모바일 보안 위협 및 보안 서비스 기술 동향

한국전자통신연구원 ▌강동호 · 김정녀 · 조현숙

1. 모바일 보안 서비스의 필요성

현재 3세대 이동통신의 발달과 이를 활용한 풍부한 모바일 애플리케이션을 제공하고 있는 스마트폰의 성장으로 인해 인터넷 서비스 이용률이 테스크탑에서 모바일 단말로 전환되고 있다. 모바일 서비스를 지원하는 모바일 단말의 진화 과정을 살펴보면 1세대에 아날로그방식의 음성 통화를 목적으로 한 기본적인 폰 기능에서 2세대에 디지털방식으로 전환되면서 음성 통화 및 SMS와 같은 소량의 데이터 전송이 가능한 데이터 서비스를 지원하였다. 현재 지원하고 있는 3세대 이동 통신은 음성, 데이터 및 영상 등을 고속으로 주고받을 수 있는 멀티미디어 통신 서비스를 지원하고 있다. 3세대 이동통신 기술을 지원하는 모바일 단말은 일반폰과 스마트폰으로 구분할 수 있고, 하드웨어적인 면에서 유사한 특징을 가지고 있다. 하지만, 모바일 서비스를 지원하는 범용 OS 및 모바일 애플리케이션을 포함하는 소프트웨어 플랫폼은 많은 차이가 있다.

최근 스마트폰의 등장과 성장에 따라 모바일 소프트웨어 플랫폼에 대한 관심이 증가하고 있다. 또한, 아이폰과 앱스토어의 성공은 스마트폰에서 사용될 애플리케이션에 대한 관심을 한층 끌어올리고 있다. 하지만,

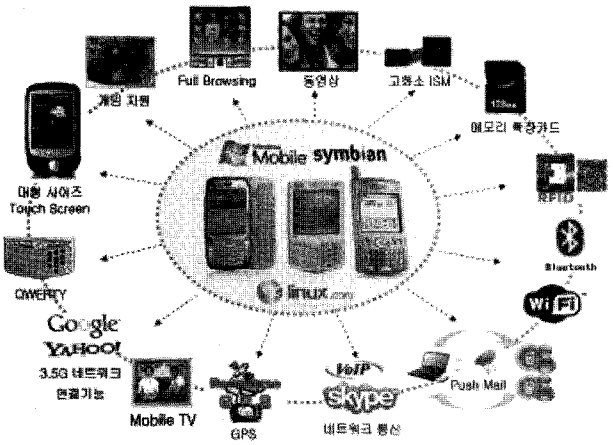


그림 1 스마트폰을 활용한 모바일 서비스[1]

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 피해가 증가할 것으로 예상된다[2]. 따라서 향후 더욱 지능화 되고 다양한 형태로 변형될 수 있는 악성코드 정보 유출, 불법 과금, 부정 사용등과 같은 보안 위협으로부터 모바일 단말 사용자를 보호하고, 활성화되고 있는 모바일 서비스 환경에 대한 안전성, 무결성, 가용성 및 신뢰성을 제공하기 위한 모바일 서비스 보안 기술 개발이 요구된다.

본 고에서는 모바일 서비스를 지원하는 모바일 단말의 보안 위협 요소 살펴보고 이들 위협에 대응하기 위한 모바일 보안 서비스 기술들을 소개 하고자 한다.

2. 모바일 보안 위협

2.1 모바일 범용 OS 보안 취약점

모바일 단말이 일반폰에서 스마트폰으로 발전되어 감에 따라 모바일 플랫폼의 개발이 가속화되어 노키아는 심비안, MS는 윈도우즈 모바일, 애플은 아이폰, 구글은 안드로이드 플랫폼을 모바일 단말에 적용하고 있다. 이들은 기본적으로 일반폰 보다 성능적으로 우수하고, 개방형 환경에 따라 자체적으로 애플리케이션을 개발하는 폐쇄형 구조에서 모든 개발자에게 표준화된 개발환경을 제공하는 공개형 구조로 발전하고 있다. 모바일 범용 OS의 특징에 따른 보안 위협은 다음 그림 2와 같다.

