스마트폰 보안 위협 및 대응 기술

Smartphone Threats and Security Technology

모바일 소프트웨어 기술 동향 특집

강동호 (D.H. Kang)	인프라보호기술연구팀 선임연구원
한진희 (J.H. Han)	융합서비스보안연구팀 선임연구원
이윤경 (Y.K. Lee)	자식정보보안연구팀 선임연구원
조영섭 (Y.S. Cho)	인증기술연구팀 책임연구원
한승완 (S.W. Han)	지식정보보안연구팀 선임연구원
김정녀 (J.N. Kim)	휴먼인식기술연구팀 팀장
조현숙 (H.S. Cho)	지식정보보안연구부 부장

목 차

Ⅰ. 서론
Ⅱ. 스마트폰 보안 위협요소
Ⅲ. 모바일 악성코드
Ⅳ. 스마트폰 보안 기술
Ⅴ. 결론

스마트폰 시장 경쟁 본격화에 따른 개방형 플랫폼 증가와 앱스토어의 등장으로 인하여 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. 따라서 향후 더욱 지능화되고 다양한 형태로 변형될 수 있는 악의적 행위에 의한 정보 유출, 불법 과금, 부정 사용 등과 같은 보안 위협으로부터 스마트폰 사용자를 보호하고, 서비스 환경에 안전성, 무결성, 가용성, 신뢰성을 제공하기 위한 스마트폰 보안 기술 개발이 요구된다. 본 고에서는 스마트폰 보안 위협요소와 모바일 악성코드 동향을 살펴보고 이들 위협에 대응하기 위한 단말 및 모바일 보안 인프라 기술들을 소개하고자 한다.

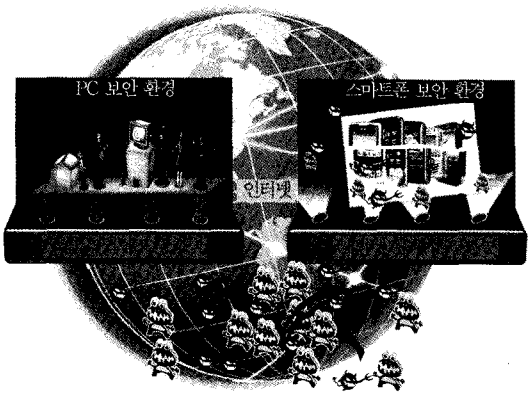
I. 서론

현재 모바일 시장은 3세대 이동통신의 발달과 스마트폰의 성장이 두드러지면서 모바일 인터넷 시대가 본격적으로 도래하고 있고, 하드웨어보다는 그 위에 탑재되는 소프트웨어 플랫폼에 대한 관심이 증가하고 있다. 또한, 아이폰과 앱스토어의 성공은 스마트폰에서 사용될 애플리케이션에 대한 관심을 한층 끌어올리고 있고, 이는 스마트폰 플랫폼으로의 경쟁으로 이어지고 있다. 하지만, 모바일 인프라 및 스마트폰 시장의 활성화는 우리에게 긍정적 효과만을 제공하지는 않는다. 스마트폰 시장 경쟁 본격화에 따른 개방형 플랫폼 증가와 앱스토어의 등장으로 인하여 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[1]. 따라서 향후 더욱 지능화되고 다양한 형태로 변형될 수 있는 악의적 행위에 의한 정보 유출, 불법 과금, 부정 사용 등과 같은 보안 위협으로부터 스마트폰 사용자를 보호하고, 서비스 환경에 대한 안전성, 무결성, 가용성, 신뢰성을 제공하기 위한 스마트폰 보안 기술 개발이 요구된다.

본 고에서는 스마트폰 보안 위협요소와 모바일 악성코드 동향을 살펴보고 이들 위협에 대응하기 위한 단말 및 모바일 보안 인프라 기술들을 소개하고자 한다.

