DOI: 10.3745/KIPSTC.2009.16-C.1.1

상이한 DRM 시스템의 호환성을 위한 보호프로파일 개발에 관한 연구

조 혜 숙[†] · 이 광 우[††] · 전 웅 렬[††] · 이 윤 호[†††] · 김 승 주[††††] · 원 동 호[†††††]

요 약

오늘날 DRM(Digital Right Management)은 악의적인 사용자에 의한 디지털 콘텐츠의 재배포, 불법 복제를 금지시키기 위해서 사용되고 있다. 그러나 여전히 현재 DRM 시스템은 상호 호환성 부족으로 인해 사용자의 불편을 초래하고 있다. 이를 해결하기 위해 상이한 DRM 시스템의 상호 호환을 위한 연동 방안이 제시되고 있다. 본 논문에서는 상이한 DRM 시스템 호환을 위해서 공통평가기준에 따른 보호프로파일을 개발한다. 특히 이러한 개발을 위해 기존에 개발된 보호프로파일을 이용해서 개발에 적용시킴으로써 시간 효율과 비용 측면에서의 효율적임을 분석을 통하여 보인다. 개발된 보호프로파일은 콘텐츠 제공자 및 사용자 권한을 관리하는 관리자가 안전한 저작권을 유지할 수 있는 요구사항을 도출할 때 참고 자료로 활용 될 수 있다.

키워드 : 디지털 저작권 관리, 보호프로파일, 공통평가기준, 콘텐츠, 저작권

A Study on Development to Be Protection Profile for Interoperability of Heterogeneous DRM Systems

Heasuk Jo[†] · Kwangwoo Lee[††] · Woongryul Jeon[††] · Yunho Lee[†††] · Seungjoo Kim[††††] · Dongho Won[†††††]

ABSTRACT

Today, Digital Right Management (DRM) is used to protect copyrights of digital contents from illegal reproduction and redistribution. Unfortunately, current DRM systems are causing user's discomfort because of lack of mutual compatibility. In order to overcome this drawback, technologies for interoperability of heterogeneous DRM systems are developing. In this paper, we study the protection profile for conversion technologies of heterogeneous DRM systems, using the Common Criteria. Especially, this paper is written by reuse of the existing protection profile. Therefore, performance analysis reveals that efficiency of time and cost is significantly improved. This protection profile can be used by contents provider and administrator who manage user's copyrights to reference data for copyright protection.

Keywords : Digital Right Management, Protection Profile, Common Criteria, Contents, Copyrights

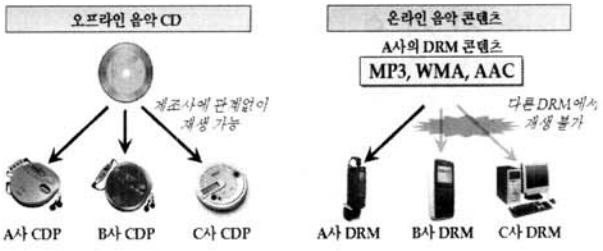
1. 서 론

DRM (Digital Rights Management)은 지적 재산권이 디지털 방식에 의해서 안전하게 보호 및 유지 되도록하는 디지털 콘텐츠 저작권 보호 기술로서, 불법 복제나 배포로 인한 저작권 침해를 막기 위해 사용된다. 이러한 DRM 기술은 1980년대부터 개발되기 시작했으며, 근래에 들어 음악, 영화 등 기존 엔터테인먼트 콘텐츠의 디지털화가 급증하면서 사용이 일반화되고 있다.

디지털 콘텐츠의 생산과 유통이 활성화되기 위해서는 DRM과 같은 불법 복제·유통을 막는 기술적인 보완 장치가 필수적이지만, 현재의 DRM 기술은 콘텐츠 소유자의 권익을 보호하기 위한 측면만 강조되고 콘텐츠를 구매한 소비자의 권리는 간과하는 측면이 있다. 예를 들어 기존 오프라인 콘텐츠 유통에서 음악 CD를 구입한 소비자는 자신이 어떠한 플레이어를 사용하더라도 구입한 CD를 자유롭게 재생하여 즐길 수 있다. 하지만 현재 DRM이 적용되어 유통되는 디지털 음악 콘텐츠는 구입 당시 지정된 DRM 솔루션을 탑재한 플레이어 외에는 사용할 수 없는 상황이다(그림 1).

† 정 회 원 : 성균관대학교 전자전기컴퓨터공학과 박사과정
†† 준 회 원 : 성균관대학교 전자전기컴퓨터공학과 박사과정
††† 준 회 원 : 성균관대학교 전자전기컴퓨터공학과 박사
†††† 종신회원 : 성균관대학교 정보통신공학부 부교수
††††† 종신회원 : 성균관대학교 정보통신공학부 교수(교신저자)

논문접수 : 2008년 11월 13일
수 정 일 : 1차 2008년 12월 10일, 2차 2008년 12월 17일
심사완료 : 2009년 1월 3일



(그림 1) 오프라인과 온라인의 콘텐츠 사용 비교

즉, 온라인을 통해 A사의 DRM 기술이 적용된 디지털 콘텐츠를 구입하였다면 A사 단말에서는 이용 가능하지만 B사의 DRM 기술이 적용된 단말에서 이용 불가능하고 B사의 DRM이 적용된 콘텐츠를 별도로 구입해야 하는 문제가 발생하게 된다. 이는 콘텐츠나 단말기에 대한 사용자의 선택권이 DRM 솔루션에 의해 제약을 받는다는 것을 의미하는 것으로 온라인 디지털 콘텐츠 유통을 활성화하기 위한 DRM 솔루션이 오히려 저해 요인으로 작용하는 것을 의미한다.

이러한 문제를 해결하기 위해 여러 가지 기술이 개발 중이고 그중에 한국전자통신연구원(ETRI, Electronics and Telecommunications Research Institute)에서 상이한 DRM 간 콘텐츠 상호 연동기술규격인 EXIM(EXport and IMport)을 개발하였다. 1단계 적용모델로 MP3 콘텐츠의 DRM 연동을 위한 기술규격과 구축사례를 발표하였고, 이 기술은 DRM 호환성 결여 문제로 인해 발생하는 사용자의 불편을 해소할 것으로 예상하고 있다. 또한 콘텐츠 유통 시장을 활성화하기 위해 시작된 DRM 연동 기술의 개발은 기존 DRM 업체 또는 표준단체의 기술을 그대로 유지하면서도 디지털 콘텐츠를 이기종의 DRM 포맷으로 변환할 수 있도록 하였다.

