情 報 保 護 學 會 誌
第23卷 第3號, 2013. 6

ITU-T SG17 스마트폰 보안 표준화 동향

김 미 주*, 윤 미 연*, 손 경 호*, 염 흥 열**

요 약

스마트폰은 휴대전화에 인터넷통신, 정보검색, 메일 송/수신, 음악 및 동영상 재생 등 컴퓨터 지원 기능이 추가된 기기로, 휴대전화의 경우 제조할 때 탑재된 기능만을 사용하는데 반해 스마트폰은 사용자의 기호에 따라 마음대로 어플리케이션을 추가로 설치하여 사용할 수 있다는 특징을 가진다. 우리나라는 2010년부터 스마트폰 사용이 대중화되기 시작하면서 스마트폰 사용인구가 급격히 증가하여 우리의 일상생활과 밀접한 관계를 가지며 영향력을 넓혀가고 있다. 하지만 스마트폰이 활성화되면서 스마트폰을 이용한 보안 위협의 발생도 증가하게 되었다. 이에 전 세계적으로 스마트폰 보안을 위한 다양한 연구 및 대응활동이 활발히 진행 중에 있다. 이와 관련하여 스마트폰 보안 표준화의 필요성을 인식하여 국제표준화를 추진하고 있는 ITU-T SG17에서의 스마트폰 보안 표준화 동향에 대한 정보를 제공하고자 한다.

Ⅰ. 서 론

2007년 애플이 아이폰을 출시한 후 전세계적으로 스마트폰 이용 인구가 급격하게 증가하면서 스마트폰의 시대가 도래하였다. 스마트폰은 피처폰이라 불리는 제한적인 기능만을 수행하는 휴대전화에 인터넷통신, 정보검색 등 컴퓨터에서 사용하는 기능과 사용자의 기호에 따라 다양한 어플리케이션을 추가로 설치하여 사용할 수 있는 기능을 탑재함으로써 편리성과 확장성을 가진다. 우리나라에서도 2010년 애플 아이폰의 국내 출시 이후로 스마트폰 이용자가 꾸준히 증가하여 2013년 3월을 기준으로 3천 500만 명을 돌파하였다. 스마트폰 사용이 활성화됨에 따라 생활패턴에 변화를 가져오는 등 우리의 일상생활과 밀접한 관계를 가지며 큰 영향을 미치고 있다.

스마트폰을 사용함으로써 사람들은 편리함을 얻게되었지만 스마트폰을 이용한 보안 위협에도 노출되게 되었다. 스마트폰 보안 위협은 앱을 이용하여 개인정보, 계좌번호 등 민감 정보를 유출하고, 문자메시지를 탈취하여 사생활을 침해하고, 유명 앱으로 위장하여 악성코드 감염을 유도하고, 소액결제 등 과금을 유발하고, 불법적으로 권한을 획득하는 등 다양한 형태로 나타나고 있으며, 피해의 규모 및 정도가 점점 심각해지고 있어 사회적인 문제가 되고 있다. 이러한 보안 위협을 대응하기 위해 전세계적으로 다양한 연구 및 대응활동이 활발히 진행되고 있다.

본 고에서는 모바일 보안 분야 국제표준화를 추진 하고 있는 ITU-T(국제전기통신연합 표준화부문) SG17(보안그룹) 내 Q.6(유비쿼터스보안 연구과제)에서 진행한 모바일 보안 표준화 동향에 대해서 살펴보고, 특히 Q.6에서 스마트폰 보안과 관련하여 추진 중인 표준화 아이템들에 대해서 중점적으로 살펴보고 관련 동향에 대한 정보를 제공하고자 한다.

Ⅱ. ITU-T SG17 Q.6 모바일 보안 표준화 동향

ITU-T SG17[1]은 정보보호 분야 국제표준을 제정하는 '보안 선도 연구그룹'으로, 사이버보안, 스팸대응, 보안관리, 클라우드 컴퓨팅 보안, 모바일보안, ID 관리 등 12개의 정보보호 연구과제에 대한 표준화를 추진하고

본 연구는 미래창조과학부의 지원을 받는 (방송통신표준기술력향상사업)의 연구결과로 수행되었음
* 한국인터넷진흥원 인터넷침해대응센터 침해예방단 연구개발팀 ({mijoo.kim, myyoon, khson}@kisa.or.kr)
** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

있다. 그 중 모바일 보안 이슈는 Q.6에서 담당하고 있다.