Ⅱ. 스마트폰 보안 위협요소

최근 스마트폰 이용 확산에 따라 시간과 장소에 구애 받지 않고 무선 인터넷을 활용하면서 기존 인터넷 사이트의 환경도 스마트폰 환경 변화에 맞춰 변화되고 있다. PC 환경에서 제공하는 인터넷 서비스가 스마트폰 환경으로 전환되면서 PC 환경의 보안 위협이 스마트폰 환경에서도 나타날 것으로 예상된다. 현재 인터넷 환경에서 PC를 대상으로 나타나는 다양한 유형의 공격은 백신, 방화벽 및 침입탐지 기술로 대응을 하고 있다. 이에 비해 스마트폰은 다양한 무선접속환경의 개방성, 휴대성, 저성능 등으로 기존 PC 환경의 보안 위협과 더불어 새로운 보안 위협에 노출되어 있다((그림 1) 참조)[2],[3].



(그림 1) PC와 스마트폰 환경의 차이점

이러한 스마트폰의 사용환경에 대한 보안 위협은 다음과 같이 정의할 수 있다.

1. 개방성

스마트폰은 일반폰보다 월등히 뛰어난 성능을 가지고 있으며 멀티미디어 처리도 우수하다. 하지만 최근에는 일반폰들의 사양이 스마트폰과 거의 차이가 없을 정도로 개선되어 이를 기준으로 스마트폰과 일반폰을 구분하기는 어렵다. 스마트폰과 일반폰을 구별짓는 가장 큰 특성은 개방성이라 할 수 있다. 스마트폰은 일반폰과는 다르게 무선인터넷 및 외부 인터페이스를 개방하여 제공하고 있다. 또한, 애플리케이션 개발시 시스템 자원의 사용을 위해 SDK를 이용하여 API를 제공하고 있다. 스마트폰의 다양한 외부 인터페이스는 사용자에게 다양한 네트워크 서비스를 지원하고, 내부 API 인터페이스 제공은 개발자에게 편리한 개발환경을 제공한다[4],[5]. 하지만 이를 보안적 측면에서 해석하면, 다양한 외부 인터페이스 제공은 악성코드 전파 경로의 다양성을 제공하고, 내부 인터페이스는 악의적인 개발자에 의해 악성코드가 은닉된 모바일 애플리케이션 제작을 용

이하게 만드는 취약점을 가지고 있다.

2. 휴대성

스마트폰의 휴대 편의성으로 인해 발생하는 분실/도난 사고는 월평균 20만 대에 이르고 있다. 스마트폰 분실/도난에 따른 직접적인 경제적 피해와 더불어 스마트폰에 저장된 개인 정보 및 모바일 오피스를 지원하는 스마트폰의 특성으로 인한 기업 중요 기밀 정보의 유출은 심각한 사회문제를 야기시킬 수 있다. 이에 따라 스마트폰에 저장된 정보를 암호화하거나 분실/도난시 저장된 정보를 원격에서 소거하는 기술들이 등장하고 있다.

3. 저성능

스마트폰은 PC에 비해 저전력, 저성능 기기이다. 따라서, PC 환경에서 제공하는 보안 소프트웨어를 스마트폰에 적용하기에는 무리가 있다. PC 환경에서는 다양한 보안 위협에 대응하기 위해서 지속적인 모니터링을 통해 악성코드를 탐지해야 하지만 스마트폰은 전력 및 성능적 제약으로 인해 백신을 비롯한 보안 소프트웨어의 적용에 어려움이 있다.

Ⅲ. 모바일 악성코드

모바일 악성코드는 스마트폰을 포함한 모바일 단말을 대상으로 정보유출, 단말 파괴, 불법 과금 등의 악의적인 행위를 수행하기 위한 악성 프로그램으로 정의할 수 있다. 모바일 악성코드는 모바일 단말의 성장과 더불어 규모면에서 빠르게 증가하고 있고, 위협 요인도 다양화되고 있다. 모바일 악성코드가 증가하는 원인은 악의적인 목적을 가진 악성코드의 제작 및 유통이 가능한 개방형 단말기의 증가와 함께 블루투스, Wi-Fi와 USB 등 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[1],[6].

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

1. 단말 장애 유발형 악성코드

단말의 사용을 불가능하게 만들거나 장애를 유발하는 공격 유형이다. 2004년에 발견된 Skulls가 단말의 기능을 마비시키는 단말 장애 유발형 악성코드의 한 예이다. 이 악성코드는 모든 메뉴 아이콘을 해골로 변경시키고 통화 이외의 부가기능을 사용할 수 없게 만든다. 2005년에 발견된 Locknut 악성코드는 단말의 일부 키 버튼을 고장내는 특성을 가지고 있다. 이외에도 전화의 송수신 기능을 마비시키는 Gavno가 등장하였다.

