情報保護學會論文誌
第 22 卷 第 1 號, 2012. 2

공통평가기준 3.1 기반 스마트폰 운영체제 보호프로파일 개발*

전 웅 렬,[1†] 김 지 연[1], 이 영 숙,[2] 원 동 호[1‡]
[1]성균관대학교, [2]호원대학교

An Efficient Mixnet for Electronic Voting Systems*

Woongryul Jeon,[1†] Jeeyeon Kim[1], Youngsook Lee,[2] Dongho Won[1‡]
[1]Sungkyunkwan University, [2]Howon University

요 약

2007년 애플의 아이폰과 구글의 안드로이드 OS를 채택한 일명 안드로이드 폰들이 잇달아 발표되면서 스마트폰 열풍이 시작되었다. 2010년 한해 스마트폰 사용자는 2010년 1월 약 100만명에서 2010년 12월 약 710만명으로 700% 증가한 수치를 나타내었으며, 2011년 3월 현재에는 천만명의 사용자가 스마트폰을 사용하고 있다고 보고되었다. 그러나 스마트폰 수요의 폭발적인 증가만큼 많은 보안문제도 대두되었다. 스마트폰은 다양한 서비스를 제공하기 위해 많은 개인정보를 저장하고 있다. 따라서 스마트폰은 다른 IT 기기에 비해 엄격한 보안기술이 적용되어야 함에도 불구하고, 개발자와 사용자 모두 보안에 대한 인식이 미비하여 여러 가지 보안사고가 발생하고 있다. 이에 본 논문은 스마트폰의 보안 강화를 위해 스마트폰의 취약성을 분석하고 스마트폰 운영체제를 평가하기 위한 스마트폰 운영체제 보호프로파일을 제안한다. 이를 위해 본 논문은 스마트폰 운영체제와 기존 운영체제의 차이점을 분석하고, 이를 기반으로 새로운 보안문제, 보안목적, 보안기술요구사항을 도출한다.

ABSTRACT

Recently, smartphone has being most popular mobile device in mobile market, not around the world, but in domestic. In Korea, there are about 710 million people are using smartphone in 2010, and it is expected that about 1 billion people will use smartphone in next year. However, with exponential growth of smartphone, several security issues come to the fore. Because, the smartphone store various private information to provide user customized services, smartphone security can be regarded most critical issues than security of other devices. However, leak of awareness for security may cause many security accidents in present. Therefore, in this paper, we analyze security features of smartphone and propose a protection profile based on Common Criteria v3.1. Our work can be distributed for developer and user of smartphone to estimate security of smartphone.

Keywords: Smartphone, protection profile, common criteria, security

접수일(2011년 5월 4일), 게재확정일(2012년 1월 27일)
* 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2011-0004751).
† 주저자, wrjeon@security.re.kr
‡ 교신저자, dhwon@security.re.kr

I. 서 론

최근 세계 IT 시장에서 "스마트"가 화두로 떠오르고 있다. IT 기기 뿐만 아니라 최근에는 TV까지 공통적으로 "스마트"라는 접두어를 포함하고 있다. 그리고 이러한 흐름은 바로 "스마트폰"에서 시작되었다. 스마트폰은 일반 PC와 유사한 성능과 서비스를 제공하는 휴대전화를 의미한다. 스마트폰에 대해 명확한 정의를 내리는 것은 어렵다. 스마트폰과 대비되는 피처폰(feature phone) 역시 하드웨어 기술의 발달로 상당한 수준의 성능과 서비스를 제공할 수 있기 때문이다. 따라서 최근에는 독자적인 운영체제와 플랫폼을 갖추고 있으며, 이를 바탕으로 다양한 응용 프로그램의 개발이 가능한 폰을 스마트폰이라 지칭한다[1].

2007년 애플의 아이폰과 구글의 안드로이드 OS를 채택한 일명 안드로이드 폰들이 잇달아 발표되면서 스마트폰 열풍이 시작되었다. 국내도 예외는 아니라서, 2010년 한해 스마트폰 사용자는 2010년 1월 약 100만명에서 2010년 12월 약 710만명으로 700% 증가한 수치를 나타내었으며, 2011년 3월 현재에는 천만명의 사용자가 스마트폰을 사용하고 있다고 보고되었다[2]. 그러나 수요의 증가만큼 많은 보안문제도 대두되고 있다.

스마트폰은 우수한 연산성능을 바탕으로 다양한 서비스를 제공하는데, 사용자의 요구에 맞춘 서비스를 제공하기 위해 보다 많은 개인정보를 저장하고 있다. 예를 들어 위치 기반 서비스를 제공하기 위해 사용자의 위치정보를 저장하고 있거나, 이메일, 문서작성 등의 서비스를 제공하기 위해 PC에서만 사용되던 다양한 문서 파일들을 저장하고 있는 것이 바로 그 예이다. 이처럼 스마트폰에는 기존 여러 IT 장비에 흩어져 저장되어 있던 정보들이 하나의 기기에 집약되어 있기 때문에 다른 IT 기기에 비해 엄격한 보안기술이 적용되어야 한다. 그러나 개발자와 사용자 모두 보안에 대한 인식이 미비하여 여러 가지 사고가 발생하고 있는 것이 현실이다. 특히 국제적으로 통용되고 있는 보안평가방법인 공통평가기준 기반 보호프로파일이 존재하지 않기 때문에, 스마트폰 자체에 대해 공인된 평가 역시 진행이 어렵다.

이에 본 논문은 스마트폰의 보안 강화를 위해 스마트폰의 취약성을 분석하고 스마트폰 운영체제를 평가하기 위한 공통평가기준(Common Criteria, CC) 기반의 스마트폰 운영체제 보호프로파일을 제안한다. 이를 위해 본 논문은 스마트폰 운영체제와 기존 운영체제의 차이점을 분석하고, 이를 기반으로 새로운 보안문제, 보안목적, 보안기술요구사항을 도출한다. 본 논문에서 제안하는 스마트폰 운영체제 보호프로파일은 추후, 공통평가기준 스마트폰 운영체제 평가에 활용될 수 있을 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 기존 운영체제에 비해 스마트폰 운영체제가 지니는 취약성과 보호프로파일의 필요성을 서술한다. 3장에서는 스마트폰 운영체제 보호프로파일의 보안문제, 보안목적 및 보안기능요구사항을 도출하고, 4장에서는 도출한 보안기능요구사항을 중심으로 기존 운영체제 보호프로파일과의 비교를 설명한다. 마지막으로 5장에서는 결론을 서술한다.