안드로이드와 같은 개방형 플랫폼을 탑재한 단말의 등장은 제조사들에게 플랫폼의 단말 적용 편의성을 제공하지만 플랫폼 소스 공개에 따른 보안 취약점 노출 위협이 증대될 수 있다. 또한, 앱스토어를 통한 애플리케이션 유통은 구매자와 개발자간에 애플리케이션 유통 편의성을 제공하지만 악성코드가 포함된 애플리케이션을 보안성 검증 절차가 미비한 앱스토어에 올려 악

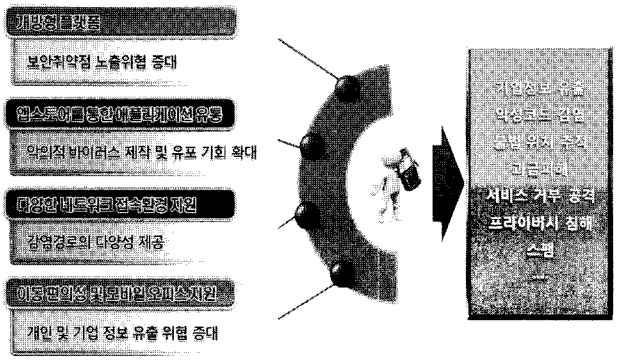


그림 2 모바일 범용OS 특징에 따른 보안 위협

의적인 바이러스 제작 및 유포 기회가 확대될 수 있다. 다양한 네트워크 접속환경 지원은 네트워크를 활용한 다양한 서비스를 제공할 수 있지만 스마트폰의 다양한 네트워크(Wi-Fi, Bluetooth, HSDPA)등을 통한 감염 경로의 다양성을 제공할 수 있다. 또한, 이동 편의성 및 모바일 오피스 지원은 언제 어디서나 단말 사용자에게 모바일 서비스를 제공 받을 수 있지만 휴대성에 따른 분실/도난 및 모바일 오피스 지원에 따른 기업의 스마트폰 수요가 증가되어 개인 및 기업 정보 유출 위협이 증대 될 수 있다. 이러한 4가지 위협요소는 정보유출, 악성코드 감염, 불법 위치 추적, 과금 피해 및 금융사고 등의 피해를 유발시킬 수 있다.

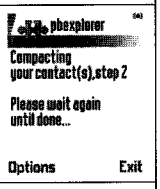
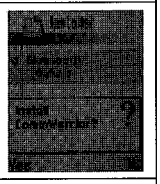
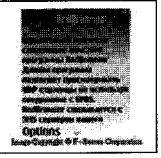
2.2 모바일 OS별 악성코드

모바일 악성코드는 스마트폰을 포함한 모바일 단말을 대상으로 정보유출, 단말 파괴, 불법 과금 등의 악의적인 행위를 수행하기 위한 프로그램으로 정의할 수 있다. 모바일 악성코드는 모바일 단말의 성장과 더불어 규모 면에서 빠르게 증가하고 있고, 위협요인도 다양화되고 있다. 모바일 악성코드가 증가하는 원인은 악의적인 목적을 가진 악성코드의 제작 및 유통이 가능한 개방형 단말기의 증가와 함께 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. 최근 스마트폰 이용 확산에 따라 시간과 장소에 구애 받지 않고 무선 인터넷을 활용한 모바일 서비스가 활성화 되면서 스마트폰의 보안 위협이 증대되고 있다. 본 절에서는 모바일 OS별 악성코드 동향을 살펴보고자 한다[3,4].

2.2.1 노키아의 심비안

심비안은 전세계에서 가장 많이 보급된 플랫폼이며 소스코드가 공개되어 있기 때문에 2004년 카비르(Cabir) 악성코드 등장이후 현재까지 가장 많은 모바일 악성코드가 발견된 플랫폼이다. 주요 악성코드를 보면 표 1과 같다.

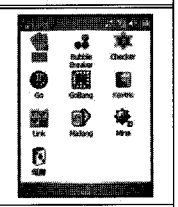
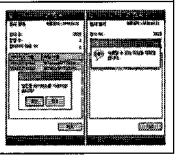
표 1 심비아 악성코드

악성코드	특징	감염증상
Skulls (2004)	· 단말 장애형 악성코드 · 애플리케이션 삭제 및 재부팅 시도	
Cardblock (2005)	· 단말 장애형 악성코드 · 애플리케이션 및 데이터 삭제 시도	
PBstealer (2005)	· 정보 유출형 악성코드 · Phonebook Stealer · 전화번호 유출 시도	
Commwarrior	· 과금 유발형 악성코드 · 주소록 연락처를 이용한 MMS 메시지 전송 시도	
RedBrowser	· 과금유발형 악성코드 · 프리미엄 메시지 전송 시도	

2.2.2 MS의 윈도우 모바일

2009년 WIPI 의무화 해제와 국내 스마트폰 확산에 따라 모바일 보안 위협이 증가하고 있는 상황에서 국내 첫 스마트폰 악성코드가 윈도우 모바일 OS에서 발견되었다. 향후, 국내에도 다양한 모바일 환경에서 악성코드 감염 피해가 증가할 것으로 예상된다.