그러나 현재 EXIM과 같은 제품은 IT 보안성에 대한 보호프로파일이 존재하지 않는다. 보호프로파일이란 보안기능이 있는 IT 제품에 대해서 보안에 관한 일반적인 요구사항을 서술한 문서이다. 더 자세한 내용은 다음 장에서 설명한다. 따라서 본 논문에서는 상이한 DRM 간 콘텐츠 상호 연동기술규격에서 필요한 표준화된 보호프로파일을 개발하는 것을 목적으로 한다. 이는 현재 전 세계적으로 가장 잘 알려진 제품과 시스템에 대한 보안성 평가기준인 ISO/IEC 15408로 표준화된 공통평가기준(CC, Common Criteria)[2-4]을 사용한다. 또한 보호프로파일은 재사용이 가능하기 때문에 기존의 개발된 보호프로파일을 이용해서 개발할 상이한 DRM 기술의 호환을 위한 보호프로파일(IHD_PP, Interoperability Heterogeneous DRM Protection Profile)에 적용시킴으로써 시간 효율과 비용 측면에서의 효율성을 갖는다.

본 논문의 2장에서는 CC, PP 및 EXIM에 대한 개념과 기존 DRM 호환 system에 대해서 설명한다. 3장에서는 상이한 DRM system을 위한 보호프로파일을 TOE(Target Of Evaluation) 설명, TOE 환경, TOE 보안목적, 보안목적의 이론적 근거로 나누어 설명한다. 4장에서는 기존의 보호프로파일을 재사용 함으로써 얻을 수 있는 장점 및 고려사항을 분석하고 5장에서는 결론을 맺는다.

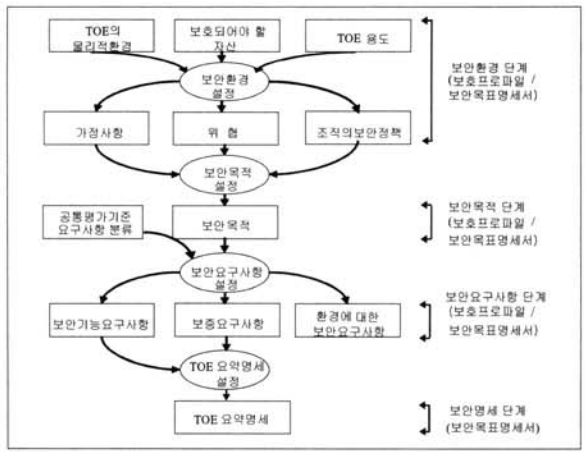
2. 관련연구

2.1 공통평가기준 및 보호프로파일(CC:Common Criteria, PP:Protection Profile)

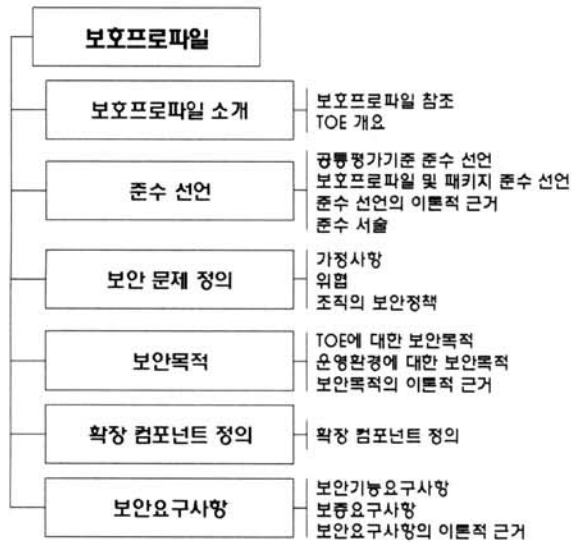
공통평가기준(CC, Common Criteria)은 보안 기능이 있는 IT 제품이나 시스템의 보안성을 평가하기 위한 공통의 요구사항을 제시한 기준으로서 미국, 영국, 프랑스 등 선진국이 참여하여 각국의 보안평가 기준을 하나로 통합 및 일원화하여 개발하고 있다. CC의 기본 개념을 더 자세히 살펴보면, 각 국의 서로 다른 평가 기준을 연계하고 평가 결과를 상호 인증하기 위해 1993년 6월 공통평가기준(Common Criteria)를 제정을 합의하고, 이어 1996년 1월 공통평가기준 버전 1.0이 발표됐다. 1998년 5월 버전 2.0이 발표되면서 ISO/IEC JTC1/SC27/WG3에서 국제 표준으로 승인되었다. 이후 현재의 버전 2.3 및 버전 3.1[2-4]에 이르기까지 지속적으로 개선 및 개정되어 왔으며, 주요 개발 연혁은 다음과 같다.

- 1998년 5월 : CC 2.0
- 1999년 12월 : CC 2.1 (ISO 15408:1999)
- 2004년 1월 : CC 2.2 (ISO FCD)
- 2005년 5월 : CC 2.3 (ISO 15408:2005) (현재 공식 평가기준)
- 2005~2006년 8월 : CC 3.0 개발 및 공개 검토 (비공식 평가기준)
- 2006년 9월 : CC 3.1 (공식 평가기준)

정보보호시스템 평가의 기본이자 핵심인 PP는 시스템이나 제품에 대한 평가대상(TOE, Target Of Evaluation:평가의 대상인 IT 제품이나 시스템과 관련된 설명서)을 설정하고, TOE의 보안문제에 대응하기 위한 보안요구사항을 기술한 문서로써, 시스템 개발자, 시스템 조달자 사이의 커뮤니케이션 수단으로 사용된다[9]. (그림 2)는 PP를 개발하기 위한 보안요구사항 및 보안명세에 대한 도출 과정을 표현하고 있다. TOE 보안요구사항은 일반적으로 보안문제정의와 보안목적을 고려하여 도출하고, 이러한 보안요구사항은 보호프로파일/보안목표명세서를 작성하는 기초자료가 된다. PP는 공통의 요구사항을 정의하고자 하는 사용자, IT 제품 개발자 등에 의해서 개발될 수 있으며, 소비자에게 보안에 필요한 사항을 설명하는 수단이 될 수 있다. 또한 이미 작성된 PP는 새로운 PP를 작성할 때 기초자료로 이용될 수 있으며, 보안목표명세서를 작성하는 기초자료로도 사용될 수 있다[2]. (그림 3)은 CC 3.1의 PP 주요 구성요소 및 설명을 나타난다.