II. 관련연구

2.1 공통평가기준

공통평가기준은 IT 제품 및 시스템의 보안기능과 보안기능의 평가과정에 적용되는 보증수단에 대한 공통의 요구사항들을 제시함으로써 독립적으로 수행한 보안성 평가 결과들 간에 상호비교를 가능하게 한다. 다시 말해서, 공통평가기준은 IT 제품 중 보안과 관계있는 시스템이나 기능을 평가할 때, 이용하는 공통의 기준이다. 공통평가기준은 소비자, 개발자, 평가자에 의해 활용될 수 있다. 소비자는 자신이 원하는 제품 또는 보안기능을 공통평가기준에 의거하여 나열하고 서술할 수 있다. 이러한 작업의 결과를 형식적인 문서로 작성한 것이 보호프로파일(Protection Profile)이다. 개발자는 소비자가 작성한 보호프로파일을 수용하여 원하는 제품 또는 기능을 구현할 수 있다. 만약 보호프로파일을 수용하지 않았을 경우, 개발된 제품에 대해 공통평가기준에 의거하여 보안기능을 설명할 수도 있다. 이런 작업을 문서화한 것이 보안목표명세서(Security Target)이다. 보안목표명세서는 보호프로파일의 내용과 많은 부분이 일치하며, 개발한 제품에서 구현한 기능에 대해 상세한 설명 등이 추가된다. 보호프로파일이나 보안목표명세서에서 다루어지는 제품 또는 기능을 TOE(Target of Evaluation)라 부른다. 평가자는 소비자나 개발자가 작성한 보호프로파일이나 보안목표명세서를 평가하기 위하여 공통평가기준을 사용할 수 있다[17].

현재 공통평가기준은 CCRA(The Common Criteria Recognition Agreement)를 통해 국제

〔표 1〕 기존 운영체제 보호프로파일 현황

번호	보호프로파일 명	설명
1	Operating System Protection Profile(OS-PP)	- PP 버전 : 2.0 - CC 버전 : 3.1 Revision 3 - 출판날짜 : 2010.06.01
2	US Government Protection Profile for General Purpose Operating Systems in a Networked Environment(COTS-PP)	- PP 버전 : 1.0 - CC 버전 : 3.1 Revision 2 - 출판날짜 : 2010.08.30
3	Compartmentalized Operations Protection Profile - Operating System(CCOPP-OS)	- PP 버전 : 2.0 - CC 버전 : 3.1 Revision 2 - 출판날짜 : 2008.06.19

적으로 통용되고 있다. 보안제품의 판매과정에서 구매자는 공통평가기준을 기준으로 하는 평가를 요구할 수 있는데, 이때 평가의 중복을 방지하기 위해 국가별로 평가결과를 인증하는 기능을 제공한다. CCRA는 9월 현재 총 26개 국가의 회원국을 포함하고 있으며, 우리나라에도 여기에 포함되어 있다. 따라서 우리나라에서 평가를 받은 제품은 다른 나라에 수출할 때, 추가적인 평가과정 없이 판매가 가능하다.

2.2 기존 운영체제 보호프로파일 분석

본 절에서는 스마트폰 운영체제의 보호프로파일을 개발하기에 앞서 기존 운영체제 관련 보호프로파일에 대해 살펴본다. 국제적으로 공인된 보호프로파일은 Common Criteria Portal 홈페이지에 게시되는데, 2011년 3월 현재 www.commoncriteriaportal.org에 등록된 운영체제 관련 보호프로파일은 4종이다. 이 중 현재 통용되고 있는 공통평가기준 v3.1을 기반으로 하는 보호프로파일은 3종으로 〔표 1〕과 같다〔3〕.

3종의 보호프로파일은 각각 일반적인 운영체제, 네트워크 환경을 기반으로 하는 운영체제, 그리고 프린터와 같이 특정 기기를 대상으로 하는 운영체제를 나타낸다. 3종의 보호프로파일은 환경이 다른만큼 각자 특징을 지니고 있는데, 〔표 2〕는 3종의 보호프로파일을 비교한 것이다.

3종의 보호프로파일의 분석결과 나타나는 주요 공통점은 크게 두 가지로 요약할 수 있다.

첫 번째, OS-PP와 COTS-PP, 2종의 보호프로파일은 평가대상에 대한 물리적인 보안을 가정사항으로 두고 있다. 일반적으로 하드웨어 장비는 지정된 장소에 설치되어 운영되고, 소프트웨어 장비는 물리적인 형태가 없기 때문에 이러한 가정은 통용된다. 물리적인 보안은 평가대상이 물리적으로 접근이 제한된 곳에서 운영되며, 도난 및 분실의 우려가 없다는 것을 의미한다.

두 번째, OS-PP, COTS-PP, CCOPP-OS, 3종의 보호프로파일 모두 사용자 및 관리자를 신뢰된

〔표 2〕 기존 운영체제 보호프로파일 비교

	OS-PP	COTS-PP	CCOPP-OS
TOE 용도	- 범용 PC 및 일반 서버에서 활용이 가능한 운영체제	- 국가보안망에서 사용되는 다중 사용자 기반 네트워크 환경의 운영체제	- 네트워크 환경에서 독립적으로 동작하는 IT 장비의 운영체제
TOE 형태	- S/W	- S/W	- S/W
보증등급	- EAL 4(ALC_FLR.3 추가)	- EAL 2(ALC_FLR.2 추가)	- EAL 4
특징	- 범용 PC의 운영체제를 TOE로 설정하고 있기 때문에 다른 운영체제에 비해 보안문제(위협, 조직의 보안정책, 가정사항)가 추상적임 - 접근제어와 관련한 항목을 위협으로 설정	- 네트워크 환경을 기준으로 하고 있기 때문에 다중사용자 및 외부 IT 객체에 의한 위협요소를 고려하여 보안문제를 구성하고 있음 - 서비스 거부 공격, 자원 재할당, 무단 세션 생성 등 네트워크 환경에 특화된 위협 설정	- 네트워크에 연결되어 사용되는 프린터, 복사기 등 사무용품의 평가기준으로 널리 활용됨 - 다른 두 보호프로파일과는 달리 TOE의 물리적인 보안을 가정하지 않음 - TOE가 물리적으로 파괴될 수 있음을 위협으로 설정

객체로 간주하고 있다. 실제 보안에서 내부자에 의한 취약성은 기술적으로 대응하기가 매우 까다롭고 드문 경우이기 때문에, 조직의 보안정책 및 가정사항으로 사용자 및 관리자에 대한 신뢰성을 보장하는 것이 일반적이다.

그러나 이러한 두 가지 특징은 스마트폰의 환경에 적용하기에는 어려움이 있다. 스마트폰은 분실의 위험이 높고, 다양한 연령대가 사용할 수 있는 장치이기 때문에, 정보화 수준에 따라 기기를 다루는 능숙함에서 차이가 발생한다.

따라서 스마트폰 운영체제에 대한 평가지침을 마련하기 위해서는 기존 운영체제 보호프로파일이 지니는 위 두 가지 특성과는 구별되는, 스마트폰의 사용환경적 특징을 바탕으로 새로운 보안문제를 정립할 필요가 있다. 이에 다음 절에서는 스마트폰의 사용환경을 중심으로 스마트폰 운영체제 보호프로파일 개발에서 고려해야 하는 사항들을 상세히 설명한다.

