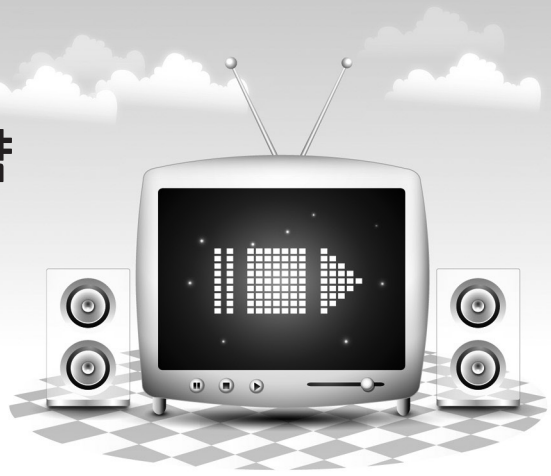
국내외 스마트폰 보안 표준화 동향 및 추진전략



염흥열 | 순천향대학교 정보보호학과 교수
장기헌 | 순천향대학교 정보보호학과

1. 머리말

스마트폰(smart phone)은 3G망은 물론 Wi-Fi, WiBro 등 다양한 인터페이스를 통해 시간과 장소의 제약 없이 인터넷을 이용할 수 있을 뿐만 아니라, 사용자의 요구에 따라 애플리케이션의 설치 및 삭제가 가능하다는 장점을 내세워 그 인기를 더해가고 있다. 최근에는 스마트폰을 이용하여 업무를 처리하는 스마트워크 및 스마트오피스가 주목 받고 있으며, 하나의 콘텐츠를 여러 개의 스크린으로 이용할 수 있는 N 스크린 시대를 위한 서비스 연동 연구가 활발히 진행되는 등 스마트폰은 사회 전반에 걸쳐 큰 관심을 불러일으키고 있다. 2010년 11월 기준 국내 스마트폰 사용자는 550만 명에 이르며, 2010년 말까지 670만 명을 넘어설 것으로 예측하고 있다.

이와 더불어, 스마트폰에서 이용할 수 있는 콘텐츠 · 앱 서비스도 급속히 증가하고 있다. 국내 최대 모바일 콘텐츠 장터인 SK텔레콤 'T스토어'에는 약 6만 개의 응용프로그램(애플리케이션)들이 올라와 있고, KT는 '올레마켓', LG U+는 '오즈(OZ)스토어'를 개설해 콘텐츠 시장을 조성하고 있다.

스마트폰의 보급과 활성화에 따라 기존 PC에서 발생하던 보안 위협이 스마트폰에서 발생하는 등 사회적으로 큰 파장을 일으키고 있다. 최근 보고된 대표적인 스마트폰을 대상으로 하는 악성코드 사례는 광고메시지에 숨어서 심비안 스마트폰 공격을 목표로 하는 중국발 악성코드가 있는 데, 이와 같은 악성코드는 스마트폰을 감염시켜 스마트폰 내에 저장되어 있는 주소록의 사람들에게 이를 또 다시 전파시켜 감염되게 한다는 점에서 그 심각성이 더해진다. 따라서 최근에는 스마트폰을 보호하고 안전하게 연동 사용이 가능케 하는 스마트폰 보안 표준에 대한 요구가 스마트폰 서비스 사업자와 보안 제품 사업자 등에서 나타나고 있다.

본 고에서는 스마트폰 보안 표준화를 다루고 국내외 표준화에 대한 추진전략을 제시하고자 한다. 본 고의 2장에서는 스마트폰 위협과 이 위협에 대한 대응 기술을 제시한다. 3장에서는 국내외 표준화 현황을 살펴보고, 4장에서는 스마트폰 표준화 추진 전략을 제시하며, 5장에서는 결론을 맺는다.

