마이크로소프트사에서 내놓은 모바일 운영체제로 임베디드용 운영 체제인 윈도 CE를 기반으로 한다. 7.0 버전이 2010년 2월에 공개되었으나 대부분의 휴대폰에는 6.x 버전이 탑재되어 있다.

윈도우 모바일 보안 특징은 다음과 같다.

○ 장치 잠금 : 시스템 관리자는 장치 잠금 전에 비활성화 기간을 지정할 수 있고 사용자에게 PIN/패스워드를 재입력하도록 요구할 수 있다.
○ 개선된 패스워드 : 관리자는 조직에 적합한 패스워드 정책을 설정할 수 있다.
○ 장치 삭제 : 장치 내 프로그램과 데이터와 사용자에게 특정한 설정은 로컬 또는 원격 장치 삭제를 통해 제거될 수 있다. 윈도우즈 모바일 6이 탑재된 장치에서 장치 삭제는 삭제 가능한 저장 카드의 컨텐츠도 지울 수 있다.
- 로컬 삭제는 사용자가 잠긴 장치에 잘못된 패스워드를 특정 수 이상 입력했을 때 수행된다.
- 원격 삭제는 OWA 또는 익스체인지 액티브싱크 콘솔로부터 명확한 삭제 명령을 발행하는 관리자를 통해 동작할 수 있다.

○ 다중 수준의 암호화 : 통신 프라이버시와 인증을 개선하기 위해 윈도우즈 모바일은 여러 계층의 암호화를 제공한다.
- SSL 채널 암호화 : SSL은 OTA 또는 유선을 통해 장치(저장 카드를 포함)와 서버 사이에 전송되는 데이터를 암호화한다.
- S/MIME 지원 : S/MIME은 장치와 서버 사이에 전송되는 또는 저장된 이메일 메시지에 대해 부가적인 보안 기능을 제공한다.
- Wi-Fi 암호화 : 윈도우즈 모바일은 802.11a/b/g 무선 LAN을 사용하기 위해 WPA(Wireless Protected Access)와 WPA2와 WEP(Wired Equivalent Privacy) 암호화 표준을 지원한다.
- 저장 카드 암호화 : 윈도우즈 모바일 6은 삭제가능한 저장 카드에 저장된 데이터를 보호하기 위해 128비트 AES 암호화를 지원한다.

○ 내장된 VPN 지원 : 기본적으로 윈도우즈 모바일은 LT2P/IPSec(Layer Two Tunneling Protocol with Internet Protocol Security encryption) 또는 PPTP(Point-to-Point Tunneling Protocol)를 이용한 VPN을 지원한다.
○ IRM(Information Rights Management) 지원 : 윈도우즈 모바일 6은 이메일과 첨부에 대해 IRM을 지원한다. IRM을 통해 사용자는 메시지와 문서를 누가 접근하여 이용할 수 있는 지를 정할 수 있다.
○ 루트 및 사용자 인증서의 용이한 관리

6.4 안드로이드

안드로이드는 리눅스 커널의 수정된 버전을 이용한 모바일 OS이다. 안드로이드사가 이 OS를 개발하였으며 후에 구글에 매각된 이후 OHA(Open Handset Alliance)에서 인수된다. 안드로이드는 개발자가 구글이 개발한 자바 라이브러리를 통제하면서 관리된 코드를 자바 언어로 기록하는 것을 허용한다.

2007년 11월 5일에 안드로이드 배포가 OHA 설립과 함께 발표되었다. OHA는 47개의 하드웨어, 소프트웨어, 통신 회사가 모여 모바일 장치의 개방형 표준을 개선하고자 만든 컨소시움이다. 구글은 아파치 라이센스(무료 소프트웨어 및 개방형 소스 라이센스) 하에서 대부분의 안드로이드 코드를 공개했다.