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. 과금 유발형 악성코드

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

4. 정보유출형 악성코드

감염된 단말의 정보나 사용자 정보를 외부로 유출시키는 공격 유형이다. 2008년 발견된 Infojack이 대표적인 예이다. 이 악성코드는 합법적인 애플리케이션이 단말에 다운로드 될 때 .cab 설치파일과 함께 포함되어 설치되고, 설치된 후 특정 웹 서버에 접속하여 Infojack의 나머지 부분을 다운로드하여 재설치한다. 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 또 다른 악성코드로는 Flexispy, PBStealer가 있다. Flexispy는 스파이웨어 형태의 상용 악성코드로써 스마트폰의 전화기록, 문자메시지 내용을 특정 웹 서버로 전송하는 기능을 가지고 있다.

5. 크로스 플랫폼형 악성코드

모바일 단말을 통해 PC를 감염시키는 공격 유형이다. 2005년에 발생된 Cardtrap.A가 최초의 크로스 플랫폼형 악성코드로써 폰의 메모리 카드에 윈도웜을 복사하여, 감염된 폰 메모리 카드를 PC에 장착했을 때 autorun를 통해 PC를 자동으로 감염시켜 데이터를 삭제하거나 성능을 저하시킨다. 모바일 기기간의 확산이 아닌 모바일 기기에서 PC를 감염시킨다는 점에서 새로운 형태의 공격 유형이라 할 수 있다.

Ⅳ. 스마트폰 보안 기술

2009년 초 WIPI 폐지가 스마트폰 시장의 활성화에 기여하였지만, 현재 WIPI 폐지에 따른 국내 스마트폰 보안 취약점 및 위협에 대한 보안 기술 개발의 준비가 미비한 상태이다. 스마트폰 보안 기술은 PC 환경과 다르게 백신, 방화벽 등과 같은 단품형 기술을 적용하기에는 한계가 있다. 또한, 다양한 OS별 스마트폰 출시와 개방 정도의 차이 등으로 인해 각기 특성에 맞는 보안 소프트웨어 적용이 요구된다. 특히, 국내의 경우에는 인터넷 보안 서비스 환경이 ActiveX를 통해 대부분 이뤄지고 있기 때문에 스마트폰을 이용한 안전한 결재 서비스에 어려움이 있으며 PC 환경과 다르게 보안 서비스도 제한적으로 지원할 수 밖에 없는 실정이다.

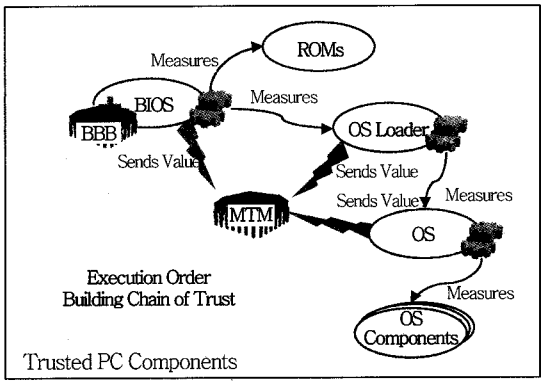
안전한 스마트폰 서비스 환경을 보장하고 향후 발생 가능한 보안 위협에 대해 선제적 방어 체계를 구축하기 위해서는 단말 내부 보안기술과 더불어 원격 보안 관리, 안전한 결재 서비스 지원 및 앱스토어를 통해 배포되는 모바일 애플리케이션 검증 등의 기술이 필요하고, 국내외적으로 기술 초기 단계에 있는 스마트폰 서비스 보안 인프라 기술 개발이 요구된다.

1. 스마트폰 단말 보안 기술

사용자의 부주의로 인한 시스템(노트북, 휴대 단말 등) 분실 혹은 외부 제 3자에 의한 시스템 도난 등을 통해 단말 복제, 도청 및 악용, 단말의 프라이버시 데이터 보호 위협, 악성 코드 삽입 등의 보안 위협은 여전히 해결되지 않은 숙제로 남아 있다.