2. 스마트폰 위협 및 보안기술

스마트폰은 기존 PC에서 가지고 있던 위협과 모바일 기기의 위협을 모두 포함하고 있다. 다시 말하면, 다양한 기능이 추가된 만큼 기존 PC에서 나타났던 많은 위협들이 그대로 상속되며, 신규 서비스 부가로 인해 신규 위협도 늘어나고 있다. 위협은 발생 위치에 따라 네트워크상에서 발생할 수 있는 위협과 소프트웨어를 이용한 위협, 그외 물리적 위협 등으로 구분된다.

스마트폰에서 악성코드가 발생하는 이유는 스마트폰이 음성 통신뿐만 아니라 인터넷 통신도 가능하며, 초고속 무선 데이터 통신을 사용하게 됨에 따라 악성코드 전파가 더욱 쉬워졌음에 기인하다. 이 외에도 Wi-Fi 및 와이브로 등의 액세스 확대, 무선 브라우징 확대, 휴대폰 기기의 성능 향상, 휴대폰의 개인화 및 전자결재 지원, 공개 플랫폼 화 등은 악성코드 전파의 확대가 가능한 주요 요인으로 작동하고 있다.

악성코드는 스마트폰을 원격으로 제어하거나, 애플리케이션의 동작 변경, 파일 실행 차단, 불필요한 통신 요금 발생, 사용자 데이터 도난, SMS 훔쳐보기, 위치정보의 유출, 다른 악성코드의 설치 및 타 스마트폰으로의 전파 등의 리스크를 초래한다. 또한, GPS는 스마트폰에서 편리한 위치기반 서비스를 제공할 수 있지만 사용자의 위치정보가 노출될 위협이 존재하며, 특히 최근 이슈가 되었던 '오빠믿지' 애플리케이션의 경우 SMS를 통해 상대 위치 정보가 노출되어 개인 프라이버시 침해 논란을 일으켰다.

스마트폰 시장이 확대되면서 애플리케이션을 사고파는 시장인 애플리케이션 스토어(일명 앱스토어)가 대중화되고 있다. 기존의 모바일 애플리케이션과는 달

〈표 1〉 스마트폰 위협 및 보안기술

영역	위협	보안 기술
단말기 영역	· 애플리케이션 분석을 통한 악용 · 애플리케이션의 기능을 이용한 악용 · 음성 도청 · 분실 및 도난 · 공개된 Exploit 공격 · 패스워드 크랙 · 악성코드 · 애플리케이션 설치 동의 우회	· 애플리케이션 코드의 난독화 기술 적용 · 데이터의 암호화 · 도난 및 분실 방지 솔루션 · 정기적인 업데이트 · 안티 바이러스
네트워크 영역	· 데이터 스니핑 및 변조 · 모바일 VoIP에서의 기존 VoIP 취약점 적용 및 스니핑	· 데이터 암호화 · 방화벽, VPN · 디바이스 인증
Service 영역	· 애플리케이션 취약점을 이용한 악용 · 웹사이트를 통한 피싱 및 악성코드 다운로드 · 이메일을 통한 악성코드 첨부 및 스팸 메일 발송 · 내부망을 우회한 외부 정보 유출	· 스마트폰 안티바이러스 기술 · 첨부파일 필터링 · 스팸 메일 필터링 · 불법 AP 및 인터넷 사용 방지
PC, Memory 영역	· 스마트폰과 PC 연결을 통한 악성코드 전파 및 접근 · 외장 메모리를 이용한 악성코드 전파 · 개인 정보 유출 · AD-HOC을 통한 비인가된 접근	· 스마트폰 안티바이러스 기술 · 보안 저장 장치 · 개인정보 유출 방지 솔루션 · AD-HOC을 통한 접근 통제
애플리케이션 스토어 영역	· 악의적 개발자에 의한 악성 프로그램 유포 · 보안 메커니즘을 우회한 악성 프로그램 등록	· 전자서명 기술을 이용한 코드 서명 기술
GPS 영역	· GPS를 통한 위치 정보 노출	· 위치정보보호