(그림 2) 요구사항 유도과정[2]

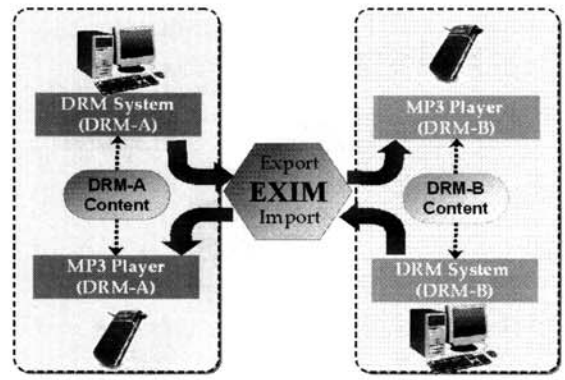


(그림 3) 보호프로파일의 구성요소

2.2 EXIM

기존의 DRM 시스템에서, 사용자는 서로 다른 콘텐츠 제공자에게 구입한 콘텐츠를 하나의 기기에서 실행을 시도할 때 실행할 수 없거나 각기 다른 해당 콘텐츠 제공자가 제공하는 소프트웨어를 설치해야만 실행할 수 있다. 이러한 호환성 결여 문제를 해결하기 위해 한국전자통신연구원(ETRI)은 DRM 연동기술인 EXIM을 개발하였다. EXIM은 사용자의 불편을 해소하고 콘텐츠 유통 시장을 활성화하기 위함이고, 기존 DRM 업체 또는 표준단체의 기술을 그대로 유지하면서도 디지털 콘텐츠를 이기종의 DRM 포맷으로 변환할 수 있도록 한다.

(그림 4)는 상이한 DRM간 콘텐츠의 상호 연동할 수 있는 EXIM의 개념을 나타낸다. 예를들어 A DRM system에서 다운받은 콘텐츠는 DRM A의 MP3 기기에서는 아무런 문제없이 실행이 가능하다. 하지만 B DRM system을 사용하는 기기에서 사용하려면 EXIM 반출(Export)을 통해서 즉 DRM A의 EXIM 모듈을 통해 중립 포맷인 EXIM 포맷으로



(그림 4) EXIM 개념

변환하여 DRM B 기기에 전송하게 된다. 이를 전송받은 DRM B 기기는 같은 방식으로 EXIM 모듈을 통해 EXIM 포맷을 자신에게 맞는 포맷 즉 DRM B 포맷으로 변경 후에 실행을 할 수 있게 된다.

2.2.1 EXIM 프로세스

다음은 [5]에서 기술한 EXIM 프로세스에 대한 설명이다. 상이한 DRM간 연동을 위한 중립적인 DRM 콘텐츠 포맷은 콘텐츠에 대한 메타데이터, 사용권한, 암호화된 리소스 이 세 가지를 저장하고 있다. (그림 5)는 상이한 DRM간 콘텐츠를 전송하는 절차를 나타낸다.

- o 소스 DRM 측 프로세스(Source DRM Client : 콘텐츠 보내려고 하는 기기)[5]

① 소스 DRM은 자신의 DRM 콘텐츠를 언패키징하여 메타데이터, 사용권한, 원본 리소스를 추출

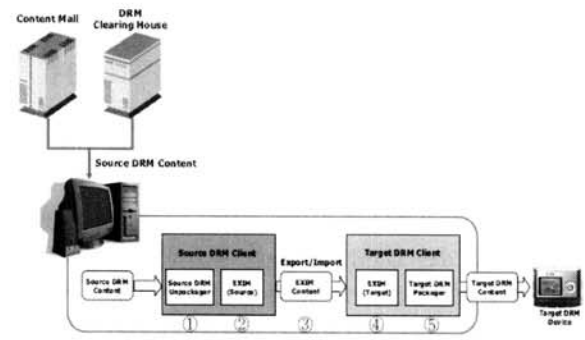
② 메타데이터, 사용권한, 원본 리소스를 이용하여 중립 포맷 DRM 콘텐츠로 패키징

③ 중립 포맷 DRM 콘텐츠를 타겟 DRM(상이한 DRM 콘텐츠를 받으려고 하는 기기)으로 Export

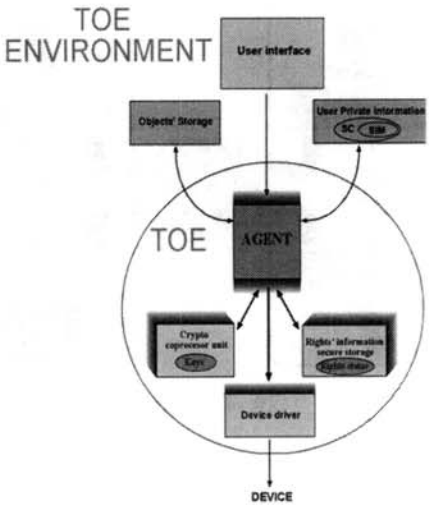
- o 타겟 DRM 측 프로세스(Target DRM Client)

④ 소스 DRM으로부터 Import한 중립 포맷 DRM 콘텐츠를 언패키징하여 메타데이터, 사용권한, 원본 리소스를 추출

⑤ 추출된 메타데이터, 사용권한, 원본 리소스를 타겟 DRM 고유의 DRM 콘텐츠 형태로 패키징 후 해당 기기에 전송



(그림 5) EXIM 프로세스[5]



(그림 6) MPDRM_PP의 TOE 정의

2.3 Mobile Phone DRM PP

Mobile Phone DRM PP(MPDRM_PP, [6])는 UMTS(Universal Mobile Telecommunications System) 무선 네트워크 환경에서 콘텐츠 관리를 위한 보호프로파일 개발을 목적으로 한다. 또한 기존의 Smart Card PP(SCPP, [11])와 Backbon Router PP(BRPP, [12])를 재사용 하여 MPDRM_PP를 생성한다. MPDRM_PP의 TOE는 [13-16]을 기초로 하여 TOE 환경(User interface, User Private Information, Objects' Storage)과 TOE 구성(MPDRM-Agent, Crypto Co-Processor Unit, Right's information secure storage, Device drivers)으로 이루어져 있다(그림 6).