2.3 스마트폰 운영체제 보호프로파일을 위한 고려사항

스마트폰이 출시된 이후 다양한 논문을 통해 스마트폰의 보안취약성이 발표되고 또 개선되어 왔다. 이러한 연구는 현재에도 진행중이다[4-14]. 본 절에서는 기존 다양한 연구들을 통해 도출된 스마트폰의 보안취약성 특징 세 가지를 설명한다.

첫 번째, 스마트폰은 휴대기기로 분실의 위험이 높다. 스마트폰은 다양한 IT 기기의 집약체로 간주할 수 있기 때문에, 스마트폰의 분실은 집약된 개인정보의 손실로 이어져 큰 보안문제를 야기할 수 있다. 최근들어 스마트폰 분실에 대비하여 원격에서 스마트폰을 제어하는 기술들이 속속 발표되는 것[15-17]도 이와 무관하지 않다.

두 번째, 스마트폰은 다양한 환경에서 활용이 가능하다. 스마트폰은 케이블을 통해 물리적으로 다른 IT 기기와 연동하여 사용할 수 있을 뿐만 아니라 무선 네트워크를 통해 다른 스마트폰, AP, 인터넷 등 여러 가지 환경과 연동하여 사용할 수 있다. 이는 스마트폰의 우수한 개방성을 나타내는 동시에, 스마트폰이 다양한 종류의 위협에 노출되어 있음을 의미한다.

세 번째, 스마트폰의 사용자는 스마트폰의 사용에 능숙하지 않을 확률이 매우 높으며, 악의적으로 스마트폰의 보안을 훼손할 수 있다. 대표적인 예로 아이폰의 탈옥과 안드로이드 폰의 루팅을 들 수 있다. 스마트폰은 단일사용자 환경에서 동작한다. 그러나 아이러니하게도 현재 스마트폰 시장을 양분하고 있는 아이폰과 안드로이드폰은 다중사용자를 기반으로 하는 PC의 운영체제에서 개발되었다(아이폰의 경우 Mac OS, 안드로이드 폰의 경우 리눅스). 사용자가 관리자의 권한을 획득하게 되면 스마트폰의 다양한 설정을 변경할 수 있는데, 여기에는 보안과 관련된 설정, 스마트폰 제조업체의 정책과 관련된 설정도 포함된다. 따라서 스마트폰 제조회사는 출고시 스마트폰 사용자에게 관리자 권한을 부여하지는 않는데, 사용자가 임의로 관리자 권한을 획득하는 과정을 탈옥 혹은 루팅이라고 부른다. 사용자에 의한 플랫폼의 변조는 보다 다양한 기능의 활용, 설정의 변경을 가능하게 하는 동시에 보안취약성을 야기할 수 있다.

스마트폰 운영체제에 대한 보호프로파일은 이러한 세 가지 특징을 고려해야 한다. 이는 기존 운영체제 보호프로파일에서 가정하고 있는, 물리적인 보안과 신뢰된 사용자 및 관리자를 스마트폰에서는 더 이상 가정할 수 없음을 의미한다.

III. 스마트폰 운영체제 보호프로파일 개발

본 장에서는 스마트폰 운영체제의 보호프로파일을 개발한다. 보호프로파일의 개발은 크게 3단계로 구분할 수 있다. 1단계는 평가대상이 되는 TOE(Target of Evaluation)을 정의하는 단계이고, 2단계는 보안문제를 정의하는 단계이다. 2단계에서는 보안문제를 바탕으로 보안목적도 정의하며, 보안목적에 대한 이론적 근거 역시 서술한다. 마지막으로 3단계에서는 1단계, 2단계에서 도출한 보안문제 및 보안목적을 바탕으로 보안기능요구사항을 도출한다.

3.1 TOE 정의

스마트폰 운영체제 보호프로파일에서 TOE는 스마트폰 운영체제 및 스마트폰 운영체제가 관리하는 저장장치로 한정한다. 네트워크 환경 및 기타 환경에서는 운영체제와 저장장치가 구분되어 운영될 수도 있으나, 스마트폰은 단일 기기이기 때문에 저장장치 역시 포함한다. 스마트폰 운영체제로 TOE를 한정하는 이유는 스마트폰에 설치되어 활용되는 다양한 응용 프로그램을 제외하기 위해서이다. 응용 프로그램은 사용자의 기호에 따라 설치의 유무가 다르고, 설치되는 종류 또한 다르기 때문에 평가대상으로써 일반화하기가 어렵다. TOE가 제공하는 보안기능인 TSF(TOE Security

〔표 3〕 TOE 보안기능

TSF	설명
감사	- TOE는 운영체제의 보안과 관련된 모든 행동을 감사하고 기록을 생성함 - 감사기록은 이벤트의 생성 시점 및 주체를 포함 - 감사기록은 로컬 저장장치에 저장되거나 중앙 서버에 저장되며, 허가되지 않은 객체로부터의 접근을 차단함
암호학적 서비스	- TOE는 외부 객체와 안전한 통신을 하기 위해 다양한 보안 프로토콜(SSH, TLS, IPSec 등)을 제공함 - TOE는 휘발성 및 비휘발성 저장장치에 대해 적합한 접근제어 정책을 제공함 - TOE는 TOE로 유입 또는 반출되는 네트워크 데이터에 대해 보안정책에 기반한 접근흐름을 제어함
식별 및 인증	- TOE는 사용자 및 객체를 식별 및 인증함 - 식별 및 인증은 로컬 또는 원격으로 가능함
관리	- TOE는 TOE가 제공하는 TSF 및 TSF 데이터를 안전한 방법으로 관리함
안전한 채널	- TOE는 신뢰된 외부 객체와 통신을 할 때 안전한 채널을 형성하고 통신함

Function)은 〔표 3〕과 같다.

우선 TOE는 감사기능을 제공한다. TOE는 보안과 관련한 모든 행동을 감시하고 기록을 생성함으로써, 문제가 발생했을 때, 추적이 가능하도록 한다. TOE는 안전한 통신 및 저장된 데이터의 보호를 위해 암호학적 서비스를 제공한다. 암호학적 서비스에는 기밀성, 무결성 그리고 가용성을 보장하기 위한 기능들이 포함되어 있다. 또 TOE는 사용자를 식별 및 인증한다. 일반적으로 TOE는 단일사용자이며, 사용자는 관리자의 권한을 활용할 수 없다. 또 TOE는 패스워드, 패턴, 지문, 성문 등 다양한 방법으로 사용자를 인증하는 기능을 제공한다.

마지막으로 TOE는 TOE가 제공하는 TSF 및 TSF 데이터를 안전한 방법으로 관리하며, 외부와의 통신에서 필요한 경우 안전한 채널을 형성하고 통신할 수 있다.