리 스마트폰에서는 애플리케이션 스토어가 개방적이기에 개발자들은 애플리케이션을 개발해 자유롭게 배포할 수 있다. 통상 개인 개발자 혹은 프로그램 제작사나 통신회사에서 만든 애플리케이션들이 오픈마켓이라고 하는 애플리케이션 스토어에 등록되고, 사용자는 무료 혹은 비용을 지불한 뒤 다운로드 받아 설치하는 방식으로 작동한다. 하지만 이러한 콘텐츠가 만일 악성코드에 감염된 상태로 배포되어 사용자에게 전파 되거나 구매한 콘텐츠 설치 과정에서 웜, 바이러스 등에 감염된다면 심각한 보안위협이 발생할 여지가 있다. 애플리케이션 스토어 상에 저장된 데이터를 기한 없이 사용하기 위한 크랙 시도, 제작 툴을 이용한 커스텀 펌웨어 생성, 탈옥(Jailbreak)한 아이폰과 안드로이드의 루팅폰에 의해 불법 애플리케이션 다운로드 등은 대표적인 애플리케이션 스토어에 대한 보안 위협이다.

또 다른 스마트폰의 위협으로 개인정보 유출을 들 수 있다. 스마트폰의 경우 신상정보, 금융정보, 개인민감 정보 등 중요한 정보를 내부에 저장하고 있기에 개인정보를 노리는 공격에 쉽게 노출되어 있다. 특히, 스마트오피스의 활성화에 따라 기업의 기밀 정보까지 유출될 가능성이 존재한다. 앞으로 이와 같이 개인정보 침해 유형의 공격이 지능화 범죄화 될 것으로 예상되며, 불특정 다수의 대량 데이터 유출뿐만 아니라, 불특정 다수의 다종류의 소량 데이터 유출 및 범죄 악용가능성도 예상된다.

이외에도 스마트폰은 분실, 음성 도청 및 아이디와 패스워드 등의 개인 크리덴셜 유출 등의 많은 보안 위협이 존재한다.

다양한 스마트폰 보안 위협에 대한 보안 기술 및 대응책은 다음과 같다.

스마트폰에는 다양한 개인정보가 저장되어 있기 때문에 이를 관리하는 것은 중요하다. 간단한 보안관리 프로세스는 동의 없이 개인정보를 포함한 중요 정보를 수집할 수 없으며, 수집된 정보는 공개가 되어서는 안된다. 이 정보를 이용할 시에는 그에 할당한 사용과 동의가 필요하며 이용 완료 시에는 파기되어야 한다. 기업의 주요 자산인 고객의 개인정보를 안전하게 보호하기 위한 정책 및 전략과 솔루션, 프로세스는 스마트폰 서비스 제공 측면에서 지속적으로 개선되어야 한다. 또한 애플리케이션 보안 정책도 중요하다. 더불어 개인정보 및 기타 주요 정보를 안전한 저장 공간을 확보하여 저장하고 이를 암호화 저장함으로써 보호해야 한다. 이 저장 매체에 접근 시 접근권한을 설정하고 각종 인증 및 개인정보를 안전하고 손쉽게 관리하는 시스템이 요구된다. 각종 개인정보, 전자 인증정보를 저장하여 필요할 때 제출하는 기술로 카드 형태로 표현된다. 또한 사용자가 이용하는 PC와 동일하게 모바일 상에서도 파일 암호화가 필요하다. 더불어 데이터 통신 시 주고받는 데이터에도 암호화가 필요하다. 이는 정보가 유출 시 해당 정보 노출을 막을 수 있다. 스마트폰이 PC에 가까워지고 PC와 흡사한 OS를 사용하며, 사용자가 늘수록 발견되지 않는 정보 유출경로가 발견될 수 있다. 모바일 VPN과 방화벽을 사용하여 모바일 디바이스를 사용자의 사설 네트워크에 안전하게 연결할 수 있으며, 하드웨어 및 무선통신 네트워크에 대한 무단 액세스 및 사용으로부터 보호한다. 이를 이용하여 악성코드의 접근이나 외부자의 접근에 대하여 보호할 수 있고, 정책을 설정하여 보다 안전한 모바일 서비스 환경을 구축할 수 있다.