2.4 상이한 DRM에 관한 호환성 연구

상이한 DRM에 대한 호환성을 위한 DRM system으로 Apple iTunes' Fairplay[17], Secure Digital Container[18], Windows Media DRM[19], The Advanced Access Content System[20], The Open Mobile Alliance's DRM scheme[21], PachyDRM[22] 등이 연구되고 있다.

DRM간 호환성을 위한 방안으로 크게 세 가지로 구분 할 수 있다[23].

- o 표준 DRM system 제정 방안(Full-format inter-operability) : 글로벌한 하나의 DRM 표준 기준을 제정하여 적용하는 방법
- o DRM 간 인터페이스 규격 제정 방안(Configuration-driven inter-operability) : End user 사이에 인터페이스 규격(Tools)을 이용하여 데이터를 변경하는 적용 방법
- o 제3기관을 이용하는 방안(Connected inter-operability) : 온라인을 통해서 제 3기관(서버 등)을 이용하여 원하는 규격으로 데이터를 변경하는 방법

첫 번째 방안으로 표준 DRM system을 제정하는 것은 현재 존재하고 있는 DRM system을 통일하는 것으로 사실상 표준제정에 어려움을 갖고 있다. 두 번째 DRM 간 인터페이스 규격 제정은 기존의 DRM system을 사용하면서 연동 인터페이스를 이용하여 데이터를 변경하는 방법으로 DRM 기업들의 협력으로 개발 가능성이 있다고 할 수 있다. 세 번째 제3기관 이용 방안은 온라인을 통한 제3기관을 이용하여 데이터를 변경하는 방안으로 이 또한 이용 가능하다.

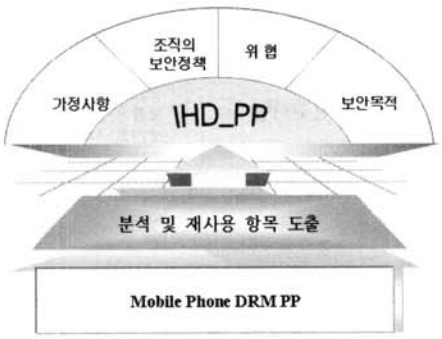
3. 본 론

3.1 상이한 DRM 시스템을 위한 보호프로파일

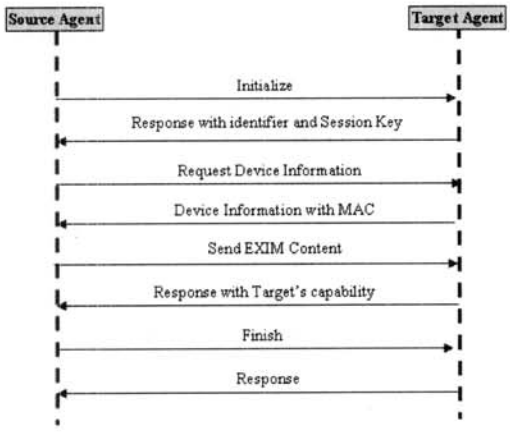
3.1.1 개 요

본 장은 상이한 DRM 기술의 호환을 위한 PP(IHD_PP, Interoperability Heterogeneous DRM Protection Profile)를 개발하는데 DRM간 인터페이스 규격(Configuration-driven inter-operability)을 따르는 EXIM을 이용한다. 본 논문은 기존의 상이한 DRM 호환성 연구결과를 가지고 요구사항 유도과정을 도출해 내야 정확하지만 각 기술마다 상세한 부분은 공개되지 않기 때문에 부득이 하게 제한된 기술을 가지고 요구사항을 도출하게 된다. 그리고 MPDRM_PP, [6,8]을 활용하여 IHD_PP를 개발 한다. IHD_PP는 TOE(Target Of Evaluation) 설명, TOE 환경, 보안문제 정의, 보안목적 그리고 보안목적의 이론적 근거로 구성된다.

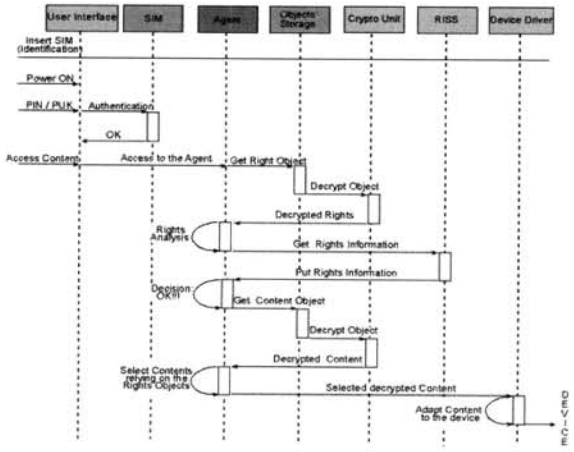
- o MPDRM_PP 활용 범위 : 개발하고자 하는 PP는 상이한 DRM 시스템의 호환 기술에 대한 부분이기에 MPDRM_PP에서의 권한정보 전송, Agent를 통한 암호화 방식, 인증서 발급 등의 공통점을 가지고 있는 이 부분을 활용한다.



(그림 7) 기존 보호프로파일 재사용



(그림 8) EXIM 처리과정[5]



(그림 9) Mobile Phone DRM 처리과정[6,13]

(그림 8)과 (그림 9)는 Mobile Phone DRM의 처리과정과 상이한 DRM 시스템의 호환을 위한 EXIM 처리과정을 나타낸다.