3.2 보안문제 및 보안목적 도출

본 절에서는 보호프로파일에서 정의하는 보안문제에 대해 설명한다. 보안문제는 위협, 조직의 보안정책, 가정사항으로 구분되며, 2장에서 언급한 스마트폰 보안의 특징을 반영한다.

3.2.1 보안문제

〔표 4〕는 본 보호프로파일에서 정의되는 위협을 나타낸다.

T.관리부실과 T.분실은 스마트폰의 보안 특징 때문에 추가된 항목으로 기존 3종의 운영체제 보호프로파일에서는 빠진 항목이다.

T.관리부실은 사용자에 의한 의도적인 플랫폼 위변조로 인해 초래될 수 있는 위협과 함께, 사용자가 스마트폰을 사용하면서 저지를 수 있는 설정실수 및 Phishing에 대한 위협을 포함한다. 스마트폰은 기본적으로 블루투스에 연결하지 않는 이상 기기의 검색을 차단하고 있다. 이는 악의적인 외부 객체가 사용자 스마트폰에 블루투스로 접근하는 것을 차단하기 위해서인데, 사용자가 이러한 설정들을 잘못 변경하는 경우 보안에 위협을 초래할 수 있다. 또 스마트폰 사용자는 스마트폰 기반 메신저, 웹브라우저 등 다양한 경로를 통해 Phishig의 위협에 노출되어 있다. T.관리부실은 이러한 위협들을 포함한다.

T.분실은 사용자가 스마트폰을 잃어버리는 경우에 대한 위협이다. 스마트폰은 분실이 가능한 휴대기기이며, 다양한 개인정보가 집적되어 있기 때문에 물리적은 보안을 가정하는 것은 위험하다. 따라서 본 보호프로파일에서는 이전 3종의 보호프로파일과는 달리 분실을 위협으로 포함한다.

T.내재된 취약성은 스마트폰 운영체제에 내재된 취약성을 악용하는 공격을 의미한다. 안드로이드 폰의 경우 리눅스를 기반으로 하고 있는데, 리눅스 및 유닉스 운영체제의 취약성을 이용한 악성코드가 안드로이드에서도 동작할 가능성이 높다.

T.플랫폼 위변조는 앞서 언급한 탈옥 및 루팅에 관한 위협이다. 사용자는 임의로 플랫폼을 위변조하여 보안기능을 훼손할 수 있으며, 소프트웨어의 잠금을 해제할 수도 있다. 실제 최근 출시된 아이폰 4S의 시리(Siri)의 잠금을 해제하여 다른 모델에서도 사용한 사례가 있다.

다음으로 조직의 보안정책을 정의한다. 아래 〔표 5〕는 본 보호프로파일이 정의하는 조직의 보안정책을 나타낸다.

조직의 보안정책은 스마트폰 운영체제를 개발하고

〔표 4〕 제안하는 보호프로파일의 위협

위협	설명
T.연속인증시도	- 위협원은 TOE에 접근하기 위해 연속적으로 인증을 시도하여 인가된 사용자의 권한을 획득할 수 있음
T.위장	- 위협원은 정당한 사용자로 가장하여 TOE에 접근할 수 있음
T.저장데이터훼손	- 위협원은 TOE에 저장된 사용자 데이터 및 TSF 데이터를 인가되지 않은 방식으로 유출, 변경, 삭제할 수 있음
T.전송데이터훼손	- 위협원은 원격의 신뢰된 객체와 TOE 사이에 전송되는 사용자 데이터 및 TSF 데이터를 인가되지 않은 방식으로 유출, 변경, 삭제할 수 있음
T.관리부실	- TOE의 인가된 사용자는 안전하지 않은 방식으로 TOE를 구성, 관리 또는 사용할 수 있음
T.악성코드	- 위협원은 무선 네트워크 및 외부 IT 객체를 통해 악성코드를 유입시켜 TOE의 자원을 소비하거나 사용자 데이터 및 TSF 데이터를 유출, 변경, 삭제할 수 있음
T.분실	- 인가된 사용자는 고의 혹은 타의에 의해 TOE를 분실할 수 있음
T.서비스 거부 공격	- 위협원은 TOE에 대해 네트워크 자원 및 TOE의 자원을 소비하여 서비스 거부 공격을 시도할 수 있음
T.내제된 취약성	- 위협원은 TOE의 내재된 취약성을 악용하여 관리자 권한을 획득하거나, 저장된 정보를 임의로 변경할 수 있음
T.플랫폼 위변조	- 위협원은 TOE의 플랫폼을 임의로 변경하여, TOE의 보안기능을 훼손할 수 있음 - 위협원은 TOE의 플랫폼을 임의로 변경하여, 저작권을 훼손할 수 있음

운영하는 조직에서 설정하는 정책이다. 스마트폰의 다양한 서비스는 사용자의 요구를 반영한 수십만개의 응용 프로그램에 기반하고 있다. 현재 아이폰 및 안드로이드의 경우 응용 프로그램 개발자를 위한 SDK (Software Developer's Kit)를 제공하기 때문에 수많은 개발자들이 다양한 응용 프로그램을 개발하고 있다. 그러나 이는 응용 프로그램의 다양성을 보장하는 반면 응용 프로그램의 안전성을 보장하는데에는 어려움이 따른다. 개발자의 응용 프로그램은 악의적인 코드를 포함하고 있거나, 호환성에서 문제를 일으킬 수 있다. 또 응용 프로그램의 구현상의 오류를 악용하여 공격자가 스마트폰 사용자 및 관리자의 권한을 획득할 가능성도 있다. 이와 같은 위협은 스마트폰 운영체제에서 직접적으로 다룰 수 있는 위협이 아니며, 스마트폰 운영체제를 개발하고 관리하는 조직에서 대응해야 하기 때문에 조직의 보안정책으로 설정하였다.

마지막으로 가정사항을 정의한다. 〔표 6〕은 본 보호프로파일이 정의하는 가정사항을 나타낸다.

본 보호프로파일이 정의하고 있는 가정사항은 A.안전한 외부객체 하나이다. A.안전한 외부객체는 스마트폰이 다양한 환경과 연동하는 것에 기인한다. 스마트폰은 다양한 외부 IT 기기와 연동하여 사용되는데, 이때 스마트폰 내부에 저장되어 있는 사용자 데이터 및 TSF 데이터가 외부 객체에 저장될 수 있다. 대표적인 예로 트레이닝 응용 프로그램을 들 수 있다. 트레이닝과 관련한 대부분의 응용 프로그램은 사용자에게 운동기록 및 경로에 대한 통계를 제공하기 위해 외부 서버에 사용자의 운동기록 및 위치정보를 저장하고 있다. 이러한 정보 또한 개인정보로서 유출될 경우 피해를 초래할 수 있다. 그러나 서버에 저장되어 있는

〔표 5〕 조직의 보안정책

조직의 보안정책	설명
P.호환성	- TOE의 개발자는 TOE가 다양한 환경 및 외부 객체와의 연동에서 호환성을 보장해야 함
P.안전한 구현	- TOE는 안전한 코딩(secure coding)기법을 적용하여 구현되었음을 보장해야 함