보안 관련 데이터 저장/데이터 접근통제/API를 통한 UICC 애플리케이션 보안 서비스를 제공하는 USSM(UICC Security Service Module) TS 102 266(stage1)가 있다. 이는 ETSI에서 정의한 UICC 보안 모델로서 표준 모델로 표준화를 진행하였으며, UMTS 기반의 목적 및 요구사항 등이 정의되어 있다.

인터넷으로부터 파일을 업로드하고 다운로드하는 경

우 통상 두 가지 보안 위협이 발생하게 된다. 하나는 게시자의 신원을 도용하는 것이고, 두 번째는 게시된 애플리케이션의 위변조 방지와 데이터 발신지 확인이다. 이를 막는 방법이 애플리케이션 게시자의 신원확인/인증이고, 게시된 애플리케이션 코드의 무결성과 데이터 인증성 확인하는 것이다. 이를 해결하는 방법이 전자서명 기법 기반의 코드(Code Signing)이며, 이를 가능케 하는 것이 공개키 인증서를 사용하고 있다.[5~7]

스마트폰 보안 연관기술은 지문/홍체/생체 인식 기술을 이용한 사용자 인증 기술이 있으며, RFID 휴대폰 잠금기능, 안티 바이러스 등이 있다.

이러한 보안기술들이 우회될 가능성을 포함하는 위협이 존재한다. 도난 및 분실 시 이러한 기능을 스마트폰의 장점 중 하나인 사용자가 기능을 추가 삭제할 수 있는 사용자 맞춤형 기능에 의해 삭제되거나 서비스를 종료 시킬 수 있다. 이에 각 통신사에서는 스마트폰 분실 및 도난솔루션을 제공하고 있으며, 모바일 보안 회사에서도 이를 제공하고 있다. 분실 시 신고가 접수되면 통신사에서는 원격으로 모든 스마트폰 OS에 대해 공장 초기화, 카메라 차단, 프린트 스크린 차단 등을 할 수 있으며, 이외에도 GPS를 이용한 핸드폰 위치 추적, 원격 잠금 기능 등을 제공하고 있다.

이 밖에도 언급되지 않은 위협과 보안기술이 존재하지만 이것만으로는 안전하다고 할 수 없다. 언제 어디서 어떤 보안 사고가 발생할지 모르며 이를 대비하기 위해서는 지속적인 연구가 필요하다.

3. 스마트폰 보안 국내외 표준화 동향

현재 스마트폰 보안 표준화는 국내 · 국제를 망론하고 초기 상태에 있다. 국내의 경우는 2010년 TTA 표준화 전략맵 작업을 통해 주요 표준화 아이템을 선정했고, 국외의 경우는 ITU-T 연구반 17에서 하나의 권고가 개발되고 있다. 또한 아이폰 앱스토어에 적용되는 기존 공개키 인증서 프로파일이 사실 표준 형태로 존재한다. 향후 표준화 수요가 증가할 것으로 예상되어 본격적인 표준화가 국내외적으로 수행될 것으로 예측된다.

3.1 국내 표준화 현황

국내에서는 2013년까지 스마트폰 관련 무선통신 국내외 표준화 추진을 통해 안전한 스마트폰 서비스 인프라 구축에 대한 기반을 마련하기 위한 목표를 설정하고 관련 연구와 표준화를 추진 중이다. 스마트폰 보안 국내 표준화는 이제 본격적으로 진행될 예정이다. 2010년 TTA 표준화 전략맵 작업에서 스마트폰에 대