3.1.2 TOE 설명

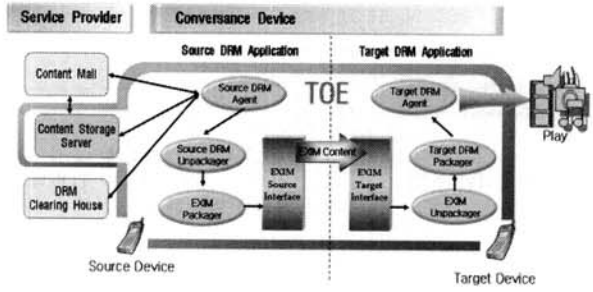
TOE 설명은 TOE에 대한 일반적인 정보를 제공하고, TOE 기능 및 TOE 범위에 대하여 설명하여 TOE 보안요구사항 및 사용목적을 이해할 수 있도록 설명한다. 즉 TOE가 보호하고자 하는 자산은 무선 단말기 또는 데스크탑에서 상이한 DRM 시스템을 탑재하고 있는 기기로 콘텐츠를 전송할 때 또는 다운 받을 때의 저작권 관리 측면에서의 콘텐츠, TOE 내부의 중요 데이터(보안 속성, TSF(TOE Security Function, TOE보안기능) 데이터 등), TOE 자체를 말한다[1, 2].

o TOE 환경

- Content Mall(CM) : 콘텐츠 제공자와 같은 역할을 한다. 사용자는 DRM agent를 통해서 Content Mall에 접속해서 사용자가 원하는 콘텐츠를 선택한다. 그 다음 그 콘텐츠에 대한 과금 처리가 이뤄지고 그 후 Content Mall은 Content Storage Server에 접속해서 사용자에 대한 콘텐츠 권리 Object (Right Object, RO)를 전송한다. RO는 사용자가 선택한 콘텐츠의 사용에 대한 "권리 정보" 즉 사용 기간, 사용 횟수 등의 사용 권한이 저장되어 있다.
- DRM Clearing House(DCH) : DCH에서는 사용자에게서 받은 DRM 콘텐츠에 대한 RO 토큰과 RO 정보 요청을 받은 후 RO 정보를 갱신 후 DRM Agent에게 전송한다.

o TOE 구성요소(그림 10)

- DRM Agent(DA) : DA는 소스 디바이스와 타겟 디바이스에 탑재된다. 여기서 소스 DA란 콘텐츠 사용 권한을 가지고 있고 이 콘텐츠를 다른 디바이스에게 전송할 디바이스를 말하고, 타겟 DA란 소스 DA에서 콘텐츠와 그에 해당하는 권한을 전송받으려고 하는 디바이스이다. DA는 콘텐츠의 전송, RO, 서비스 정보 등을 CM, CSS, DCH와 연결하여 제공받는다.



(그림 10) TOE 구성

- DRM Unpackager와 Packager(DU, DP) : 소스 디바이스의 DU에서는 CSS에서 받은 DRM 콘텐츠를 언패키징하여 메타 데이터, 사용권한, 원본 리소스를 추출한다. 타겟 디바이스의 DP에서는 ETI에서 언패키징한 메타데이터, 사용권한, 원본 리소스를 타겟 디바이스에 적합한 DRM 콘텐츠로 패키징 한다.
- EXIM Unpackager와 Packager(EU, EP) : 소스 디바이스의 EP는 DU에서 받은 메타 데이터, 사용권한, 원본 리소스를 EXIM 포맷에 맞게 변환 후 패키징 한다. 타겟 디바이스의 EU는 EXIM 포맷을 언패키징 해서 추출된 데이터를 DP에게 전송한다.
- EXIM Interface(EI) : 소스 디바이스의 EI는 타겟 디바이스의 EI와 EXIM 포맷으로 패키징된 데이터를 주고받는 역할을 한다.
- Content Storage Server(CSS) : CSS는 콘텐츠를 저장하고 있다. 그리고 독립적인 서버로 존재할 수도 있고, CM에 속할수 있고, 사용자 디바이스에 존재할 수도 있다. 예를 들어 네트워크 스토리지, 일반 PC, USB와 같은 이동 장치가 있다.

3.1.3 보안문제 정의

TOE 보안 환경은 TOE 보안 환경에 미치는 잠재적인 위협, 조직의 보안정책, 가정사항을 도출 한다. 본 장에서는 IHD_PP에서 필요한 보안문제를 정의하고 필요시 MPDRM_PP를 활용하여 IHD_PP에 적합한 항목을 재사용하여 기술한다. 각 재활용 식별 마크로는 새로 도출한 IHD_PP의 요구사항은 "New"로 표시하고 MPDRM_PP에서 재사용된 항목은 "M"으로 표시한다.

3.1.3.1 위협(Threats)

본 절에서 기술하는 위협은 TOE가 보호하고자 하는 콘텐츠 및 사용자 정보에 대한 내.외부적인 위협을 나열한다. 특히 위협원은 비정상적인 방법으로 TOE 및 내부의 자산에 해를 가하는 외부 실체 및 사용인 또는 외부에서 TOE 및 내부의 자산에 불법적인 접근을 시도하는 것 등이다. <표 1>은 위협에 대한 항목이다.

〈표 1〉 위협

이 름	설 명	비고
T.논리적인 공격	위협원은 논리적인 인터페이스를 악용해서 사용자 데이터나 TSF 데이터를 변경, 노출할 수 있다. 논리적인 인터페이스는 TOE와 소스 디바이스 또는 CSS 간 데이터 교환을 악용해 구문이나 해석 차이를 악용하거나, 특정한 사용을 위한 명령어를 악용하여 공격한다.	New
T.권리_수정	위협원은 RO의 사용자 정보를 변경, 노출하여 정보를 악용할 수 있다.	New
T.불법프로그램	인가된 사용자가 악의적인 코드가 포함된 응용프로그램을 TOE에 불법적으로 설치하여 사용자 데이터나 TSF 데이터를 변경, 노출할 수 있다.	New
T.고장	TOE가 사용중이나, 외부 공격 등에 의해 고장이 발생하여 사용자에게 정상적인 서비스를 제공하지 못하게 할 수 있다.	New
T.자원공유충돌	위협원은 다른 응용프로그램의 실행 영역을 침범하여 디바이스에 오동작을 유발하거나, 사용자 데이터나 TSF 데이터를 변경, 노출할 수 있다.	New
T.비의도적고장	콘텐츠를 전송받는 도중 또는 RO 정보를 전송받는 중 전원 공급이 중단되거나, 충격 등으로 TSF 서비스가 불완전하게 종료되어 사용자 데이터 및 TSF 데이터가 노출 및 손상을 위협원이 악용할 수 있다.	New
T.잔여정보	TOE가 자원을 재사용할 경우, 객체의 정보를 적절하게 제거하지 못해 위협원이 정보에 불법적으로 접근할 수 있다.	New
T.정보누출	위협원은 TOE를 정상적으로 사용하는 동안 TOE로부터 누출된 정보를 악용할 수 있다.	New
T.불법기기사용	위협원은 인가되지 않은 디바이스를 이용해서 사용자 데이터나 TSF 데이터를 변경, 노출할 수 있다.	New
T.교체	TOE의 일부를 물리적으로 교체할 수 있다.	M
T.조작	위협원은 TOE에게 조작된 정보를 전달함으로써 TSF 정보를 취득할 수 있다.	M
T.권리남용	원본이 아닌 RO정보나 일반적인 RO 정보를 콘텐츠 취득에 사용할 수 있다.	M
T.암호공격	위협원은 brute force 공격을하거나 알고리즘에 대해 암호 공격을 함으로써 TSF 위협할 수 있다.	M
T.리스트_수정	위협원은 타겟 디바이스에 대한 서비스 및 금지 리스트 업데이트 시 이를 조작할 수 있다.	New
T.시스템 오류	사용자 에러, 하드웨어 에러, 전송 에러 등의 시스템 에러가 발생 했을 때 TOE에 의해 보호되는 콘텐츠, 사용자 정보 또는 서비스가 제공될 수 있다.	New
T.데이터 공격	위협원은 RO 없이 특정 콘텐츠에 접속하기 위해 특정 콘텐츠에 암호해독 공격을 시행한다.	M
T.정보유출(1)	위협원은 일반적인 사용시 TOE에서 유출되는 TSF 정보를 획득할 수 있다.	M
T.부인	위협원은 인가된 사용자에게 서비스 또는 정보를 얻고서 그것에 대한 송수신 사실을 부인할 수 있다.	New
T.정보유출(2)	위협원은 TOE와 외부 상호작용에 대해 유출시킬 수 있다.	M
T.특권남용	인증된 사용자나 관리자가 자신이 가지고 있는 특권을 가지고 보안기능 또는 보호되어야 하는 데이터 실행을 통해 TSF 데이터 또는 사용자 데이터를 공격하거나 남용할 수 있다.	M
T.감사정보파괴	특별한 행동을 한 인가된 사용자의 감사정보가 보안정책에 따르지 않고 삭제될 수 있다.	New
T.TOE 오류	소스 디바이스가 타겟 디바이스에게 사용자 정보 또는 콘텐츠 정보를 보내는 동안에 시스템 오류로 인해서 TOE 보안 상태가 보내는 정보와 일치하지 않을 때 TSF는 옳게 작동하지 않을 수 있다.	New