〔표 6〕 제안하는 보호프로파일의 가정사항

가정사항	설명
A.안전한 외부객체	- 외부 IT 객체(서버, PC 등)는 관리자에 의해 안전한 방법으로 관리되며, 따라서 외부 IT 객체에 저장되어 있는 사용자 데이터 및 TSF 데이터는 유출되지 않음을 가정

〔표 7〕 제안하는 보호프로파일의 보안문제

보안목적	설명
O.감사	- TOE는 보안과 관련된 행동에 대한 책임을 추적하기 위해 보안관련 사건을 정확하게 기록하고 안전하게 유지해야 하며, 기록된 감사데이터를 검토할 수 있는 수단을 제공해야 함
O.관리	- TOE는 TOE의 인가된 사용자가 TOE를 효율적으로 관리할 수 있는 방법을 제공해야 함 - TOE의 관리자/사용자는 TOE를 항상 최신의 상태로 유지해야 함
O.식별 및 인증	- TOE는 사용자를 유일하게 식별해야 하며, TOE에 대한 접근을 허용하기 전에 사용자의 신원을 인증해야 함
O.저장 데이터 보호	- TOE는 TOE에 저장된 TSF 데이터를 인가되지 않은 노출, 변경, 삭제로부터 보호해야 함
O.전송 데이터 보호	- TOE는 원격의 신뢰된 객체와 TOE 사이에 전송되는 데이터를 인가되지 않은 노출, 변경, 삭제로부터 보호해야 함
O.악성코드 차단	- TOE는 네트워크, PC 등에서 유입되는 악성코드를 탐지하고 이에 대한 대응수단을 제공해야 함
O.네트워크 흐름	- TOE는 TOE의 보안정책에 따라 TOE와 외부 객체 사이의 통신을 중재해야 함
O.플랫폼 위변조 방지	- TOE는 플랫폼의 임의적인 변경을 방지해야 함
OE.원격 데이터 삭제	- TOE를 분실한 경우, TOE 운영환경은 원격에서 TOE를 제어(잠금, 초기화, 데이터 삭제)할 수 있는 기능을 제공해야 함
OE.안전한 외부 객체	- TOE의 외부 IT 객체는 안전하게 관리되어야 함
OE.사전 시험	- TOE에 설치되는 응용 프로그램은 보안 및 호환성을 보장하기 위해 사전에 검증되고 시험되어야 함
OE.업데이트	- 제조사 및 개발사는 TOE의 보안성 및 효율성의 향상을 위해 주기적/비주기적으로 업데이트를 제공해야 함

사용자 데이터 및 TSF 데이터는 본 보호프로파일이 대상으로 하는 스마트폰 운영체제의 외부에 저장되는 것으로 대응수단을 마련하는 것이 어려우므로, 가정사항으로 설정하였다.

3.2.2 보안목적

본 절에서는 이전 절에서 정의한 보안문제를 바탕으로 보안목적을 정의한다. 보안목적은 보안기능의 추상적인 형태로, 앞서 명시한 보안문제에 대응하기 위한 방법을 나타낸다. 〔표 7〕은 본 보호프로파일이 정의하고 있는 보안문제를 나타낸다.

O는 Object의 약자로 보안목적을 나타내며, OE는 운영환경의 보안목적을 나타낸다. 하나의 보안목적은 하나 이상의 보안문제와 대응한다. 부록의 〔표 A-1〕은 보안목적과 보안문제의 대응관계를 나타낸다. 대응관계는 정의한 보안목적이 보안문제들을 모두 포괄하고 있음을 나타낸다.

3.3 보안기능요구사항

본 장에서는 3장에서 도출한 보안문제 및 보안목적을 바탕으로 보안기능요구사항을 도출한다. 보안기능요구사항은 공통평가기준 v3.1 Revision 3을 근간으로 한다. 〔표 8〕는 본 보호프로파일이 정의하는 보안기능요구사항을 나타낸다.

〔표 8〕 보안기능요구사항

클래스	보안기능 요구사항	설명
보안감사	FAU_ARP.1	- 보안감사 자동대응
	FAU_GEN.1	- 감사데이터 생성
	FAU_GEN.2	- 사용자 신원 연관
	FAU_SAA.1	- 잠재적 위반 분석
	FAU_SAR.1	- 감사 검토
	FAU_SAR.2	- 감사 검토 권한 제한
	FAU_STG.1	- 감사 증적 저장소 보호
암호 지원	FCS_CKM.1	- 암호키 생성
	FCS_CKM.4	- 암호키 파기
	FCS_COP.1	- 암호 연산
사용자 데이터 보호	FDP_ACC.1	- 부분적인 접근통제
	FDP_ACF.1	- 보안속성에 기반한 접근통제
식별 및 인증	FIA_AFL.1	- 인증실패처리
	FIA_ATD.1	- 사용자 속성 정의
식별 및 인증	FIA_SOS.1	- 비밀정보의 검증
	FIA_UAU.1	- 인증
	FIA_UID.1	- 식별
보안관리	FMT_MOF.1	- 보안기능 관리
	FMT_MSA.1	- 보안속성 관리
	FMT_MTD.1	- TSF 데이터 관리
	FMT_SMF.1	- 관리기능 명세
	FMT_SMR.1	- 보안역할
프라이버시	FPT_STM.1	- 신뢰된 타임스탬프
	FPT_TST.1	- TSF 자체시험
TOE 접근	FTA_SSL.1	- TSF에 의한 세션 잠금
	FTA_SSL.2	- 사용자에 의한 세션 잠금
안전한 경로	FTP_ITC.1	- TSF간 안전한 채널

〔표 9〕 보안기능요구사항의 이론적 근거

	O.감사	O.관리	O.식별및인증	O.저장데이터보호	O.전송데이터보호	O.악성코드차단	O.네트워크흐름	O.플랫폼위변조방지
FAU_ARP.1	O						O	
FAU_GEN.1	O							
FAU_GEN.2	O							
FAU_SAA.1	O	O						
FAU_SAR.1	O							
FAU_SAR.2	O							
FAU_STG.1	O							
FCS_CKM.1				O	O			
FCS_CKM.4				O	O			
FCS_COP.1				O	O			
FDP_ACC.1		O		O		O	O	O
FDP_ACF.1		O		O		O	O	O
FIA_AFL.1			O					
FIA_ATD.1			O					
FIA_SOS.1			O			O		
FIA_UAU.1		O	O	O		O		
FIA_UID.1		O	O	O				
FMT_MOF.1		O						
FMT_MSA.1		O						
FMT_MTD.1		O						
FMT_SMF.1		O						
FMT_SMR.1		O						
FPT_STM.1	O					O		
FPT_TST.1		O				O		
FTA_SSL.1		O						
FTA_SSL.2		O						
FTP_ITC.1		O			O		O	

보안기능요구사항은 보호프로파일을 참조하여 보안목표명세서(security target)를 개발하는 작성자에 따라 보다 상세화 될 수 있다. 〔표 9〕은 보안기능요구사항과 보안목적의 대응관계를 나타낸다. 운영환경의 보안목적은 보안기능요구사항이 다루는 범주가 아니기 때문에 제외한다.