〈표 2〉 TTA 표준화 전략맵에 도출한 표준화 대상항목

표준화 대상항목	표준화 내용
스마트폰 플랫폼 보안기준	· 스마트폰에서 발생 가능한 침투공격, 스마트폰의 결함을 유도, 스마트폰의 정보 유출과 같은 악성 행위에 대하여 보호하고 이를 평가할 수 있는 기준 마련
스마트폰 앱 보안 기준	· 스마트폰에 제공되는 앱 서버나 앱 스토어의 앱 소프트웨어에 대한 보안 표준을 선정하여 앱에 대한 보안 평가와 검증 기준 설정
스마트폰 인터페이스 보안 기준	· 스마트폰과 PC나 다른 기기와의 연결에 사용되는 터널링(VPN) 기법
스마트폰 기반의 악성코드 수집/분석 프레임워크	· 스마트폰 등 모바일 기기를 대상으로 하는 악성코드의 수집 및 분석을 위한 프레임워크 요구사항 정의

〈표 3〉 국내외 스마트폰 표준화 동향 및 관련 추진 사항

국내외	기관	내용
국내	금융결제원	· 옴니아2, 아이폰, 안드로이드폰 등의 스마트폰에 대한 스마트폰 뱅킹의 표준화 추진
	행정안전부	· 공공부문 모바일 응용서비스에 모바일 웹 및 모바일 앱 개발을 위한 개발 가이드라인 작성
	TTA	· PG605 : 모바일 웹 서비스 보안 평가 가이드라인, 웹서비스 보안정책 모델 등 다수의 웹서비스 보안 관련 표준 제정, 모바일 종단간 통신을 위한 인증구조 외 3건 단체 표준 제정
		· PG504 : 모바일 웹 서비스에서의 메시지 보안을 위한 보안 구조 표준 제정
	방송통신위원회	· '모바일 시큐리티 포럼'을 통해 스마트폰 정보보호 주체별 역할을 정립하여 '스마트폰 이용자 10대 안전수칙'을 발표
국외	ITU-T SG17	· 모바일 상의 주요 보안 위협을 소개하며 보안 요구사항을 명시. 보안 기술 및 메커니즘을 제시하는 권고 개발 중
	MCPC	· 모바일 컴퓨팅 시스템 시장 확대를 목표로 하고 있으며 서비스 활성화를 위해 각 분야의 관심과 협력을 도모함
	PPCA	· 새로운 모바일과 무선 기술에 대한 평가
	LIPS Forum	· 스마트폰과 일반 휴대폰(피처폰)을 포함하는 휴대폰 단말기의 다양한 사용 프로필에 대한 사양을 정의

한 정의와 주요 표준화 대상 항목을 정의한 바 있다.[1] 전략맵에서는 무선 통신망 보안 항목에 스마트폰 보안 세부항목을 설정했고, 스마트폰 세부 표준화 항목은 '스마트폰 플랫폼 보안기준', '스마트폰 앱 보안 기준', '스마트폰 인터페이스 보안기준' 등이며, 세부 내용은 〈표 2〉와 같다. 이외에 방송통신위원회 등 국내 주요 기관에서 스마트폰 보안 표준과 연관된 주요 활동 계획은 〈표 3〉과 같다.

〈표 2〉에서와 같이 행정안전부에서는 공공부문 모바일 응용서비스에 모바일 웹 및 모바일 앱 개발을 위한 개발 가이드라인을 만들 예정이며, 금융결재원에서는 스마트폰 뱅킹의 표준화를 추진하고 있다.

특히, 스마트폰 보안과 연관되어 TTA PG 605에서는 모바일 웹 서비스 보안 평가 가이드라인[TTAS.KO-10.0245], 웹 서비스 보안 정책 모델[TTAS.KO-10.0243] 등 다수의 웹 서비스 보안 관련 표준 및 모바일 종단간 통신을 위한 인증 구조 외 3건의 단체 표준을 제정한 바 있다.[2]