Q.6는 모바일 보안을 비롯한 USN, M2M, 스마트그리드, IPTV 보안 등 다양한 유비쿼터스 서비스에서의 보안 기술에 대한 표준들을 개발하고 있다. 의장단으로는 우리나라의 백종현 수석(KISA)이 라포처로, 일본의 Yutaka Miyake(KDDI)가 부라포처로 Q.6 연구그룹을 이끌고 있다.

Q.6에서 모바일 보안 이슈와 관련하여 개발한 표준으로는 모바일 데이터 통신에서의 보안 위협, 모바일 사용자와 어플리케이션 서비스 제공자를 위한 보안 요구사항, 모바일 데이터 통신에서의 보안 기술들을 명세한 X.1121[2], PKI 기술을 사용하여 안전한 모바일 시스템 구현을 위한 가이드라인을 제공하는 X.1122[3], 종단간 안전한 모바일 데이터 통신을 위해 보안 정책을 세 가지로 분류함으로써 차별화된 서비스를 제공하는 X.1123[4], 네트워크에서 다양한 서비스 제공자와 모바일 사용자 간의 모바일 데이터 통신을 위한 인증 구조를 정의한 X.1124[5], 안전하지 않은 단말로부터 모바일 네트워크를 보호하기 위한 대응시스템에 관한 X.1125[6]가 있다.

또한, 스마트폰 활성화에 따른 다양한 보안 위협의 출현으로 Q.6에서도 스마트폰 보안의 중요성 및 필요성을 인식하고 이에 대한 표준화 작업을 추진하고 있다. 스마트폰 보안 표준화 아이템으로는 지난 2013년 3·4월 정기회의에서 부속서로 승인된 스마트폰 보안 개요(Sup.19)[7]와 현재 국제표준 개발 작업을 진행하고 있는 악성코드 감염 단말 대응 가이드라인(X.msec-7)[8], 안전한 스마트폰 앱 배포 프레임워크(X.msec-8)[9]가 있다. 다음의 Ⅲ, Ⅳ, Ⅴ절에서는 각각의 표준화 아이템들에 대한 내용 및 동향에 대해서 기술한다.

Ⅲ. 스마트폰 보안 개요

스마트폰 보안 개요(security aspects of smartphones, ITU-T X.1120 series Sup.19)는 스마트폰 보안과 관련하여 ITU-T SG17 Q.6에서 추진한 첫 번째 표준화 아이템이다. 지난 2012년 8·9월 정기회의에서 표준 개발을 완료하여 각국 회람을 진행하였으며, 2013년 3·4월 정기회의에서 회람 결과를 검토하여 X.1120 시리즈의 부속서 Sup.19으로 채택되었다.

Sup.19에서는 스마트폰에 대한 특징, 자산, 보안 고려사항 등 스마트폰 보안에 관한 일반적인 이슈부터, 스마트폰 보안 위협, 프레임워크, 솔루션 등 스마트폰 보안 기술에 대한 다양한 관점에서의 이슈를 다루고 있다.

3.1 스마트폰 보안 일반

스마트폰의 특성은 지속적으로 변화하지만 기존 휴대전화와 구분되는 몇 가지 기능을 가진다. 다음은 스마트폰의 일반적인 특성을 나타낸다.

- 음성통화, SMS 전송 등 기존 휴대전화 기능
- 빌트인 프로세스의 빠른 속도 및 확장된 메모리 스토리지에 따른 강력한 성능
- TCP/IP 프로토콜을 이용한 인터넷 접속
- Wi-Fi, 블루투스, NFC, USB 등 다양한 주변 장치 인터페이스
- 위성, 네트워크, 하이브리드 포지셔닝(positioning) 능력을 이용한 다양한 위치 정보 기반 서비스 제공
- 노트북, PC 등 다른 단말 데이터와의 동기화
- 필요에 따른 어플리케이션 검색, 다운로드, 설치, 이용 지원

또한 스마트폰 자산은 크게 사용자 데이터, 소프트웨어, 하드웨어로 나뉘며, 각각의 자산에 대한 종류 및 중요도는 [표 1]과 같다.