표 2 윈도우 모바일 악성코드

악성코드	특징	감염증상
Infojack (2008)	· 정보유출형 악성코드 · 단말 보안설정 변경 및 단말 정보 전송 시도	
TredDial (2010)	· 과금유발형 악성코드 · 국내 최초의 스마트폰 악성코드 · 50초마다 국제전화 시도	

2.2.3 애플의 아이폰 OS

국내 아이폰의 등장은 스마트폰 및 모바일 서비스 시장 활성에 기여하고 있아이폰은 다른 모바일 단말에 비해 풍부한 애플리케이션을 앱스토어를 통해 이용할 수 있다. 정상적인 아이폰은 애플리케이션을 앱스토어에서 구입하지만 탈옥 아이폰은 씨디아(Cydia) 스토어를 통해 애플이 거부한 애플리케이션과 다양한 부가 기능을 내려 받아 설치 할 수 있기 때문에 전세계적으로 아이폰을 탈옥하는 비율이 증가하고 있다. 이를 통한 보안 위협은 증가하고 있다. 2009년부터 탈옥(Jailbroken) 아이폰에 대해 3건의 해킹 피해 사례가 등장하였다.

표 3 아이폰 OS 악성코드

악성코드	특징	감염증상
ikee (2009)	· 탈옥(Jailbroken) 단말 · 배경 화면을 유명 가수 사진으로 변경	
Privacy.A (2009)	· 정보유출형 악성코드 · 탈옥(Jailbroken) 단말 · 개인정보(문자메시지, 이메일 등) 유출 시도	
iBotNet (2009)	· 단말 장애형 악성코드 · 탈옥(Jailbroken) 단말 · DDOS공격을 위한 좀비 단말에 활용	

2.2.4 구글의 안드로이드

2010년 가트너가 발표한 안드로이드 보안 평가 자료에 따르면 안드로이드는 개방형 OS 지원에 따른 시스템 자원 및 서비스에 대한 불법적 접근이 가능한 프레임워크 취약점이 존재하고, 개발자 검증 기능이 없어 애플리케이션의 취약점이 존재하고 있다고 평가하였다. 이와 같은 평가는 결국 앱스토어 환경에서 악성코드가 은닉된 애플리케이션의 유포 가능성을 보여주고 있다.

표 4 안드로이드 악성코드

악성코드	특징	감염증상
악성코드 은닉 애플리케이션 (Royal Bank of Canada)	· 정보유출형 악성코드 · 모바일 뱅킹 프로그램으로 가장하여 정보 유출	

3. 모바일 보안 기술

2009년초 WIPI 폐지가 모바일 서비스 시장의 활성화에 기여하였지만, 현재 WIPI 폐지에 따른 국내 모바일 서비스 보안 취약점 및 위협에 대한 보안 기술 개발의 준비가 미비한 상태이다. 모바일 보안 기술은 PC환경과 다르게 백신, 방화벽 등과 같은 단품형 기술을 적용하기에는 한계가 있다. 또한, 다양한 OS별 모바일 단말 출시 와 개방 정도의 차이 등으로 인해 각기 특성에 맞는 보안 S/W 적용이 요구된다. 특히, 국내의 경우 인터넷 보안 서비스 환경이 액티브엑스를 통해 대부분 이뤄지고 있기 때문에 모바일 단말을 이용한 안전한 결제 서비스에 어려움이 있으며 PC 환경과 다르게 보안 서비스도 제한적으로 지원 할 수 밖에 없는 실정이다. 안전한 모바일 서비스 환경을 보장하고 향후 발생 가능한 보안 위협에 대해 선제적 방어 체계를 구축하기 위해서는 단말 내부 보안기술 과 더불어 원격 보안관리, 안전한 결제 서비스 지원 및 앱스토어를 통해 배포되는 모바일 애플리케이션에 대한 검증을 통해 국내외적으로 기술 초기 단계에 있는 모바일 보안 기술의 개발이 요구된다. 본 장에서는 안전한 모바일 서비스 지원을 위한 주요 모바일 보안 기술에 대해서 살펴보고자 한다.