일반적으로 소프트웨어는 하드웨어에 비해 쉽게 조작될 수 있기 때문에 물리적 보안성을 제공해주는 MTM을 이용하여 외부 공격으로부터 데이터, 키, 인증서 등을 안전하게 보호하고, 스마트폰 단말 플랫폼의 무결성 검증을 통해 악성 코드 실행을 사전에 탐지하여 차단함으로써 보다 향상된 보안 기능을 제공할 수 있다[7].

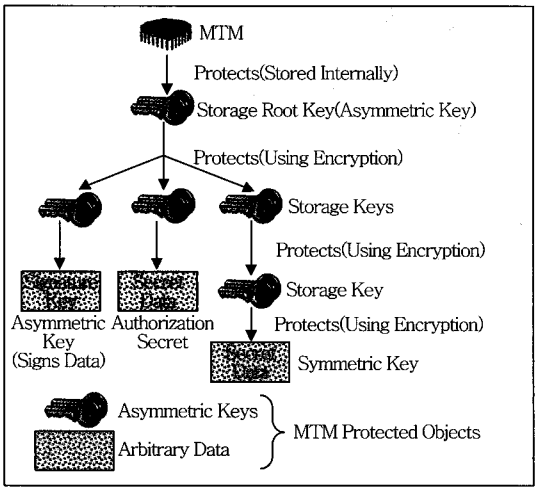
Root of trust 기능을 제공해주는 MTM은 tamper-resistant 컴포넌트로써 데이터를 안전하게 저장하는 RTS, 시스템 상태를 신뢰할 수 있는 방법으로 증명하는 RTR 역할을 담당하며, 시스템의 상태를 PCR에 기록하는 RTM 역할은 CRTM이 담당한다. CRTM은 power-on 시에 가장 먼저 실행되고, 항상 신뢰할 수 있는 컴포넌트로 PC의 경우 BIOS에 포함될 수 있으며 임의로 수정할 수 없는 특징을 갖는다[8],[9].



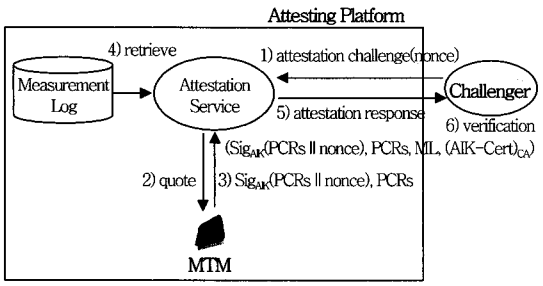
(그림 2) MTM의 Chain of Trust 과정

(그림 2)는 스마트폰 단말 플랫폼의 무결성 측정 과정을 보여준다. 단계별로 이루어지는 각 컴포넌트별 무결성 측정 과정은 chain of trust라고 보통 불리는데 일례로, CRTM이 BIOS의 무결성을 측정하고 결과 값을 검사하여 안전하다고 판단되면 MTM에 결과 값을 저장한 후 제어권을 BIOS에 넘긴다. 이후 BIOS는 동일한 방법으로 메모리, OS 등의 무결성을 측정하고 결과 값을 검사한 후 이상이 없을 경우 MTM에 결과 값을 저장한 후 제어권을 OS에 넘긴다. 이와 같은 무결성 검증 기능을 통해 OS 로드 후 MTM이 탑재된 스마트폰 상에서 악성 모바일 응용 프로그램을 실행하려 할 때, 별도의 IMVA agent가 항상 동작하면서 RIM certificate를 이용하여 해당 응용 프로그램의 무결성을 측정하고 검증하기 때문에 악성 코드 및 바이러스, 불법 프로그램들은 스마트폰상에서 실행될 수 없게 된다[10],[11].