〔표 1〕 스마트폰 자산

자산	종 류	중요도
사용자 데이터	주소록, 전화기록, SMS/MMS, 이메일, 사진, 오디오, 계좌 정보, 위치 정보, 메모, 일정 등	매우 중요
소프트웨어	초기 설치된 어플리케이션, 사용자가 설치한 어플리케이션, 운영체제 등	중요
하드웨어	CPU, RAM, 플래시, 배터리 등	중요

일반적으로 스마트폰에 기능이 추가될수록 더 많은 보안 위협에 노출되게 되는 양상을 보인다. 스마트폰 보안의 목표는 증가하는 스마트폰 기능과 동일한 수준으로 보안성을 향상시키는 것이 될 수 있다. 이를 위해서는 보안 위협을 분석하고, 보안 위협 및 보안 목표에 맞는 보안 요구사항을 도출하여, 해당 보안 요구사항을 충족하는 보안 솔루션을 도입하는 로드맵을 그려볼 수 있다.

3.2 스마트폰 보안 위협

스마트폰 보안 위협은 스마트폰 자체 취약점을 이용한 보안 위협과 외부 공격에 의한 보안 위협으로 분류할 수 있다.

취약점의 유형은 다음과 같다.

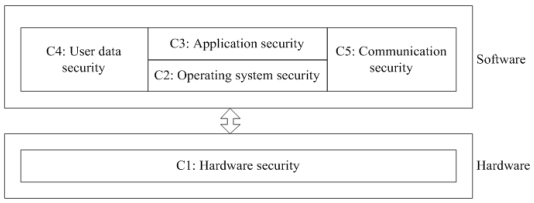
- 시스템 결함
- 안전하지 않은 무선 채널
- API 관리 부실
- 사용자 인식 부족 등

또한, 공격의 유형은 다음과 같다.

- 물리적 통제
- 악성코드
- 백도어 공격
- 불법복제
- 무선 공격
- 인가되지 않은 접근
- 스팸
- 주변 인터페이스 공격 등

3.3 스마트폰 보안 프레임워크

스마트폰 사용자 프라이버시 및 정보 보호를 위해, 스마트폰은 기밀성, 무결성, 가용성이 반드시 보장되어야 하며, 이를 위해 Sup.19에서는 [그림 1]과 같은 보안 프레임워크를 정의하였다.



〔그림 1〕 스마트폰 보안 프레임워크

하드웨어 보안, 운영체제 보안, 어플리케이션 보안, 사용자 데이터 보안, 통신 보안 각각에 따른 보안 고려사항은 다음과 같다.

- 하드웨어 보안 고려사항(C1)
  · IMEI와 같은 민감한 ID의 변경 방지
  · 칩셋 무결성 검증
  · 보안 관련 정보의 변경 방지
- 운영체제 보안 고려사항(C2)
  · 시스템 코드의 무결성 검증, 데이터 트래픽 모니터링, 응용 서비스 보안 등 안전하고 신뢰성있는 환경 제공
  · 인가되지 않은 OS 이미지 및 어플리케이션의 설치 및 업데이트 방지
  · 어플리케이션 무결성 확인
  · 시스템 관련 데이터의 무결성 확인
  · 서로 다른 어플리케이션 간의 안전한 통신 메커니즘 제공
  · 어플리케이션 권한 관리
- 어플리케이션 보안 고려사항(C3)
  · 인지도가 낮은 어플리케이션 설치 주의
  · 악성코드 탐지 및 대응
  · 어플리케이션 실행 분리
  · 설치된 어플리케이션에 대한 검증
  · 스팸 필터링
- 사용자 데이터 보안 고려사항(C4)
  · 스마트폰 분실 경보
  · 사용자 데이터 무결성 및 기밀성 보장
  · 사용자 데이터에 대한 접근 통제
- 통신 보안 고려사항(C5)
  · DoS 공격 방지
  · 원치않는 접근 통제를 위한 방화벽 제공
  · 단말 인증 메커니즘 제공
  · 사용자 ID 기밀성 보장

3.4 스마트폰 보안 솔루션

스마트폰 보안 솔루션에는 운영체제 및 초기 설치된 어플리케이션들의 취약점들을 제거하는 등 시스템의 보안성을 향상시키는 유형과 외부 공격으로부터 대응하는 안티바이러스, 방화벽, IDS와 같은 보안 툴이 있다.

시스템 보안을 향상시키는 유형의 보안 솔루션은 보안 부팅, 사용자 확인, 안전한 API, 어플리케이션 분리, 복구 불가능한 데이터 삭제, 방화벽, 자동 잠금, 민감 데이터 암호화, 어플리케이션 디지털 서명, 접근 제어, 인증, 원격 데이터 보호, 네트워크 접근 보호 등이 있다.