IV. 기존 운영체제 보호프로파일과 비교

본 장에서는 기존 운영체제 보호프로파일과 논문에서 제안하는 스마트폰 운영체제 보호프로파일의 비교분석을 통해 스마트폰 운영체제 보호프로파일이 앞서 언급한 고려사항을 어떻게 반영하고 있는지 설명한다.

비교대상이 되는 항목은 OS-PP와 COTS-PP이다. CCOPP-OS는 제한적인 기능을 제공하는 운영체제를 기본으로 하고 있기 때문에, 실제 PC와 유사한 기능을 제공하는 스마트폰 OS와는 차이가 있으므로 제외하였다. 비교항목은 보안문제과 보안기능요구사항으로 두 가지 항목에 대한 비교를 통해 제안하는 스마트폰 운영체제 보호프로파일이 2장에서 언급한 고려사항을 충실히 반영하였음을 논증한다.

4.1 보안문제 비교

위협은 보호프로파일마다 정의 및 서술에 차이가 있기 때문에 정확히 일대일로 대응하기는 어렵다. 그러나 기존 보호프로파일과 제안하는 보호프로파일의 공격유형을 개략적으로 비교하면 부록의 〔표 A-2〕와 같다. OS-PP는 사용자의 과실에 의한 위협, 서비스 거부 공격, 악성코드, 분실의 위협을 포함하고 있지 않다. COTS-PP는 다양한 위협을 포함하고 있으나, 역시 악성코드와 분실의 위협은 언급하고 있지 않음을 확인할 수 있다.

부록의 〔표 A-2〕를 살펴보면 제안하는 보호프로파일에서 독자적으로 설정한 위협은 T.악성코드, T.분실, T.내제된 취약성, T.플랫폼 위변조, 4가지이다. 이는 스마트폰이 다양한 경로를 통해 악성코드에 감염될 수 있으며, 스마트폰은 휴대기기로 분실의 위협이 높다는 점을 반영한 설정이다. 또 사용자가 임의로 플랫폼을 위변조 하거나, 플랫폼에 내재된 취약성을 악용하는 다양한 악성코드에 대응하기 위해 T.내제된 취약성, T.플랫폼 위변조를 추가하였다. COTS-PP에서 다른 보호프로파일과 대응하지 않는 위협 3가지, T.RESIDUAL_DATA, T.UNATTENDED_SESSION, T.UNKNOWN_STATE는 다중 사용자의 세션설정과 관련한 것으로 스마트폰은 단일 사용자 환경이기 때문에 포함하지 않는다.

부록의 〔표 A-3〕은 조직의 보안정책에 대한 비교를 나타낸다. 본 보호프로파일에서는 기존의 보호프로파일과 구분되는 조직의 보안정책 두 가지를 설정하였다. 이는 스마트폰이 개인용 기기라는 특징에서 기인한다. 스마트폰은 개인이 사용하는 기기이기 때문에 기존 보호프로파일들이 정의하고 있는 보안정책, 예를 들어 신뢰된 사용자에게만 접근권한을 허가하고, 역할을 부여하는 등의 보안정책이 무의미하다. 단, 본 보호프로파일은 스마트폰의 취약성 분석 내용을 바탕으

로 스마트폰의 가용성 및 코드 상의 오류를 보완하기 위해 스마트폰 운영체제를 개발하는 조직에서 갖추어야 할 정책 2 가지를 설정하였다.

부록의 〔표 A-4〕는 가정사항에 대한 비교를 나타낸다. 표에서 나타난 바와 같이 제안하는 보호프로파일은 기존 보호프로파일과는 달리 물리적인 보안을 가정사항으로 포함하지 않는다.

보안문제에 대해 종합적으로 살펴보면 본 논문에서 제안하는 스마트폰 운영체제의 보호프로파일은 2장에서 언급한 고려사항, 분실의 가능성과 사용자의 과실 혹은 고의에 의해 발생할 수 있는 위협을 모두 포함하고 있음을 확인할 수 있다.

4.2 보안기능요구사항 비교

본 절에서는 기존 운영체제 보호프로파일과 본 논문에서 제안하는 스마트폰 운영체제 보호프로파일의 보안기능요구사항을 비교한다. 보호프로파일은 보안문제를 바탕으로 보안목적을 도출하고, 보안목적을 중심으로 보안기능요구사항을 다시 도출하는데, 이때 보안목적은 보안기능요구사항의 추상적 개념이므로 본 논문에서는 보안기능요구사항을 통해 실체화된 보안기능을 비교하고자 한다.

부록의 〔표 A-5〕는 보안기능요구사항의 비교를 나타낸다.

〔표 A-5〕에서 COTS-PP의 보안기능요구사항 중 접미어 _EXT가 추가된 항목은 보호프로파일에서 새롭게 정의한 보안기능요구사항을 의미한다. 제안하는 보호프로파일과 COTS-PP의 보호프로파일의 보안기능요구사항 비교에서 차이가 나는 부분은 COTS-PP의 다중 사용자 환경 및 네트워크 환경에 기인한다. 스마트폰은 다중 사용자 환경이 아니며, 네트워크에서 여러 객체에 자원을 할당하고 세션을 설정하는 등 네트워크 기반 환경이 아니기 때문에 해당하는 보안기능요구사항들은 제외하였다. OS-PP와 구별되는 보안기능요구사항들은 스마트폰의 연산성능을 고려하여 보안기능요구사항의 적용을 완화한 것이다.

본 논문이 제안하는 스마트폰 운영체제 보호프로파일이 설정한 새로운 위협, T.악성코드, T.분실은 TOE 보호 클래스의 FTP_TST.1과 암호지원 클래스의 FCS_CKM.1, FCS_CKM.4로 대응하고 있다.

V. 결 론

현대 사회에서 스마트폰은 선택이 아닌 필수다. 사용자는 스마트폰을 통해 PC 환경에서 처리하던 업무를 이제 시간과 장소에 구애받지 않고 처리할 수 있게 되었다. 그러나 다양한 개인정보가 하나의 기기에 집약된다는 보안상의 문제도 점점 커지고 있다. 스마트폰을 분실한다는 것은 통신장비를 하나 잃어버리는 것이 아니다. 내 지갑, 내 이메일, 내 PC에 저장되어 있는 문서, 내 ID와 패스워드 등 개인의 모든 것을 잃어버리는 것과 마찬가지다. 따라서 스마트폰에는 보다 엄격한 보안기준이 적용되어야 하나, 현재까지 마땅한 지침이 없었으며, 스마트폰의 보안을 평가하기 위한 방법론 또한 전무하였다. 이에 본 논문은 스마트폰의 다양한 사용환경을 바탕으로 위협을 도출하고 이에 대응하기 위한 기술과 기술을 평가하기 위한 방법론을 공통평가기준을 통해 제시하였다.