3.2 국외 표준화 현황

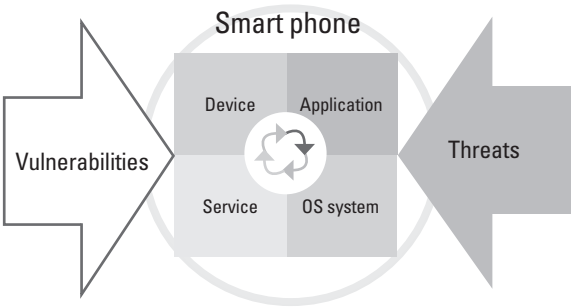
ITU-T 연구반 17 연구과제 6은 스마트폰 보안 표준(X.msec-6)를 2009년 9월부터 개발하고 있다. 이 권고의 제목은 '모마일 폰 보안 특성'이며, 스마트폰보다 포괄적인 개념을 갖는 모바일 폰에 대한 보안 위협과 보안 기술 및 메커니즘에 대해 표준화를 추진할 예정이다.

X.msec-6에서는 스마트폰에 대한 위협의 유형을 [그림 1]과 같이 인터페이스, 사용자, ID 카드, 모바일 앱 서비스, 외부 인터페이스로부터 위협 등으로 구분되며, [그림 2]와 같이 스마트폰이 가진 취약성을 공격자가 이용한 다양한 위협 모델을 제시하고 있다.

스마트폰 보안 요구사항은 하드웨어 보안과 소프트웨어 보안으로 구성되며, 다시 소프트웨어 보안은 통신 보안, OS 보안, 애플리케이션 보안, 사용자 데이터 보안으로 구분된다. 모바일상의 취약점을 피하고, 위협 및 공격으로부터 피해를 감소시키기 위해 보안기술 및 메커니즘 기반의 하드웨어 및 소프트웨어가 만들어져야한다.

또한 아이폰 애플리케이션 게시자 신원확인 및 애플리케이션 코드의 데이터 인증 및 무결성을 확인하기 위해, 아이폰 앱 스토어에서는 ITU-T 권고 X.509에 기반한 인증서 프로파일을 사용한다.[6] 윈도 및 안드로이드의 경우에도 인증서 기반의 코드사인을 통하여 데이터 인증 및 무결성을 확인한다.[5][7] 코드사인 인증서는 국외 인증서 발급 기관 및 국내 공인인증기관에서 발급된 인증서로 사용이 가능하다. 대표적인 발급 기관에는 Verisign(국외), 금융결제원(국내) 등이 있다.

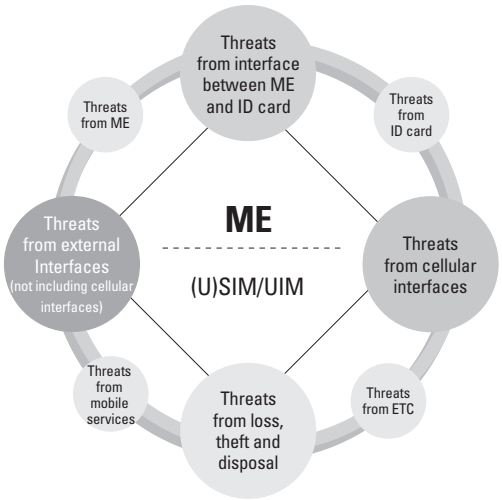
또한, 모바일 컴퓨팅 시스템의 시장 확대를 목표로 하고 있는 일본 컨소시엄인 MCPC(Mobile Computing Promotion Consortium)에서는 Smartphone 위원회를 신설하고 관련 연구와 표준화를 추진 중이다. 그리고 PPCA(Portable Computer and Communications Association)와 LIPS Forum(Linux Phone Standard) 등이 스마트폰 연구와 표준화를 진행할 예정이다.[4]



[그림 1] 취약성과 위협 관계[3]

〈표 4〉 ITU-T SG17 X.msec6 주요 사항[3]