3.1 MTM 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, 악성코드 삽입 등의 보안 위협은 여전히 해결되지 않은 숙제로 남아있다.

일반적으로 소프트웨어는 하드웨어에 비해 쉽게 조작될 수 있기 때문에 물리적 보안성을 제공해주는 MTM (Mobile Trusted Module)을 이용하여 외부 공격으로부터 데이터, 키, 인증서 등을 안전하게 보호하고, 스마트폰 단말 플랫폼의 무결성 검증을 통해 악성코드 실행을 사전에 탐지하여 차단함으로써 보다 향상된 보안 기능을 제공할 수 있다[5].

Root of Trust 기능을 제공해주는 MTM은 Tamper-resistant 컴포넌트로써 데이터를 안전하게 저장하는 RTS(Root of Trust for Storage), 시스템 상태를 신뢰할 수 있는 방법으로 증명하는 RTR(Root of Trust for Reporting) 역할을 담당하며, 시스템의 상태를 PCR(Platform Confi-guration Register)에 기록하는 RTM(Root of Trust for Measurement) 역할은 CRTM(Core Root of Trust for Measurement)이 담당한다. CRTM은 Power-on 시에

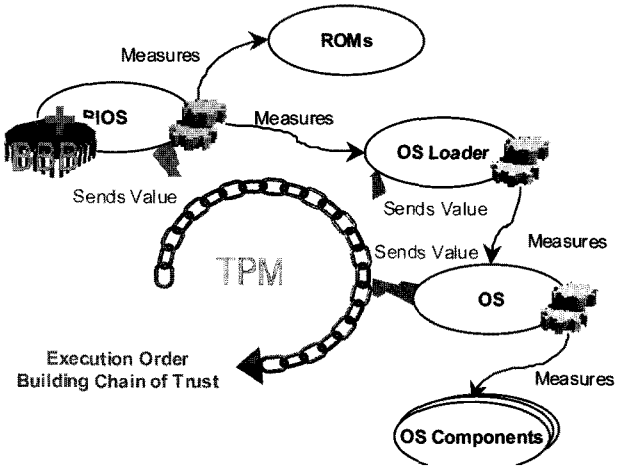


그림 3 MTM의 Chain of Trust 과정

가장 먼저 실행되고, 항상 신뢰할 수 있는 컴포넌트로 PC의 경우 BIOS에 포함될 수 있으며 임의로 수정할 수 없는 특징을 갖는다[5,6].

그림 3은 모바일 단말 플랫폼의 무결성 측정 과정을 보여주고 있다. 단계별로 이루어지는 각 컴포넌트 별 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 모바일 단말에서 악성코드가 실행되려 할 때, 별도의 IMVA(Integrity Measurement and Verification) 에이전트가 항상 동작하면서 RIM(Reference Integrity Metric) Certificate를 이용하여 해당 응용 프로그램의 무결성을 측정하고 검증하기 때문에 악성 코드는 모바일 단말에서 실행될 수 없게 된다[7,8].

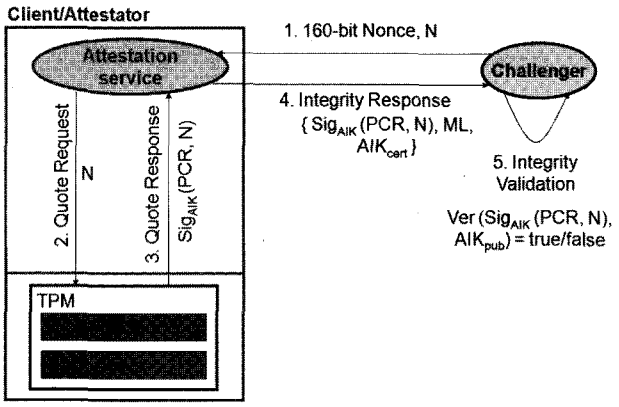


그림 4 Remote Attestation

플랫폼이 신뢰할 수 있는 상태임을 다른 플랫폼에게 증명하기 위해 사용되는 remote attestation 과정은 그림 4와 같다.