본 논문에서 제안하는 스마트폰 운영체제 보호프로파일은 추후, 공통평가기준 스마트폰 운영체제 평가에 활용될 수 있을 것이다.

참고문헌

〔1〕 http://en.wikipedia.org/wiki/Smartphone

〔2〕 http://www.ebn.co.kr/news/n_view.html?id=487279

〔3〕 http://www.commoncriteriaportal.org/pps

〔4〕 전응렬, 김지연, 이영숙, 원동호, "스마트폰 보안위협과 대응기술 분석", 한국컴퓨터정보학회 논문지 제16권 2호, pp153-163, 2010년 02월.

〔5〕 강동호, 김기영, "개방형 모바일 환경에서 스마트폰 보안기술", 한국정보보호학회지 제19권 5호, pp.21-28, 2009년 10월.

〔6〕 배근태, 김기영, "모바일 단말 보안 운영체제 기술동향", 전자통신동향분석 제23권 제4호, pp.39-47, 2008년 08월.

〔7〕 Collin Richard Mulliner, "Security of Smart Phone", Master's Thesis of University of California, June 2006.

〔8〕 Jengchung V. Chen, David C. Yen, and Kuanchin Chen, "The acceptance and diffusion of the innovative smart phone use:

A case study of a delivery service company in logistics", Information & Management Volume 46, Issue 4, pp.241-248, March 2009.
〔9〕 Asaf Shabtai, Yuval Fledel, Uri Kanonov, Yuval Elovici, and Shlomi Dolev, "Google Android : A State of the Art Review of Security Mechanisms", arXiv 2009, Nov. 2009.
〔10〕 http://seriot.ch/resources/talks_papers/iPhonePrivacy.pdf
〔11〕 http://www.mt.co.kr/view/mtview.php
〔12〕 Andrew Monk, Evi Fellas, and Eleanor Ley, "Hearing only one side of normal and mobile phone conversations", Behaviour & Informaion Technology, Volume 23, Issue 5, pp.301-305, Sep. 2004.
〔13〕 http://threatcenter.smobilesystems.com
〔14〕 Xudong Ni, Zhimin Yang, Xiaole Bai, Adam C. Champion, and Dong Xuan, "DiffUser : Differentiated User Access Control on Smartphones", Mobile Adhoc and Sensor Systems 2009, pp.1012-1017, Oct. 2009.
〔15〕 http://www.dt.co.kr/contents.html?article_no=2011032102010531742001
〔16〕 http://www.dt.co.kr/contents.html?article_no=2011030802011060746001
〔17〕 정한재, 최윤성, 전웅렬, 양비, 김승주, 원동호, "보안 USB 플래시 드라이브 취약점 분석과 CC v3.1 기반의 보호프로파일 개발", 한국정보보호학회 논문지 제17권 6호, pp.99-119, 2007년 12월.
〔18〕 곽진, 홍순원, 이완석, "보안토큰의 취약성/보안요구사항 분석 및 CC v3.1 기반 보호프로파일 개발", 한국정보보호학회 논문지 제18권 2호, pp.139-150, 2008년 04월

부 록

〔표 A-1〕 보안목적의 이론적 근거

	O. 감사	O. 관리	O. 식별및인증	O. 저장데이터보호	O. 전송데이터보호	O. 악성코드차단	O. 네트워크흐름	O. 플랫폼위변조방지	OE. 원격데이터삭제	OE. 안전한외부객체	OE. 사전시험	OE. 업데이트
T.연속인증시도	O		O									
T.위장	O		O									
T.저장데이터훼손			O	O								
T.전송데이터훼손					O							
T.관리부실	O	O	O									
T.악성코드						O					O	
T.분실				O					O			
T.서비스 거부 공격	O						O					
T.내제된 취약성		O										O
T.플랫폼 위변조				O				O				
P.호환성											O	
P.안전한 구현											O	
A.안전한 외부객체					O		O			O		

〔표 A-2〕 위협 비교

제안하는 보호프로파일	OS-PP	COTS-PP
T.연속인증시도/T.위장	T.ACCESS.TSFDATA	T.UNAUTHORIZED_ACCESS
	T.ACCESS.USERDATA	T.MASQUERADE
	T.ACCESS.TSFFUNC	T.TSF_COMPROMISE
	T.ACCESS.COMM	
T.저장데이터훼손	T.IA.MASQUERADE	T.AUDIT_COMPROMISE
	T.IA.USER	T.CRYPTO_COMPROMISE
T.전송데이터훼손	T.RESTRICT.NETTRAFFIC	-
T.관리부실	-	T.ADMIN_ERROR
	-	T.ADMIN_ROGUE
	-	T.OPERATIONAL_ERRORS
	-	T.UNIDENTIFIED_ACTIONS
T.서비스 거부 공격	-	T.RESOURCE_EXHAUSTION
T.악성코드	-	-
T.분실	-	-
T.내제된 취약성	-	T.RESIDUAL_DATA
T.플랫폼 위변조	-	T.UNATTENDED_SESSION
-	-	T.UNKNOWN_STATE

〔표 A-3〕 조직의 보안정책 비교

제안하는 보호프로파일	OS-PP	COTS-PP
P.호환성	-	-
P.안전한 구현	-	-
-	P.ACCOUNTABILITY	P.ACCOUNTABILITY
-	P.USER	P.AUTHORIZATION
-	-	P.ACCESS_BANNER
-	-	P.CRYPTOGRAPHY
-	-	P.I_AND_A
-	-	P.NEED_TO_KNOW
-	-	P.ROLES
-	-	P.TRACE
-	-	P.TRUSTRED_RECOVERY

〔표 A-4〕 가정사항 비교

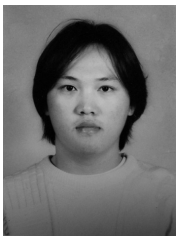
제안하는 보호프로파일	OS-PP	COTS-PP
A.안전한 외부 객체	-	-
-	A.PHYSICAL	A.PHYSICAL
-	A.MANAGE	-
-	A.AUTHUSER	-
-	A.TRAINEDUSER	-
-	A.DETECT	-
-	A.PEERMGT	-
-	A.PEERFUNC	-
-	A.CONNECT	-