또한, MTM은 중요한 데이터 및 키를 외부로 절대 유출시키지 않으며, MTM 내에 데이터나 키를 저장할 수 있는 공간이 부족할 경우 SRK를 이용하여 MTM 외부에 중요한 데이터나 키 값을 저장하는 protected storage 기능을 제공한다. (그림 3)을 보면 모든 key는 parent key로 암호화되어 계층적 구조 형태로 저장되며, 특정 key를 사용하기 위해서는 해당 key와 parent key가 MTM 내의 key slot으로 로딩된 후 해당 키를 MTM 내에서 복호화 한다. 즉, SRK의 private 값은 MTM 외부로 절대 유출되지 않기 때문에 MTM 내에 안전하게 저장되어 있는



(그림 3) MTM의 Protected Storage 구조



(그림 4) Remote Attestation

SRK를 통해 MTM 외부에 데이터나 키 값을 보다 안전하게 저장하여 사용할 수 있다[12].

플랫폼이 신뢰할 수 있는 상태임을 다른 플랫폼에게 증명하기 위해 사용되는 remote attestation 과정은 (그림 4)와 같다. Challenger는 remote attestation 과정을 통해 신뢰할 수 있는 MTM이 스마트폰 플랫폼에 장착되어 있으며, 현재 증명하고자 하는 스마트폰 플랫폼의 상태가 안전한지를 Privacy-CA와 AIK 및 AIK certificate를 이용하여 검증할 수 있다[8],[9].

결론적으로, 앞서 기술한 MTM의 무결성 측정 및 검증 기능, protected storage를 통해 스마트폰 단말 보안 기능을 강화하고, remote attestation을 통해 MTM이 장착된 플랫폼들간의 플랫폼 보증을 통해 보다 안전하고 신뢰할 수 있는 무선 네트워크 환경을 구축할 수 있을 것이다.

2. 스마트폰 보안 관리 기술

원격 보안 관리 기술은 단말 관리 프로토콜을 사용하여 모바일 단말의 보안기능을 원격에서 제어하고 관리하는 기술이다. 이를 위해 모바일 서비스 표준화 단체인 OMA에서 정의한 DM 프로토콜을 사용할 수 있다. DM 프로토콜은 두 통신 상대가 장치 관리 서비스를 제공하는 서버와 장치 관리 서비스를 받아 처리하는 클라이언트 관계를 갖는 프로토콜이다. 장치 관리 서버의 역할은 클라이언트에게 장치 관리 명령을 요청하고, 클라이언트는 주어진 명령을 수행한다.

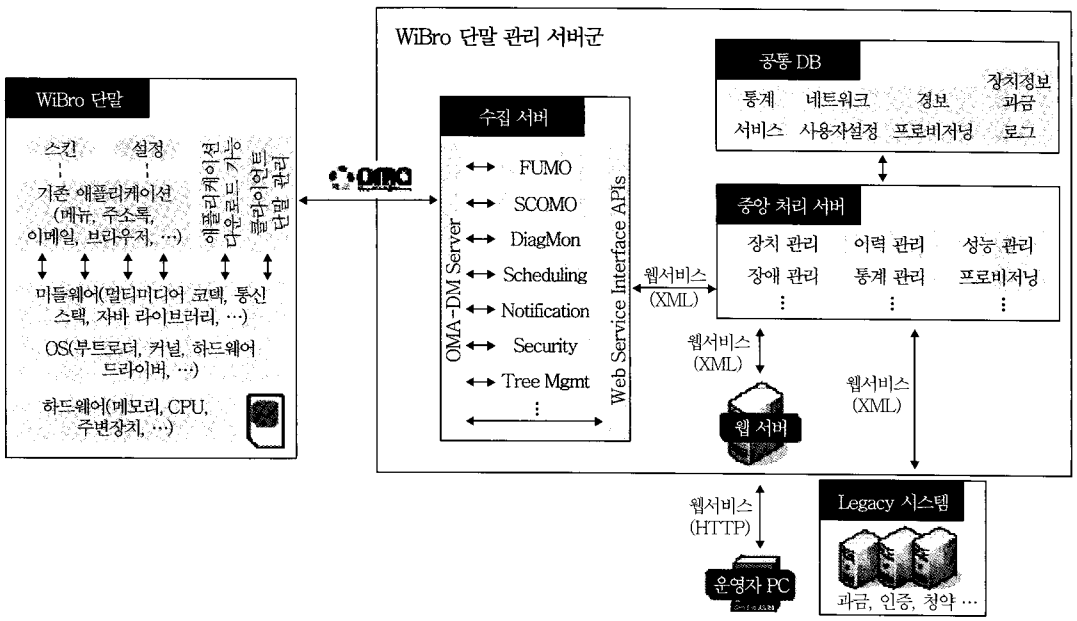
(그림 5)는 WiBro 단말 관리 시스템 구성도의 예를 보이고 있다[13].