3.1.3.2 조직의 보안정책(Organizational Security Policies)

조직의 보안정책은 IHD_PP를 수용하는 TOE의 운영환경에 적용되어야 하는 조직의 보안정책 사항을 나타낸다. <표 2>는 조직의 보안정책에 대한 항목이다.

3.1.3.3 가정사항(Assumption)

TOE의 운영환경에서 시행되거나 유지되어야 하는 가정사항을 보여준다. TOE가 가정사항을 만족시키지 못하는 운영환경에 설치될 경우, TOE는 모든 보안 기능성을 제공할 수 없게 될 것이다[2]. 가정사항은 운영환경의 물리적, 인적 및 연결성 측면을 포함한다. <표 3>은 가정사항에 대한 항목이다.

3.1.3.4 보안목적

본 장에서는 보안목적을 TOE 보안목적 및 환경에 대한 보안목적으로 분류하여 정의한다. TOE 보안목적은 TOE에 의해서 직접적으로 다루어지는 보안목적이고, 환경에 대한 보안목적은 IT 영역이나 비기술적/절차적 수단에 의해 다루어지는 보안 목적이다. TOE 보안목적은 "E" 인덱스로, 환경에 대한 보안목적은 "OE"로 표기한다. <표 4>는 보안목적에 대한 항목이다.

3.1.3.5 보안목적의 이론적 근거

보안목적의 이론적 근거는 명세한 보안목적이 적합하고 보안문제를 다루기에 충분하며, 과도하지 않고 반드시 필요한 것임을 입증하는 것이다. 보안목적의 이론적 근거는 다음을 입증한다. <표 5>는 보안목적의 이론적 근거를 나타낸 표이다.

- o 각 가정사항, 위협, 조직의 보안정책이 최소한 하나의 보안목적에 의해서 다루어진다.
- o 각 보안목적은 최소한 하나의 가정사항, 위협, 조직의 보안정책을 다룬다.

〈표 2〉 조직의 보안정책

이 름	설 명	비고
P.감사	보안과 관련된 모든 행동에 대한 책임을 추적[3]하기 위해 보안관련 사건은 기록 및 유지되어야 하며, 기록된 데이터는 검토가 되어야 한다.	New
P.암호	타겟 디바이스와 소스 디바이스간 키교환시 암호화 알고리즘은 승인된 암호 알고리즘 및 모듈을 사용하여야 한다.	New
P.가이드	CM(Content Mall)은 사용자가 어떤 방식으로 사용 서비스를 이용해야 하는지 그 가이드라인을 제공해야 한다.	M
P.업데이트	사용자 디바이스는 CM에 접속하여 상이한 DRM 시스템을 변환하기 위한(EXIM과 같은 소프트웨어) 소프트웨어 업데이트 받아야 한다. 이 때 디바이스의 DA(DRM Agent)는 필요시 자동적으로 소프트웨어를 다운받을 수 있어야 한다.	New

〈표 3〉 가정사항

이 름	설 명	비고
A.안전한 경로	TOE와 TOE의 통신 상대인 디바이스는 안전한 경로와 채널[3]에서 통신을 한다.	New
A.TSF 데이터	TOE 운영 과정에서 TOE 외부로 유출되어 처리되는 TSF 데이터[3]는 안전하게 관리된다.	New
A.물리적보안	TOE는 안전한 파워와 클럭을 유지한다.	M
A.신뢰된 관리 및 사용	TOE의 인가된 관리자 및 사용자는 악의가 없으며, TOE 관리 기능에 대하여 적절한 교육을 받고, 관리자 지침에 따라 의무를 수행한다.	New
A.운영체제보강	TOE에 필요하지 않은 운영체제상의 서비스나 수단 등을 제거하는 작업과 운영체제상의 취약점에 대한 보강 작업을 수행하여 운영체제에 대한 신뢰성과 안전성을 보장한다.	New
A.키관리	모든 중요한 암호키는 안전한 방법으로 보관된다.	M
A.불법수정차단	TOE에 악의적인 사용자에 의해 TOE의 내용이 변경되었을 때 TOE는 차단되고 컴포넌트들은 재저장된다.	M
A.인증기관	타켓 디바이스와 소스 디바이스 간의 키 교환시 인증서를 발급 받는다면 발급 기관은 신뢰할 수 있는 인증기관이다.	New