〔표 A-5〕 보안기능요구사항 비교

제안하는 보호프로파일	OS-PP	COTS-PP	비고
FAU_GEN.1	FAU_GEN.1	FAU_GEN.1	- 감사데이터 생성
FAU_GEN.2	FAU_GEN.2	FAU_GEN.2	- 사용자 신원 연관
FAU_SAA.1	-	-	- 잠재적 위반 분석
FAU_SAR.1	FAU_SAR.1	FAU_SAR.1	- 감사 검토
FAU_SAR.2	FAU_SAR.2	FAU_SAR.2	- 감사 검토 권한 제한
-	-	FAU_SAR.3	- 선택 가능한 감사 검토
-	FAU_SEL.1	FAU_SEL.1	- 선택적인 감사
FAU_STG.1	FAU_STG.1	FAU_STG.1	- 감사 증적 저장소 보호
-	FAU_STG.3	FAU_STG.3	- 감사 데이터 손실 예측 시 대응 행동
-	FAU_STG.4	-	- 감사 데이터의 손실 방지
-	-	FCS_BCM_EXT.1	- FIPS 140-2 검증을 받은 암호 알고리즘 사용(새롭게 정의)
FCS_CKM.1	FCS_CKM.1	FCS_CKM.1	- 암호키 생성
FCS_CKM.4	FCS_CKM.4	FCS_CKM.4	- 암호키 파기
-	-	FCS_COA_EXT.1	- TOE가 제공해야 하는 암호 알고리즘 목록 정의(새롭게 정의)
FCS_COP.1	FCS_COP.1	FCS_COP.1	- 암호 연산
-	-	FCS_RBG_EXT.1	- TOE가 사용할 난수생성기 정의(새롭게 정의)
FDP_ACC.1	FDP_ACC.1	FDP_ACC.1	- 부분적인 접근통제
FDP_ACF.1	FDP_ACF.1	FDP_ACF.1	- 보안속성에 기반한 접근통제
-	FDP_IFC.2	-	- 완전한 정보흐름 통제
-	FDP_IFF.1	-	- 단일계층 보안 속성

제안하는 보호프로파일	OS-PP	COTS-PP	비고
-	FDP_ITC.2	-	- 보안속성 없이 사용자 데이터 유입
-	FDP_RIP.2	FDP_RIP.2	- 부분적인 잔여정보 보호
-	FDP_RIP.3	-	- 전제적인 잔여정보 보호
FIA_AFL.1	FIA_AFL.1	FIA_AFL_EXT.1	- 인증실패처리 (FIA_AFL_EXT.1은 인증실패에 대한 예시를 상세화)
FIA_ATD.1	FIA_ATD.1	FIA_ATD.1	- 사용자 속성 정의
FIA_SOS.1	FIA_SOS.1	FIA_SOS.1	- 비밀정보의 검증
FIA_UAU.1	FIA_UAU.1	FIA_UAU.1	- 인증
-	FIA_UAU.5	-	- 다중 인증 메커니즘
-	-	FIA_UAU.6	- 재인증
-	FIA_UAU.7	FIA_UAU.7	- 인증 피드백 보호
FIA_UID.1	FIA_UID.1	FIA_UID.1	- 식별
-	FIA_USB.2	FIA_USB.2	- 사용자-주체 연결
FMT_MOF.1	-	FMT_MOF.1	- 보안기능 관리
FMT_MSA.1	FMT_MSA.1	FMT_MSA.1	- 보안속성 관리
-	-	FMT_MSA.2	- 안전한 보안속성
-	FMT_MSA.3	FMT_MSA.3	- 정적 속성 초기화
-	FMT_MSA.4	-	- 보안속성 값 상속
FMT_MTD.1	FMT_MTD.1	FMT_MTD.1	- TSF 데이터 관리
	FMT_REV.1	FMT_REV.1	- 폐지(보안속성 폐지를 의미함)
	-	FMT_SAE.1	- 보안속성 유효기간의 관리
FMT_SMF.1	FMT_SMF.1	FMT_SMF.1	- 관리기능 명세
FMT_SMR.1	FMT_SMR.1	FMT_SMR.1	- 보안역할
-	-	FPT_ITT.1	- 내부 전송 TSF 데이터의 기본적인 보호
-	-	FPT_ITT.3	- 내부 전송 TSF 데이터의 무결성 검사
-	-	FPT_RCV.1	- 수동 복구
FPT_STM.1	FPT_STM.1	FPT_STM.1	- 신뢰된 타임스탬프
-	FPT_TDC.1	-	- TSF 간 전송되는 TSF 데이터의 기본적인 일관성
-	-	FPT_TRC_EXT.1	- 내부 복제 TSF 데이터의 일관성
FPT_TST.1	-	FPT_TST_EXT.1	- TSF 자체시험 - FPT_TST_EXT.1의 경우 앞서 정의한 암호알고리즘 및 난수생성기도 시험할 것을 정의
-	-	FRU_RSA.1	- 자원의 최대할당치
-	-	FTA_MCS.1	- 기본적인 동시 세션 수의 제한
FTA_SSL.1	FTA_SSL.1	FTA_SSL.1	- TSF에 의한 세션 잠금
FTA_SSL.2	FTA_SSL.2	FTA_SSL.2	- 사용자에 의한 세션 잠금
-	-	FTA_TAB.1	- TOE 접근 경고
-	-	FTA_TAH.1	- TOE 접근 이력
FTP_ITC.1	FTP_ITC.1	-	- TSF간 안전한 채널

〈著者紹介〉



전 웅 렬 (Woongryul Jeon) 학생회원
2006년 2월: 성균관대학교 컴퓨터공학과 학사 졸업
2008년 2월: 성균관대학교 전자전기컴퓨터공학과 석사 졸업
2008년 3월~현재: 성균관대학교 전자전기컴퓨터공학과 박사과정
〈관심분야〉 정보보증, 정보보호, 암호이론 등

김 지 연 (Jeeyeon Kim) 종신회원
1995년 2월: 성균관대학교 정보공학과 학사 졸업
1997년 2월: 성균관대학교 컴퓨터공학과 석사 졸업
2008년 2월: 성균관대학교 컴퓨터공학과 박사 졸업
1996년~2007년: 한국정보보호진흥원(現 한국인터넷진흥원) 선임연구원
〈관심분야〉 암호프로토콜, 암호이론, 정보보호관리체계 인증 등

이 영 숙 (Youngsook Lee) 종신회원
1987년 2월: 성균관대학교 정보공학과 학사 졸업
2005년 2월: 성균관대학교 정보보호학과 석사 졸업
2008년 2월: 성균관대학교 컴퓨터공학과 박사 졸업
2009년 3월~현재: 호원대학교 사이버수사경찰학부 교수
〈관심분야〉 암호프로토콜, 암호이론, 네트워크 보안 등

원 동 호 (Dongho Won) 종신회원
1976년~1988년: 성균관대학교 전자공학과 (공학사, 공학석사, 공학박사)
1978년~1980년: 한국전자통신연구원 전임연구원
1985년~1986년: 일본 동경공업대 객원연구원
1988년~2003년: 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장
1996년~1998년: 국무총리실 정보화추진위원회 자문위원
2002년~2003년: 한국정보보호학회장
현재 : 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, IT보안성평가연구회 위원장