현재 OMA DM은 단말 잠금과 데이터 삭제 기능을 정의하고 있다. 따라서, 이러한 기능을 스마트폰에 적용할 경우 보안 관리적 측면에서 장치 관리 서버는 스마트폰 보안 관리 서버의 역할을 담당하고, 클라이언트는 스마트폰에 설치하여 다양한 원격 보안 관리 서비스를 제공할 수 있다. OMA DM 프로토콜은 HTTP, Wireless Session Protocol, OBEX 등의 전송 프로토콜과 바인딩 규격들이 마련되어 있으므로 산업계 인터넷 표준인 Web 환경, WAP 환경, 블루투스 환경에서 프로토콜 메시지 전송이 가능하다.

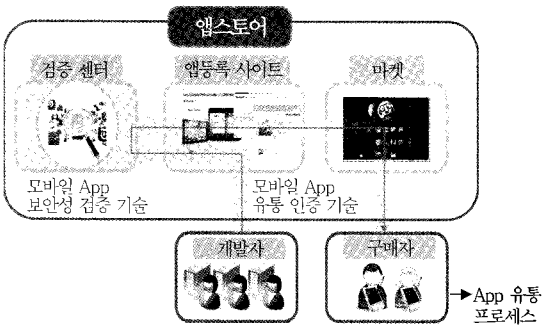
3. 앱스토어 보안 기술

개방형 모바일 환경의 변화 및 개방형 플랫폼 도입으로 스마트폰 기술 및 시장에 많은 변화가 이뤄지고 있고, 개방형 모바일 단말에 일부 악의적인 개발자가 악성코드가 포함된 프로그램을 제작 및 유포해서 단말에 침해를 가하거나 개인정보를 습득할 수 있는 위협이 발생되고 있다. 현재 대부분의 앱스토어에서는 등록된 애플리케이션의 심의 및 안정성 검증을 수동으로 진행하거나 보안을 위한 검증 절차가 이뤄지지 않고 있다. 이로 인해 앱스토어를 통해 다운로드받은 애플리케이션에 악성코드가 존재하는지 확인하는 데 한계가 있다. 실제 정보유출 공격을 수행하는 악성코드가 인터넷 뱅킹 관련 애플리케이션으로 은닉되어 앱스토어에 등록 및 배포된 사례가 발생되었다.

앱스토어에 애플리케이션을 등록하고 배포시, 애



(그림 5) WiBro 단말 원격 관리 구조 예



(그림 6) 앱스토어 보안 기술

플리케이션의 안전성을 확보하기 위해서는 모바일 애플리케이션의 유통 인증 기술과 앱스토어에 등록된 애플리케이션에 대한 보안 검증 기술의 적용이 요구된다((그림 6) 참조).

모바일 애플리케이션의 유통 인증 기술은 애플리케이션이 앱스토어에 등록되어 구매자에게 전달되기까지 유통자 증명을 제공하는 기술로써 이를 위해 코드 사이닝(code signing) 기술을 적용하고 있다. 개발자는 개발한 모바일 애플리케이션의 신원증명을 위해 인증서로 코드 사이닝하여 앱스토어에 등록하고 앱스토어에서는 해당 애플리케이션에 대한 신원증명을 확인하여 개발자 확인 절차를 수행한다. 일부 앱스토어에서는 공인인증서를 통한 코드 사이닝을 적용하고 있지만 자가 서명(self signing)이나 코드 사이닝을 적용하지 않는 앱스토어가 대부분이다. 따라서, 개발자 신원 증명 부재에 따른 악성코드 유포자의 확인이 불가능한 사례가 발생되고 있다. 개발자의 신원증명을 위해서는 공인인증서를 이용한 애플리케이션 코드 사이닝 기법을 적용하여 개발자 신원 증명 절차가 요구된다.