항목	내용
일반 보안 위협	· 모바일폰 일반 위협
특화 보안 위협	· 단말 분실 및 도난 · 전자적 도청 · 단말 복제 · 셀룰러 인터페이스를 통한 위협 · 다중 외부 인터페이스를 통한 위협 · 비인가된 접근 · 악성코드 · 스팸 · 비인가된 위치정보의 접근
보안 요구 사항	· 하드웨어 보안, · 소프트웨어 보안(통신 보안, 운영체제 · 보안, 응용 보안, 사용자 데이터 보안)
보안 기술 및 메커니즘	· 악성코드 설치 방지 · 응용 간 상호 접근 예방 · 악성 행위 분석 · 안전한 전송 · 암호화 · 스팸 필터 · 보안 민감 응용 · 프라이버시 보호 기술 · 원격제어 기술 · Anti-spoofing 대안



[그림 2] 모바일 위협[3]

〈표 5〉 스마트폰 표준화 추진 전략

항목	내용
표준화 추진	· 국내 표준화와 국제 표준화를 동시 추진
기간	· 3년 이내에 추진
국내 의견수렴	· 국내 이동통신사의 요구사항을 반영한 국내 표준을 개발하고, 이를 바탕으로 국제 표준화를 추진함
추진 기관	· 국내 표준화는 TTA PG503을 통해 추진하고, 국제 표준화는 ITU-T SG17 연구과제 6 또는 3GPP/3GPP2를 통해 추진할 필요 있음

4. 표준화 추진전략

스마트폰은 국내뿐만 아니라 국제적으로도 큰 관심을 불러일으키고 있지만 현재 국내외 스마트폰 보안 관련 표준화 작업은 이제 막 시작하는 수준이다. 따라서 TTA를 통한 국내 표준의 추진과 ITU-T를 통한 국제 표준의 추진 등 국내외 표준화 추진을 동시에 진행하여 국내 기술의 국제 표준을 선점할 필요성이 있다.

표준화 아이템의 경우, 〈표 2〉와 같은 항목에 '앱 개발자와 앱 스토어 간의 인증 방식 및 보안 터널' 등의 다양한 보안 아이템의 지속적인 개발이 필요하다.

구체적으로는 보안 기술의 표준 제정을 담당하는 주체로는 국내 표준 주체의 경우 TTA의 PG503가 적정하며, 국제표준 주체의 경우 ITU-T의 SG17/Q6가 적절하다. 또한, 국제표준화의 경우 이동통신 표준화 기구인 3GPP/3GPP2도 또 다른 국제 표준 추진 주체로 고려해야 한다. 표준화 추진 일정은 향후 스마트폰의 보급과 관련 기술 수요의 시급성, 시장이 성숙되는 시점을 고려했을 때 3년 이내가 적절할 것으로 보이며 표준 개발 시에는 국내 이동통신 서비스 3사의 의견을 적극 반영하고 이외 의견을 수렴하여 국내외 표준개발을 진행해야 할 것이다.

5. 맺음말

본 고에서는 스마트폰 보안과 연관된 국내외 표준화 동향을 살펴보고 추진 전략을 제시했다. 스마트폰은 기업 비즈니스, 정부 업무, 그리고 다양한 응용 분야에서 활용되고 있으며, 보안은 이를 안전한 스마트폰 기반의 서비스를 제공하기 위한 필수 요소가 되고 있다. 향후에는 국내 표준과 국제 표준을 개발하여 상호 연동 가능하고 안전한 스마트폰 기반의 다양한 서비스를 제공할 수 있을 것으로 기대된다.

[참고문헌]

[1] TTA(www.tta.or.kr), 표준화전략맵, '네트워크&시스템보안-4차-배포자료', 2010.09.03

[2] TTA(www.tta.or.kr), '응용보안 평가인증 보고서', 2010.11.01

[3] ITU-T, 'Security aspects of mobile phones', T09 SG17 100407 TD PLEN 1012, 2010.04.16

[4] ITU-T, T REC Y.Sup8-201001-I, 'Supplement on a survey of global ICT forums and consortia', 2010.01

[5] Microsoft, http://msdn.microsoft.com/en-us/library/ms537361.aspx

[6] Apple, http://developer.apple.com/, 'code signing guide', 2009.10.13

[7] Google Android, http://developer.android.com/, http://developer.android.com/guide/publishing/app-signing.html

TTA