Challenger는 remote attestation 과정을 통해 신뢰할 수 있는 MTM이 스마트폰 플랫폼에 장착되어 있으며, 현재 증명하고자 하는 스마트폰 플랫폼의 상태가 안전한지를 Privacy-CA와 AIK (Attestation Identity Key) 및 AIK certificate 을 이용하여 검증할 수 있다[5,14].

결론적으로, 앞서 기술한 MTM의 무결성 측정 및 검증 기능을 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 것으로 예상된다.

3.2 모바일 단말 원격 보안 관리 기술

원격 보안관리 기술은 단말관리 프로토콜을 사용하여 모바일 단말의 보안기능을 원격에서 제어하고 관리하는 기술이다. 이를 위해 모바일 서비스 표준화 단체인 OMA(Open Mobile Alliance)에서 정의한 DM(Device Management) 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 수행하고, 클라이언트는 주어진 명령을 수행한다.

현재 OMA DM에 정의된 보안기능은 단말 잠금 과 데이터 삭제 기능을 정의하고 있다. 하지만 보안 관리적 측면에서 장치 관리 서버는 스마트폰 보안 관리 서버의 역할을 담당하고, 클라이언트는 스마트폰에 설치하여 다양한 원격 보안관리 서비스를 제공할 수 있다. OMA DM 프로토콜은 HTTP, Wireless Session Protocol, OBEX(Object Exchange)등의 전송 프로토콜 등과의 바인딩 규격들이 마련되어 있으므로 산업계 인터넷 표준인 Web환경, WAP환경, 블루투스 환경에서 프로토콜 메시지 전송이 가능하다.

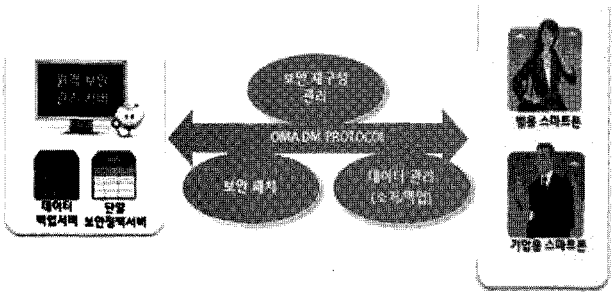


그림 5 원격보안 관리 개념도

3.3 앱스토어 보안 기술

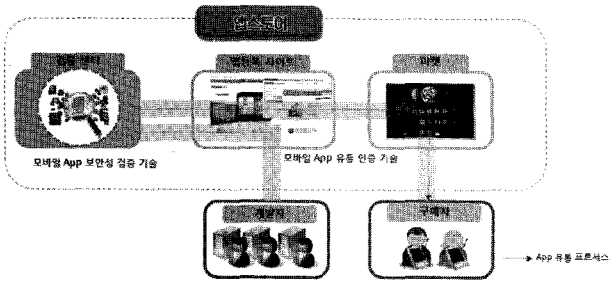


그림 6 앱스토어 보안 기술

앱스토어에 애플리케이션을 등록하고 배포 시, 애플리케이션의 안전성을 확보하기 위해서는 모바일 애플리케이션의 유통 인증 기술과 앱스토어에 등록된 애플리케이션에 대한 보안 검증 기술의 적용이 요구된다.

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 필요하다. 모바일 애플리케이션 보안 검증 기술은 앱스토어에 등록된 애플리케이션에 대해서 등록 전에 검증 센터에서 보안성 검사를 통해 애플리케이션의 안전성 여부를 확인하는 절차를 의미한다. 검증센터에서는 보안성 검사를 진행하여 애플리케이션의 이상 유무를 확인하는 절차가 필요하다.

3.4 모바일 전자결제 기술

온라인 상에서 주로 사용되는 결제 수단은 신용카드, 무통장 입금, 실시간 계좌이체, 휴대폰 결제 등이다. 이러한 결제 수단 중 무통장 입금이나 휴대폰 결제는 모바일 환경에서도 쉽게 적용될 수 있었다. 그러나 모바일단말에서 신용카드의 사용이나 실시간 계좌이체는 공인인증서 사용의 문제로 인해 최근까지 본격적으로 활성화되고 있지 못하고 있는 실정이었다. 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 대부분의 웹 사이트에서는 쉽게 구현할 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 해 줄 것을 요구하여 왔다[10].