〈표 4〉 보안목적

이 름	설 명	비고
OE.안전한 통신	TOE 통신하는 컴포넌트는간에는 안전한 경로를 제공해야 한다.	New
OE.TSF데이터	TOE가 운영되는 과정에서 TOE 외부로 유출되어 처리되는 TSF 데이터는 안전하게 관리되어야 한다.	New
OE.물리적보호	TOE는 물리적으로 공격에 내구성이 있어야 하고, 공격이 어디서 이루어 졌는지 알아낼 수 있어야 한다.	M
EO.가이드	CM은 사용자가 콘텐츠 DRM 서비스를 받을 수 있는 가이드라인을 사용자가 알기 쉽게 제공해야 한다. 또한 사용자 및 관리자의 사용시 주의사항 및 의무에 대해서 명시되어야 한다.	New
OE.운영체제보강	TOE에 의해 필요하지 않은 운영체제상의 서비스나 수단 등을 제거하는 작업과 운영체제상의 취약점에 대한 보강 작업을 수행하여 운영체제에 대한 신뢰성과 안전성을 보장해야 한다.	New
OE.키관리	모든 수집된 암호키는 사용자의 필요에 따라 제공되어야 한다.	M
OE.인증기관	사용자는 신뢰할 수 있는 CA 인증기관을 통해서 인증서 등을 발급받는다.	New
OE.물리적안전성	잘못된 데이터를 삽입으로 연속된 프로빙(probing)에도 견뎌야(resistant) 한다.	M
O.감사	TOE 보안을 위협하는 잠재적인 위협원에게서 보호되기 위해 디바이스는 저장된 보안관련 정보를 갖는다.	New
O.암호	TOE는 암호화 사용 정책과 표준을 따르는 암호 기능(function)을 사용해야 한다.	New
O.업데이트(1)	소프트웨어는 주기적으로 업데이트 되어야 한다.	New
O.업데이트(2)	TOE 시스템 오류 등으로 오 동작시 이를 감지하고 재설치 되고 업데이트 되어야 한다.	New
O.데이터 보호(1)	사용자 권리와 콘텐츠는 안전하게 암호화되어야 하고 저장되어야 한다.	New
O.데이터 보호(2)	TOE는 저장된 데이터를 인가되지 않은 노출, 변경 삭제로부터 보호해야 한다.	New
O.데이터 보호(3)	TOE는 인가된 사용자만이 사용자 데이터 및 TSF 데이터에 접근 및 수정할 수 있도록 보장해야 한다.	New
O.설치	인가되지 않은 소프트웨어는 설치되지 않아야 한다.	New
O.정보누출대응	TOE는 TOE를 정상적으로 사용시 누출되는 정보를 악용하지 못하도록 대응책을 구현해야 한다.	New
O.불법변경감지	TSF는 불법변경 감지를 위한 소프트웨어 또는 하드웨어를 가지고 있어야 한다.	M
O.인가된고장수리	TOE는 내부 저장된 데이터 보호를 위해 인가된 사용자만이 고장수리를 할 수 있도록 보장해야 한다.	New
O.인증 및 식별	사용자가 TOE 사용자 데이터 및 TSF 데이터에 접근 시도 시 인증과정을 거쳐야 한다. TOE는 논리적인 인터페이스를 사용할 수 있는 사용자와 역할에 따라 사용할 수 있는 사용자 식별을 명확하게 해야 한다.	New
O.잔여정보제거	TOE는 TSF가 사용하는 작업영역에 사용 종료시 사용자 데이터나 TSF 데이터를 남기지 않는 것을 보장해야 한다.	New
O.권한	TOE는 DCH에서 암호화된 RO(Rights Objects)만 수락한다. RO에는 개인 정보가 저장되어 있다.	New
O.환경적 스트레스	환경적인 스트레스(stress)로 TOE 상황에 대한 보안 정보의 노출을 막아야 한다.	M
O.초기화	TOE는 power up, reset, restart 후에 즉시 초기화를 취해야 한다.	M
O.흐름정보	TOE는 보안정책에 따라 인가되지 않은 정보 흐름을 통제해야 한다.	New
O.논리적보호	TOE는 논리적인 속임이나 수정에 대해서 스스로를 보호할 수 있어야 한다.	M
O.라이프싸이클	TOE는 의도에 의한 리이프 싸이클(life cycle) 활동의 Object, 의미있는 테스트와 디버그 사용을 제안하고 제어하는 수단을 제공해야 한다.	M
O.Brute_Force	보안정보를 찾기위한 brute force 공격(암호등을 알아내기 위해 모든 경우의 수를 체크하는 방법)으로 연속는 입력 공격으로부터 보호되어야 한다.	M

〈표 5〉 보안목적의 이론적 근거

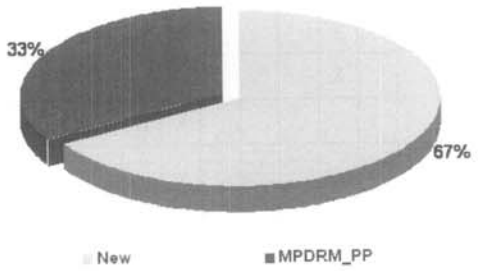
보안문제 정의 \ 보안목적	OE. 안전한 통신	OE. TSF 데이터	EO. 물리적 보호	EO. 가이드	OE. 운영체제 보강	OE. 키관리	OE. 인증기관	OE. 물리적 안전성	O. 감사	O. 암호	O. 업데이트(1)	O. 업데이트(2)	O. 데이터 보호(1)	O. 데이터 보호(2)	O. 데이터 보호(3)	O. 설치	O. 정보 누출 대응	O. 불법 변경 감지	O. 인가된 고장 수리	O. 인증 및 식별	O. 잔여정보 제거	O. 권한	O. 환경적 스트레스	O. 초기화	O. 흐름 정보	O. 논리적 보호	O. 라이프 싸이클	O. Brute_Force
A.안전한 경로	X																											
A.TSF 데이터		X																										
A.물리적보안			X																									
A.신뢰된관리및사용				X																								
A.운영체제보강					X																							
A.키관리						X																						
A.불법수정차단									X																			
A.인증기관							X																					
P.감사									X																			
P.암호										X																		
P.가이드				X																								
P.업데이트											X																	
T.논리적인 공격														X					X	X								
T.권리_수정													X	X			X	X										
T.불법프로그램																X		X										
T.P고장			X																X					X				
T.자원공유충돌																			X									
T.P비의도적고장																							X	X				
T.잔여정보																					X							
T.정보누출																	X											
T.불법기기사용															X													
T.P교체			X					X																				
T.조작																								X	X			
T.권리남용													X									X						
T.암호공격																									X			X
T.리스트_수정													X	X				X		X								
T.시스템 오류	X											X											X	X				
T.데이터 공격										X			X															
T.정보유출(1)	X									X							X											
T.부인									X																			
T.정보유출(2)	X														X											X		
T.특권남용									X														X	X		X	X	X
T.감사정보파괴		X							X																			
T.TOE 오류	X								X															X				