보안 툴에는 안티스팸, 안티바이러스, 백업 소프트웨어, 통합 보안 솔루션 등이 있다.

[표 2]는 각 보안 솔루션과 보안 고려사항과의 상관관계를 나타낸다.

〔표 2〕 보안 솔루션과 보안 고려사항과의 관계

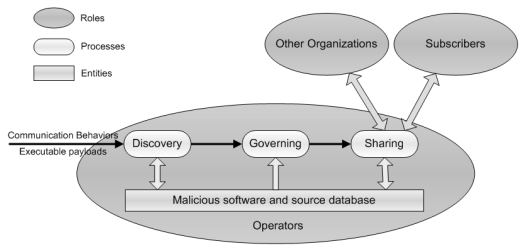
보안 솔루션	보안 고려사항
보안 부팅	C1, C2
사용자 확인	C1, C2, C3, C4, C5
안전한 API	C3
어플리케이션 분리	C3
복구 불가능한 데이터 삭제	C4
방화벽	C2, C3, C5
자동 잠금	C2
민감 데이터 암호화	C4
어플리케이션 디지털 서명	C3
접근 제어	C2, C3, C4, C5
인증	C2, C3, C4, C5
원격 데이터 보호	C4
네트워크 접근 보호	C5
안티 스팸	C3
안티 바이러스	C1, C2, C3, C4, C5
IDS	C1, C2, C3, C4, C5
백업 소프트웨어	C4

Ⅳ. 악성코드 감염 단말 대응

악성코드 감염 단말 대응 가이드라인(Guidelines on the management of infected terminals in mobile networks, X.msec-7)은 2012년 2·3월 정기회의에서 중국으로부터 제안되어 표준화아이템으로 채택된 아이템이다.

X.msec-7에서는 행위, 프로토콜 헤더, 제어 패킷 분석에 따른 의심 단말 탐지, 비정상 단말에 대한 검증 및 피해 최소화를 위한 조치 등 관리, 보안 조직 등에 악성코드 정보 공유 방식을 이용하여 악성코드에 감염된 단말 대응 가이드라인을 제공한다.

본 표준에서는 운영자가 네트워크 측면에서 가입자 단말의 비정상 행위를 탐지 및 관리하여 가입자에게 위협을 알리고 다른 조직과 악성 소프트웨어 정보를 공유하는 [그림 2]와 같은 프레임워크를 정의하였다.



〔그림 2〕 악성코드 감염 단말 대응 프레임워크

탐지 프로세스에서는 통신 행위와 프로토콜 헤더&제어 패킷을 수집하여 이상행위를 분석하고, 이상행위가 발견되면 감염이 의심스러운 단말과 함께 관리 프로세스에 보고된다. 관리 프로세스에서는 이상행위를 확인하여 가입자와 운영자에 피해를 막을 수 있는 수단을 제공한다. 모바일 악성코드 관리 및 대응을 위한 정보를 시기적절하게 제공하기 위해서 지능화된 공유 프로세스가 수립되어야 한다. 공유 프로세스에서는 산업 전반에 걸쳐 보안을 향상시키기 위해 다른 회사의 운영자, 관련 보안 기관을 비롯한 타 조직과 악성 소프트웨어에 대한 정보를 공유한다. 탐지, 관리, 공유 전 프로세스 전반에는 악성 행위 패턴 및 악성 소스를 포함한 악성 소프트웨어 관련 정보을 저장하고 제공하는 악성 소프트웨어 및 소스에 대한 데이터베이스가 있다. 데이터베이스에 저장된 정보는 이상행위를 식별하고, 악성코드에 감염된 단말의 단말을 통제하고, 악성 소프트웨어 정보를 발표하는데 도움을 준다.

Ⅴ. 스마트폰 앱 보안

안전한 스마트폰 앱 배포 프레임워크(Secure application distribution framework for communication devices, X.msec-8)는 2012년 2·3월 정기회의에서 한국 및 일본으로부터 제안되어 표준화아이템으로 채택된 아이템이다.