모바일 애플리케이션 보안 검증 기술은 앱스토어에 등록된 애플리케이션에 대해서 마켓 등록 전에 검증 센터에서 보안성 검사를 통해 애플리케이션의 안전성 여부를 확인하는 절차를 의미한다. 검증센터에서는 애플리케이션에 대해서 역공학(reverse engineering) 기법 및 가상 시험을 통해 보안성 검사를 진행하여 애플리케이션의 이상 유무를 확인하는 절차를 수행한다.

4. 스마트폰 전자결제 기술

온라인 상에서 주로 사용되는 결제 수단은 신용카드, 무통장 입금, 실시간 계좌이체, 휴대폰 결제 등이다. 이러한 결제 수단 중 무통장 입금이나 휴대폰 결제는 스마트폰에서도 쉽게 적용될 수 있다. 그러나 스마트폰에서 신용카드의 사용이나 실시간 계좌이체는 공인인증서 사용의 문제로 인하여 최근까지 본격적으로 활성화되지 못했는데, 이는 전자금융거래에서 30만 원 이상 거래금액일 때 공인인증서를 사용해야 하는 의무 규정이 준수되어야 했기 때문이다.

현재 국내 대부분의 웹 사이트에서는 공인인증서를 통한 전자서명을 지원하기 위해 쉽게 구현하여 사용할 수 있는 ActiveX 기술을 이용하여 전자서명을 제공하고 있다. 이 기능은 웹 브라우저의 플러그인 형태로 동작하게 된다. 그러나 이러한 방식은 국내 전자거래 환경이 MS의 기술에 종속되는 결과를 가져왔다는 논란을 야기하였다. 스마트폰이 확산됨에 따라 오픈웹 등에서는 전자결제를 위한 보안 기술로 기존의 공인인증서를 이용한 전자서명 기술뿐만 아니라, SSL과 OTP를 이용하는 기술도 사용할 수 있도록 해줄 것을 요구한다[14].

이에 따라 방송통신위원회 등에서 전자금융 거래시 공인인증서 이외에도 '공인인증서와 동등한 수준의 안전성'이 인정되는 보안방법을 도입할 수 있도록 하였다[15]. 이에 따르면, 30만 원 이상의 전자거래에서는 공인인증서나 또는 공인인증서에 준하는 안전성을 평가 받은 기술이 사용될 수 있으며, 30만 원 미만의 소액 결제에 대해서는 공인인증서를 사용하지 않아도 된다. 이에 따라 스마트폰을 이용한 전자거래시 기존 공인인증서뿐만 아니라 다양한 보안 기술이 전자결제시 활용될 것으로 보인다.

현재 국내에서는 하나은행이 최초로 아이폰에서 동작하는 스마트폰 뱅킹을 구현하였으며, 이에 대한 대응으로 타 은행들의 경우 은행권 공용 애플리케이션을 개발하고 있는 상황이다. 최근에는 은행권 공용 애플리케이션과는 별도로 각 은행별로 스마트폰

(그림 7) 우리은행 스마트폰 뱅킹 애플리케이션

뱅킹 애플리케이션을 개발하고 있다.

(그림 7)은 우리은행에서 개발한 스마트폰 뱅킹 애플리케이션을 보인다.

이외에도 예스24 등과 같은 인터넷 전자상거래 웹 사이트들의 경우 스마트폰에서 신용카드결제가 가능한 모바일 안심클릭 서비스를 제공하고 있다. 최근에는 NFC를 탑재하는 스마트폰에 신용카드를 발급하여 비접촉식으로 대금을 지불할 수 있는 결제 기술도 개발중에 있다.

그러나 현재 개발되고 있는 스마트폰 전자결제 기술은 초기단계 상태로 스마트폰에서 사용자가 전자결제 기능을 사용할 수 있도록 해주는 데 초점이 맞추어져 있다. 또한 전자결제 기술들이 상호 독립적으로 개발되고 있어 결제 기술은 사용자에게 일관된 경험을 제공하지 못해 혼란과 불편을 가중시킬 수 있다.