○ 안드로이드 구조

안드로이드는 크게 어플리케이션, 어플리케이션 프레임워크, 라이브러리, 안드로이드 런타임, 리눅스 커널로 구성된다.

- 어플리케이션 : 안드로이드는 이메일 클라이언트, SMS 프로그램, 캘린더, 지도, 브라우저, 연락처 등을 포함해 여러 핵심 어플리케이션을 탑재한다. 모든 어플리케이션은 자바 프로그래밍 언어를 이용하여 개발된다. 소스는 비공개이다.
- 어플리케이션 프레임워크 : 개방형 개발 플랫폼을 제공함으로써 안드로이드는 개발자가 어플리케이션 개발이 가능하도록 한다. 개발자는 자유롭게 장치 하드웨어 접근 위치 정보의 장점을 가질 수 있고 백그라운드 서비스를 작동하며 알람을 설정하고 상태 바에 알림을 추가하는 등의 개발을 할 수 있다. 개발자들은 핵심 어플리케이션이 이용하는 동일한 프레임워크 API에 완전히 접근할 수 있다. 소스는 비공개이다.
- 라이브러리 : 안드로이드는 안드로이드 시스템의 다양한 요소에서 사용되는 C/C++ 라이브러리를 포함한다. 이러한 기능은 안드로이드 어플리케이션 프레임워크를 통해 개발자에게 공개된다.
- 안드로이드 런타임 : 안드로이드는 대부분의 기능을 자바 프로그래밍 언어의 핵심 라이브러리에 제공되는 핵심 라이브러리를 포함한다. 소스는 비공개이다.
- 리눅스 커널 : 안드로이드는 보안, 메모리 관리, 프로세스 관리, 네트워크 스택 및 드라이버 모델과 같은 핵심 시스템 서비스에 대해 리눅스 버전 2.6을 기반으로 한다. 이 커널은 하드웨어와 나머지 소프트웨어 스택 사이의 추상화 계층으로 동작한다. 소스가 공개된다.

<표 3> 안드로이드 구조

구분	설명
어플리케이션	이메일 클라이언트, 캘린더, 지도, 연락처 등의 어플리케이션이 탑재되는 계층
어플리케이션 프레임워크	개방형 플랫폼 계층으로 윈도우 매니저, 액티비티 매니저, 기술 매니저, 자원 매니저 등 개발자가 어플리케이션을 개발할 수 있는 플랫폼을 제공
안드로이드 런타임	핵심 라이브러리와 가상 머신을 포함하는 계층
라이브러리	어플리케이션을 개발할 수 있는 라이브러리를 포함하는 계층
리눅스 커널	하드웨어와 나머지 소프트웨어 스택 사이의 추상화 계층으로 디스플레이 드라이버, 카메라 드라이버, 키패스 드라이버, WiFi 드라이버가 동작

○ 보안 대책

- 보안 샌드박스(Secure sandbox) : 안드로이드 보안 구조 설계의 핵심은 기본적으로 어떠한 어플리케이션도 다른 어플리케이션 또는 OS 또는 사용자에게 악의적인 영향을 주는 동작을 수행하지 못한다는 것이다. 이것은 사용자의 비밀 데이터의 읽기/기록과 다른 어플리케이션의 읽기/기록 또는 네트워크

접근 수행 등을 포함한다. 어플리케이션 프로세스는 보안 샌드박스이다. 이것은 명시적으로 기본 샌드박스에서 제공되지 않는 부가적인 기능이 필요하다고 허가를 선언하는 것을 제외하고는 다른 어플리케이션을 건드리지 않는다. 이러한 허가는 인증서를 기반으로 자동적으로 허용하거나 허용하지 않거나 함으로써 또는 사용자의 허가에 따르는 다양한 방법으로 통제된다. 어플리케이션에서 필요로 하는 허가는 해당 어플리케이션에서 선언된다.