이에 따라 방송통신위원회 등에서 전자금융 거래 시 공인인증서 이외에도 '공인인증서와 동등한 수준의 안전성'이 인정되는 보안방법을 도입할 수 있도록 하였다[11]. 이에 따르면, 30만원 이상의 전자거래에서는 공인인증서나 또는 공인인증서에 준하는 안전성을 평가받은 기술이 사용될 수 있으며, 30만원 미만의 소액 결제에 대해서는 공인인증서를 사용하지 않아도 된다. 이에 따라 모바일 단말을 이용한 전자거래 시 기존 공인인증서뿐만 아니라 다양한 보안 기술이 전자결제로 활성화 될 것으로 보인다.

현재 개발되고 있는 모바일 단말 전자결제 기술은 초기단계 상태로 사용자가 전자결제 기능을 사용할 수 있도록 해 주는데 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 모바일 전자결제 기술은 사용자의 개인행동 패턴에 기반하여 최적의 결제 수단을 자동으로 선택해주는 기능을 제공할 필요가 있다. 또한 전자결제 기술로 공인인증서뿐만 아니라 이에 준하는 다양한 보안 기술을 통합적으로 제공하여 전자결제 애플리케이션의 특성에 맞는 보안 기술이 자동으로 제공될 수 있도록 해야 한다.

4. 결 론

지금까지 모바일 보안 위협 요소와 모바일 악성코드 동향을 살펴보고 이들 위협에 대응하기 위한 모바일 보안 기술들을 소개하였다.

향후 모바일 서비스 시장은 소셜 네트워킹 기반 서비스 확대에 따라 개인의 불법적인 위치정보 노출 위

협에 직면해 있으며 모바일 오피스가 확대되면 기업 내부 정보의 유출 피해와 같은 신규 보안 위협에 노출되어 있다. 안전한 모바일 서비스 환경을 보장하고 향후 발생 가능한 보안 위협에 대해 대응 체계를 구축하기 위해서는 단말 내부 보안기술 과 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 기술은 모바일 서비스 산업의 저해요인을 제거하고 신규 모바일 서비스 활성화를 도모 할 수 있을 것으로 예상된다.

참고문헌

[1] KIEI, "휴대폰(스마트폰) 및. 부품/소재 기술 시장 분석 세미", 2009.

[2] KISA, "인터넷 & 시큐리티 이슈", 2010.03.

[3] 김기영, 강동호, "개방형 모바일 환경에서 스마트폰 보안 기술", 정보보호학회지 제19권 5호, 2009.12.

[4] 유지은, "스마트폰의 Key Enabler: 소프트웨어", SW Insight, 2009.04.

[5] Trusted Computing Group, "TCG Specifica- ation Architecture Overview. Specification Revision 1.4", August 2, 2007.

[6] Trusted Computing Group, "TCG Mobile Reference Architecture. Specification version 1.0, Revision 1", June 12, 2007.

[7] Trusted Computing Group, "TCG Mobile Trusted Module Specification. Specification version 1.0, Re- vision 1", June 12, 2007.

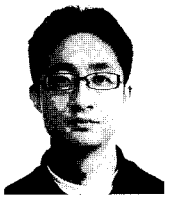
[8] Reiner Sailer, "Xiaolan Zhang, Trent Jaeger, Leen- dert van Doorn: Design and Implementation of a TCG-based Integrity Measurement Architecture", 13th Usenix Security Symposium, 2004.

[9] Siani Pearson, "How trusted computers can enhance privacy preserving mobile applications", Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, 2005.

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

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

약 력



강 동 호

1999 한남대학교 컴퓨터공학과 졸업
2001 한남대학교 컴퓨터공학과 석사
현재 한국전자통신연구원 보안관제연구팀 선임연구원
관심분야: 네트워크보안, 임베디드 보안 OS 등
E-mail: dhkang@etri.re.kr

김 정 녀

1987 전남대학교 전산통계학과 졸업
1996 OSF/RI 공동연구 파견(미국)
2000 충남대학교 컴퓨터공학과 석사
2004 충남대학교 컴퓨터공학과 박사
현재 한국전자통신연구원 휴먼인식기술연구팀장 책임연구원
관심분야 : 시스템·네트워크보안, 보안 OS, 바이오보안 등
E-mail : jnkim@etri.re.kr

조 현 숙

1979 전남대학교 수학교육과 졸업
2001 충북대학교 박사
현재 한국전자통신연구원 지식정보보안연구부장 책임연구원
관심분야 : 정보보안
E-mail : hscho@etri.re.kr