따라서 향후 개발될 스마트폰 전자결제 기술은 사용자의 개인 행동 패턴에 기반하여 최적의 결제 수단을 자동으로 선택해주는 기능을 제공할 필요가 있으며, 전자결제 기술로 공인인증서뿐만 아니라 이에 준하는 다양한 보안 기술을 통합적으로 제공하여 전자결제 애플리케이션의 특성에 맞는 보안 기술이 자동으로 제공될 수 있도록 해야 한다.

V. 결론

지금까지 스마트폰 보안 위협 요소와 모바일 악성코드 동향을 살펴보고 이들 위협에 대응하기 위한 단말 및 모바일 보안 인프라 기술들을 소개하였다.

스마트폰 확산에 따른 무선 인터넷, 앱스토어를 이용한 애플리케이션 활용 및 모바일 전자결제 서비스 등 급격한 환경변화에 맞춰 보안위협 및 장애요인에 대응하기 위해서는 정부와 산학연간의 종합적이고 체계적인 대응 방안이 요구된다.

안전한 스마트폰 서비스 환경을 보장하고 향후 발생 가능한 보안 위협에 대해 선제적 방어 체계를 구축하기 위해서는 단말 내부 보안기술과 더불어 원격 보안 관리, 안전한 결제 서비스 지원 및 앱스토어를 통해 배포되는 모바일 애플리케이션에 대한 검증 기술이 요구된다. 국내외적으로 기술 초기 단계에 있는 스마트폰 서비스 보안 인프라 기술은 스마트폰 서비스 산업 활성화를 도모할 수 있을 것으로 예상된다.

● 용 어 해 설 ●

코드 사이닝(Code Signing): 실행 가능한 코드의 변조 방지 및 서명자 인증을 위한 전자 서명 기술

MTM(Mobile Trusted Module): TCG 그룹에서 표준화가 진행중인 모바일 플랫폼용 신뢰보안모듈

약어 정리

AIK	Attestation Identity Key
CRTM	Core Root of Trust for Measurement
DM	Device Management
IMVA	Integrity Measurement and Verification
MTM	Mobile Trusted Module
NFC	Near Field Communication
OBEX	Object Exchange
OMA	Open Mobile Alliance
OTP	One Time Password
PCR	Platform Configuration Register
RIM	Reference Integrity Metric

RTM	Root of Trust for Measurement
RTR	Root of Trust for Reporting
RTS	Root of Trust for Storage
SRK	Storage Root Key
SSL	Secure Socket Layer

참 고 문 헌

[1] 김기영, 강동호, "개방형 모바일 환경에서 스마트폰 보안 기술," 정보보호학회지, 제19권 5호, 2009. 12.

[2] 모바일 악성코드 침해 대응 가이드, KISA 2009.

[3] KISA, "인터넷 & 시큐리티 이슈," 2010. 3.

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

[5] DAI-Labor, "Malicious Software for Smartphones," Technical Report, 2008.

[6] Ken Dunham, "Mobile Malware Attacks and Defense," SYNGRESS 2009, 2009.

[7] Trusted Computing Group: TCG Specification Architecture Overview. Specification Revision 1.4, Aug. 2, 2007, http://www.trustedcomputinggroup.org

[8] Trusted Computing Group: TCG Mobile Reference Architecture. Specification version 1.0, Revision 1, June 12, 2007, http://www.trustedcomputinggroup.org

[9] Trusted Computing Group: TCG Mobile Trusted Module Specification. Specification version 1.0, Revision 1, June 12, 2007, http://www.trustedcomputinggroup.org

[10] Reiner Sailer, Xiaolan Zhang, Trent Jaeger, and Leendert van Doorn: Design and Implementation of a TCG-based Integrity Measurement Architecture, *13th Usenix Security Symp.*, Aug. 2004.

[11] Siani Pearson: How Trusted Computers Can Enhance Privacy Preserving Mobile Applications, *Sixth IEEE Int'l Symp. on a World of Wireless Mobile and Multimedia Networks*, June, 2005.

[12] Trusted Computing Group: TCG Software Stack. Specification version 1.2, Mar. 7, 2007, http://www.trustedcomputinggroup.org

[13] 이지은 외 2인, "OMA DM 기반의 휴대인터넷 단말 관리 시스템," KNOM Review, Vol.10, No.2, 2007.

[14] http://openweb.or.kr/

[15] http://kcc.korea.kr/