- 어플리케이션 서명 : 모든 안드로이드 어플리케이션(.apk 파일)은 인증서로 서명되어야 한다. 인증서의 개인키는 개발자가 소유한다. 이 인증서는 어플리케이션의 개발자를 식별한다. 안드로이드 어플리케이션이 자가 서명된 인증서를 사용하는 것을 허용하며 어플리케이션 사이의 신뢰 관계를 구축할 경우에만 사용된다. 서명이 보안에 영향을 주는 가장 중요한 점은 누가 서명 기반의 허가에 접근할 수 있고 누가 사용자 ID를 공유할 수 있을 지를 결정하는 것이다.

- 사용자 ID와 파일 접근 : 장치 상에 인스톨된 각 안드로이드 패키지(.apk) 파일에 유일한 리눅스 사용자 ID가 주어진다. 이 사용자 ID는 파일에 대해 샌드박스를 생성하고 다른 어플리케이션을 건드리는 것(또는 다른 어플리케이션이 파일을 건드리는 것)을 방지한다. 어플리케이션이 장치에 인스톨될 때 이러한 사용자 ID가 지정되며 장치에 존재하는 한 영구적으로 존재한다. 보안 시행이 프로세스 수준에서 발생하기 때문에 임의의 두 개의 패키지의 코드가 동일한 프로세스에서 동작할 수 없다. 사용자는 각 패키지의 AndroidManifest.xml의 태그 내의 sharedUserID 특성을 이용하여 두 개의 패키지에 동일한 사용자 ID를 지정하도록 할 수 있다. 이렇게 함으로써 두 패키지가 동일한 사용자 ID와 허가를 갖는 동일한 어플리케이션으로 다뤄질 수 있다. 보안을 유지하기 위해 동일한 서명으로 서명된 두 개의 어플리케이션에만 동일한 사용자 ID가 주어지게 된다. 어플리케이션이 저장하는 데이터에 해당 어플리케이션 사용자 ID가 지정되어 다른 패키지에 접급할 수 없게 된다. getSharedPreferences (String, int) 또는 openFileOutput (String, int) 또는 openOrCreateDatabase(String, int, SQLiteDatabase. CursorFactory)으로 새로운 파일을 생성할 때 사용자는 다른 패키지가 그 파일을 읽고 기록할 수 있도록 하기 위해 MODE_WORLD_READABLE 또는 MODE_WORLD_WRITEABLE 플래그를 이용할 수 있다. 이러한 플래그를 설정하면 그 파일이 사용자의 어플리케이션 소유이나 글로벌 읽기 또는 쓰기 허가가 설정되어 임의의 다른 어플리케이션이 그 파일에 접근할 수 있다.
- URI 허가 : 앞에서 설명한 일반적인 허가 시스템은 컨텐츠 제공자가 사용하기엔 충분치 못한 면이 있다. 컨텐츠 제공자는 읽기/쓰기 허가로 컨텐츠를 보호하고자 하는 반면 클라이언트 또한 다른 어플리케이션에 대한 특정 URI에 접속하기를 바란다. 예를 들어 메일 어플리케이션 내의 첨부가 있다. 메일에의 접근은 허가로 보호되어야 한다. 왜냐하면 메일은 민감한 사용자 데이터이기 때문이다. 그러나 만약 이미지 첨부에 대한 URI가 이미지 뷰어에 주어지면 그 이미지 뷰어는 허가가 없어 그 첨부를 열 수 없게 된다. 왜냐하면 이미지 뷰어는 모든 이메일에 접근할 허가를 가질 이유가 없기 때문이다. 이러한 문제를 해결하기 위한 것이 URI별 허가이다.

Ⅶ. 결론

본 논문에서는 스마트폰의 전반적인 시정 동향과 보안 제품 동향 및 주요 스마트폰 OS의 보안 기술을 분석하였다.

아래 표는 OS별 주요 보안 메커니즘을 보여준다.