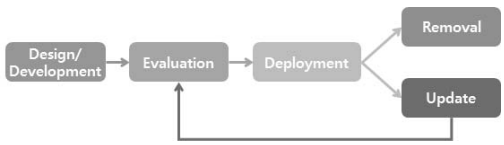
표준안의 범위는 스마트폰을 비롯한 태블릿 PC, 셋톱박스(Set-top-box, STB) 등 앱스토어로부터 어플리케이션을 다운하고 실행할 수 있는 능력을 갖춘 단말을 대상으로 안전한 어플리케이션 개발을 위한 가이드라인, 어플리케이션의 생명주기에 따른 보안 요구사항, 어플리케이션 검증, 개발자 인증 등에 대한 보안 요구사항을 포함한다.

2012년 6월 서울에서 개최된 Q.6 인터림 회의에서 한국측 에디터로부터 어플리케이션 생명주기 및 어플리케이션 보안 검증을 위한 기준(안) 등이 포함된 첫 번째 드래프트가 제안되었고, 2012년 9월 스위스 제네바에서 개최된 정기회의에서 일본측 에디터로부터 표준화아이템의 범위를 수정하여 앱스토어 자체의 보안 요구사항을 제안하였으나 합의를 보지 못하였다.

2013년 3,4월 정기회의에서 표준안의 범위에 대해서 재논의되어 어플리케이션 보안 고려사항, 보안 검증을 비롯한 앱스토어 전반에 관한 보안 이슈를 다루는 것으로 잠정적으로 합의를 보았으나, 상세 내용에 대해서는 차기회의에서 다시 논의하기로 하였다.

현재 X.msec-8 표준안은 스마트폰 어플리케이션 생명주기에 따른 보안 고려사항, 안전한 스마트폰 앱 배포 프레임워크, 프레임워크 각 보안 기능별 보안 요구사항 등으로 구성되어 있다.

스마트폰 어플리케이션 생명주기는 [그림 3]과 같이 5가지 단계로 나타낼 수 있으며, 각 단계별 보안 고려사항은 다음과 같다.



〔그림 3〕 어플리케이션 배포 생명주기

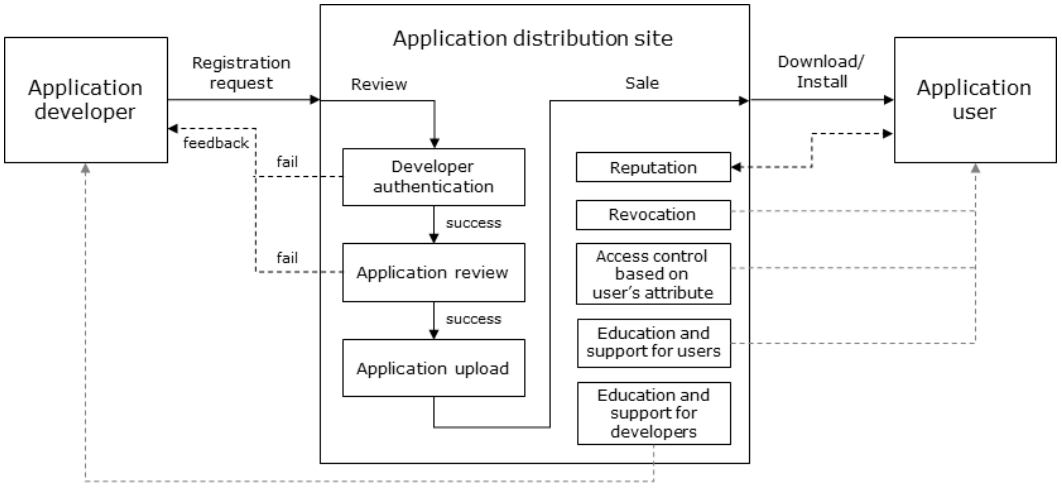
- 설계/개발(Design/Development)
  설계/개발은 개발자가 모바일 어플리케이션을 설계하고 개발하는 단계로, 개발자는 모바일 어플리케이션 설계 시 보안을 고려해야 하고, 코드 상에 취약점이 없도록 안전하게 코딩해야 한다. 앱스토어에서는 개발자들이 보안을 고려하여 모바일 어플리케이션을 개발할 수 있도록 교육을 제공하거나 안전한 모바일 어플리케이션 개발을 위한 지원을 할 필요가 있다.
- 평가(Evaluation)
  평가는 개발자가 만든 모바일 어플리케이션을 앱스토어의 어플리케이션 검증자가 검토하는 단계이다. 앱스토어에 모바일 어플리케이션 등록 요청이 오면 앱스토어에 등록하기 이전에 해당 어플리케이션이 안전한 어플리케이션인지 보안성이 검토되어야 한다. 이 과정에서 앱스토어는 개발자의 신원을 검증하고, 어플리케이션의 보안성을 검토하여 안전하다고 판단된 경우 앱스토어에 등록하고 그렇지 않은 경우 개발자에 피드백을 제공한다.
- 배포(Deployment)
  배포는 모바일 어플리케이션이 배포되어 사용자가 해당 어플리케이션을 사용하는 단계이다. 일부 앱스토어의 경우 최소한의 정책으로 어플리케이션을 검토하기 때문에, 배포되는 어플리케이션들이 안전하지 않을 수 있다. 사용자는 어플리케이션을 다운로드하고 설치하여 사용하는데 주의를 기울여야한다. 앱스토어는 사용자들이 어플리케이션을 다운받아 사용할 때 주의를 기울일 수 있도록 교육을 제공하거나 평판시스템을 도입할 필요가 있다.
- 업데이트(Update)
  업데이트는 개발자가 모바일 어플리케이션에 대한 기능 및 내용 상의 수정으로 업데이트를 하는 단계이다. 이런 경우에도 어플리케이션은 앱스토어의 어플리케이션 검증자로부터 보안성 등에 대한 검토를 다시 받아야 한다.
- 삭제(Removal)
  삭제는 사용자의 스마트폰 단말에서 어플리케이션을 제거하는 것으로, 어플리케이션 배포된 이후에 해당 어플리케이션이 악성 어플리케이션으로 판단된 경우 앱스토어는 사용자 동의 및 규정에 따라 원격으로 스마트폰에 설치된 어플리케이션을 삭제할 수 있어야 한다.