<표 4> 스마트폰 OS에서 사용되는 보안 메커니즘

폰 모델	보안 메커니즘
심비안 OS	인증서 관리 및 암호 등
윈도우즈 모바일	보안 정책, 역할 및 인증
안드로이드	리눅스 기능(사용자 및 그룹 ID) 허가 수준 보안
아이폰 OS	인증 프레임워크, 공통 암호 구조 제공 등

일상생활에 스마트폰이 활용되면 될수록 스마트폰에는 기업/개인/고객 정보 등의 주요 정보의 집적은 증대될 것이다. 그러므로 이러한 주요 정보에 대한 보안 및 개인정보보호 측면에서의 연구가 지속적으로 진행될 것이다.

참고문헌

[1] 위키백과사전, http://ko.wikipedia.org/wiki/

[2] 셀룰러, http://www.cellular.co.kr/news/articleView.html? idxno=5646

[3] 1인 미디어 뉴스 공동체 BLOTER.NET, http://www.bloter.net/archives/22183

[4] http://blog. cellphoneshop.com/2010/01/rising-demand-for-smartphone-security.html

[5] 방송통신소비자신문, http://www. u-press.co.kr

[6] 서울경제

[7] 경향신문, 2010년 1월 26일.

[8] 디지털타임스, 로아그룹

[9] http://ncsp.forum.nokia.com/downloads/nokia/documents/Known_Issues_in_the_Nokia_6600_v1_0_en.pdf

[10] http://www.cewindows.net/bugs/wm2003netsec.htm

[11] http://www.atstake.com/research/tools/info_gathering/

[12] http://www.bluestumbler.org

[13] Attacks on GPRS - Candolin, Lundberg

[14] MIDP 2.0 Security Enhancements - Kolsi, Virtanen

[15] http://www.symantec.com/norton/

[16] 가이언에지, http://www.guardianedge.com/shared/ds_smartphone.pdf

[17] http://www.f-secure.com/system/fsgalleries/brochures/FSC_ms6_consumers_htc.pdf

[18] http://www.fortinet.com/products/forticlient/

[19] 트렌드 마이크로 모바일 시큐리티 6.5, http://kr.trendmicro.com/kr/about/news/pr/article/20091207120739. html

[20] SecuBox for Smartphone, http://www.aikosolutions.com/products/secubox-for-smartphone/

[21] http://www.touchnsafe.com/

[22] Datanet, http://www.datanet.co.kr/news/news_view.asp? id=48794&acate1=0&acate2=3

[23] 안철수 연구소 AMS, http://www.ahnlab.com/kr/site/product/

[24] http://www.usatoday.com/tech/columnist/edwardbaig/2007-06-26-iphone-review_N.htm

[25] http://www.usatoday.com/tech/columnist/edwardbaig/2007-06-26-iphone-review_

[26] http://www.latimes.com/news/opinion/la-oew-healey 6aug06,0,3456267.story

■ 저자소개 ■

이 영 숙
Lee, Young Sook

2009년 3월~현재
호원대학교 사이버수사경찰학부
전임 강사
2008년 8월 성균관대학교 컴퓨터공학과
(공학박사)
2005년 2월 성균관대학교 정보보호학과
(공학석사)
1987년 2월 성균관대학교 정보공학과(공학사)

관심분야 : 암호프로토콜 암호이론, 네트워크 보안
E-mail : ysooklee@howon.ac.kr

김 지 연
Kim, Jee Yeon

1996년 12월~2007년 1월
한국정보보호진흥원 선임연구원
2006년 2월 성균관대학교 컴퓨터공학과
(공학박사)
2007년 2월 성균관대학교 정보공학과(공학석사)
1995년 2월 성균관대학교 정보공학과(공학사)

관심분야 : 암호프로토콜 암호이론,
정보보호관리체계 인증
E-mail : jeeyeonkim@paran. com

논문접수일 : 2010년 4월 10일
수 정 일 : 2010년 4월 23일
게재확정일 : 2010년 5월 25일