[그림 4]는 안전한 스마트폰 앱 배포를 위한 프레임워크를 나타낸다. 프레임워크에서는 어플리케이션 개발자가 어플리케이션을 개발하여 앱스토어에 등록하고, 사용자가 해당 어플리케이션을 다운로드하여 설치하기까지의 과정과 앱스토어의 보안 기능을 나타낸다.

어플리케이션 개발자는 어플리케이션 개발 후 앱스토어에 등록을 요청한다. 앱스토어는 개발자에 대한 인증(Developer authentication)을 수행함으로써 등록된 개발자인지 판단한다. 이 후 개발자가 제출한 어플리케이션에 대한 검토(Application review)를 통해 어플리케이션의 안전성 등을 판단하여, 검증을 통과한 경우 앱스토어에 게시하여 사용자에게 다운로드하여 설치할 수 있게 된다. 검증을 통과하지 못한 경우, 사유와 함께 개발자에 피드백을 제공한다.

어플리케이션 검증에는 다음의 관점에서 어플리케이션의 보안성을 검증한다.

- 네트워크 보안
- 데이터 보안
- 바이러스 및 악성코드 감염
- 로그인 보안
- 권한 관리



〔그림 4〕 안전한 스마트폰 앱 배포 프레임워크

- 단말 관리
- 푸쉬 알람 서비스 보안
- 컴플라이언스

추가로 앱스토어에서는 어플리케이션 사용자와 개발자를 위한 보안 기능으로 사용자로 하여 안전한 어플리케이션을 선별할 수 있도록 어플리케이션에 대한 평판 시스템(Reputation), 악성코드 및 안전하지 않은 어플리케이션을 원격에서 삭제(Revocation)할 수 있는 기능, 미성년자 보호를 위한 사용자 속성에 따른 접근제어(Access control based on user's attribute), 사용자에게 안전한 어플리케이션 다운로드 및 이용 등에 대한 인식 제고 및 문제발생 시 도움을 줄 수 있는 사용자 교육 및 지원(Education and support for users), 개발자에게 안전한 어플리케이션 개발 등을 지원하기 위한 어플리케이션 개발자 교육 및 지원(Education and support for developers)등의 기능을 제공해야 한다.

또한 본 표준안에서는 프레임워크의 각 보안 기능 요소들에 대한 구현을 돕기 위해 보안 메커니즘, 가이드라인, 보안 기준 등에 대한 정보를 제공하고 있다.

Ⅵ. 결 론

스마트폰의 대중화로 우리는 스마트폰을 이용해 업무를 보고, 길에서 인터넷 검색을 하고, 위치정보를 이용해 다양한 서비스를 제공받는 일이 일상이 되는 등 우리의 생활 패턴에 큰 변화를 가져왔다. 스마트폰이 우리 생활과 밀접한 관계를 이어가는 가운데, 스마트폰을 이용해 중요정보를 유출하고, 과금을 유발하고, 사생활을 침해하는 등 사용자들을 위협하는 다양한 유형의 보안 위협들이 뒤따르고 있다. 이러한 스마트폰 보안 위협을 예방하고 피해를 최소화하기 위해 다양한 연구 및 대응활동이 전 세계적으로 활발히 진행 중에 있으며, 본 논문에서는 스마트폰 보안을 위해 ITU-T SG17에서 추진 중인 국제 표준화 추진 동향에 대해서 살펴보았다. 스마트폰 보안 관련 표준화 및 연구를 진행하는 전문가들에게 유익하게 활용되길 바라며, 본 논문에서 다뤄진 스마트폰 보안 표준화 활동이 좋은 결실을 이뤄 사용자들에게 안전한 스마트폰 사용 환경을 제공하는데 도움이 되길 기대해 본다.

참고문헌

[1] ITU-T SG17, http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/default.aspx
[2] ITU-T X.1121, Framework of security technologies for mobile end-to-end data communications
[3] ITU-T X.1122, Guideline for implementing secure mobile systems based on PKI
[4] ITU-T X.1123, Differentiated security service for secure mobile end-to-end data communication
[5] ITU-T X.1124, Authentication architecture for mobile end-to-end data communication
[6] ITU-T X.1125, Correlative Reacting System in

mobile data communication
[7] ITU-T Sup.19, ITU-T X.1120 series - Supplement on security aspects of smartphones
[8] ITU-T draft Recommendation X.msec-7, Guidelines on the management of infected terminals in mobile networks
[9] ITU-T draft Recommendation X.msec-8, Secure application distribution framework for communication devices

〈著者紹介〉

김 미 주 (Mijoo Kim)
순천향대학교 정보보호학과 학사 졸업
순천향대학교 정보보호학과 석사 졸업
순천향대학교 정보보호학과 박사 과정
2008년 4월~2009년 7월 : 한국정보보호진흥원 주임연구원
2009년 7월~현재 : 한국인터넷진흥원 선임연구원
<관심분야> 인터넷 보안, USN 보안, 사이버보안, 모바일·스마트폰 보안, 스마트그리드 보안

윤 미 연 (Mi Yeon Yoon)
가톨릭대학교 수/컴퓨터학과 학사 졸업
숭실대학교 컴퓨터공학과 석사 졸업
숭실대학교 컴퓨터공학과 박사 졸업
2005년 6월~2009년 7월 : 한국정보보호진흥원 선임연구원
2009년 7월~현재 : 한국인터넷진흥원 책임연구원
<관심분야> 인터넷 보안, USN 보안, 멀티캐스트/IPTV 보안, 모바일 보안, 스마트그리드 보안, 클라우드 보안

손 경 호 (Kyung Ho Son)
2001년 2월 : 성균관대학교 전기전자컴퓨터공학과 학사
2004년~현재 : 성균관대학교 컴퓨터공학과 석·박사과정 수료
2001년 1월~현재 : 한국인터넷진흥원 연구개발팀 팀장
<관심분야> 침해사고대응기술, 융합보안, 네트워크보안, 보안 시험·평가, 클라우드·빅데이터 보안

염 흥 열 (Heung Youl Youm)
종신회원
한양대학교 전자공학과 학사 졸업
한양대학교 대학원 전자공학과 석사 졸업
한양대학교 대학원 전자공학과 박사 졸업
1982년 12월~1990년 9월: 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국정보보호학회 총무이사, 학술이사, 교육이사, 논문지편집위원 위원장, 수석부회장(역), 학회장(역), 명예회장(현)
2005년~2008년 : ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월 (구) 정통부 정보보호 PM/, 정보통신연구진흥원 정보보호전문위원
2011년 1월~12월 : 한국정보보호학회 회장(역)
2008년 7월~현재 : 방송통신위원회 자체평가위원회
2008년 7월~2013년 2월 : 행정안전부 정책자문위원회
2013년 5월~현재 : 미래창조과학부 자체평가위원회
2009년 5월~현재 : 국정원 암호검증위원회 위원
2009년~현재 : ITU-T SG17 부의장/SG17 WP3 의장
2012년 6월~현재 : 정보보안산업 표준 포럼 의장
<관심분야> 인터넷 보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