4. 분 석

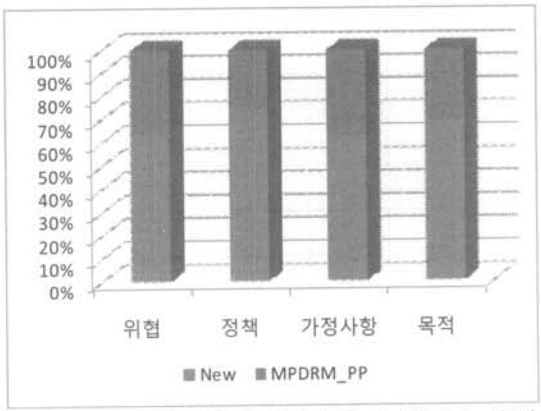
본 장에서는 3장에서 기술한 기존의 보호프로파일을 재사용하고, 새로 필요한 항목을 추가 생성하는 방법으로 IHD_PP를 개발함에 있어 그 효율성 및 활용성 측면을 분석한다. PP를 재사용하기에 앞서 기존 PP는 개발하고자 하는 PP와 비슷한 기능과 환경을 가지고 있어야 하며 그 다음에 기존 PP를 분석 및 참고하여 재사용함으로써 보안환경 및 보안목적을 도출하는데 그 시간과 비용 면에서 상대적인 효율성을 보인다.

(그림 11)은 IHD_PP 개발에 있어 기존 PP 활용 비율을 나타낸다. IHD_PP 개발에 앞서 개발 하고자 하는 PP와 유사한 성능을 가지고 있는 MPDRM_PP를 선정한다. 결과적으로 IHD_PP의 보안문제정의 및 보안목적을 도출하는데 IHD_PP 전체를 100%로 봤을 때 MPDRM_PP에서 33%를 추출하여 활용하였고 나머지 67%는 새로 추가하여 기술하였다. 이와 같은 결론은 PP를 개발하는데 67%의 노력이 필요하다는 것이 아니라 개발하고자 하는 PP와 비슷한 환경과 기능의 PP를 선택해서 선택한 PP의 분석을 통해 재사용할 수 있는 항목을 추출해 냄으로써 시간과 비용 측면에서 효율적으로 PP가 개발됨을 보여준다. (그림 12) 또한 각각의 보안문제정의와 보안목적의 활용 정도를 나타낸다.

그러나 재사용 할 PP 즉 기존 PP 선택 시 신중을 기해야 한다. 왜냐하면 한번 잘못 선택된 PP는 재사용 하기위한 분석 시간 및 비용에 비해 재사용 율이 떨어질 수 있기 때문에 다음 사항을 고려해서 PP를 선정해야 할 것이다. PP 선택 시 고려사항으로는 다음의 세 가지를 들 수 있다. 개발할 제품과의 보안 기능의 유사성은 있는가, 보안 환경은 비슷한가, 사용자 및 관리자를 비교해 공통사항이 충분히 존재하는가를 검토하고 유사성이 있을 때 그 효율성을 극대화 할 수 있다.



(그림 11) IHD_PP개발에 있어 MPDRM_PP의 재사용율(New: 새로 생성된 항목)



(그림 12) IHD_PP개발에 있어 각 항목 당 MPDRM_PP의 재사용율

5. 결 론

디지털 콘텐츠의 저작권을 보호하기 위한 기술로서 DRM 기술이 사용되고 있다. 이러한 DRM 기술은 근래에 들어 엔터테인먼트 콘텐츠의 디지털화가 급증하면서 DRM 사용이 일반화되었다. 하지만 콘텐츠 서비스 업체 간에 각기 다른 기술규격의 DRM 시스템 적용으로 DRM 호환성이 보장되지 못하고 있다. 이러한 문제를 해결하기 위해 다양한 기술이 개발되고 있다.

본 논문은 공통평가기준을 기반하여 상이한 DRM 시스템 연동기술의 보안성에 대한 보호프로파일(IHD_PP)을 개발했다. 또한 기존의 PP를 재사용하여 IHD_PP를 개발하는데 활용하였다. 개발하고자 하는 IHD_PP와 비슷한 환경의 기존 PP를 선택하고, 분석을 통해 재사용할 수 있는 항목을 추출해 IHD_PP에 적용함으로써 보안 문제정의와 보안목적을 도출하는데 시간 효율과 비용 측면에서의 효율적임을 보였다. 본 논문에서 개발한 IHD_PP 또한 타 PP 또는 보안목표명세서에서 재사용됨으로써 좋은 참고자료가 될 것으로 기대된다. 또한 콘텐츠 제공자 및 사용자 권한을 관리하는 관리자가 안전한 저작권을 유지할 수 있는 요구사항으로 활용할 수 있다.

참 고 문 헌

[1] International Standard ISO/IEC 15408, "Common Methodology for Information Technology Security Evaluation",Version 3.1, 2006.10.

[2] International Standard ISO/IEC 15408, "Common Criteria for Information Technology Security Envluation, Part1",Version 3.1, 2006.10.

[3] International Standard ISO/IEC 15408, "Common Criteria for Information Technology Security Envluation, Part2",Version 3.1, 2006.10.

[4] International Standard ISO/IEC 15408, "Common Criteria for Information Technology Security Envluation, Part3",Version 3.1, 2006.10.

[5] 정연정, 윤기송, 강호갑, "상이한 DRM간 연동을 통한 DRM 상호 호환성 지원 방안", 정보처리학회논문지, 제13-C권, 2006.4.

[6] Amer Bazerbachi Jaafari, "Mobile Phone Digital Rights Management Protection Profile", Polytechnic University,

2004.2.
[7] 국가정보원, "국가기관용 개방형 스마트카드 플랫폼 보호프로파일 v1.1", 2006. 5.17.
[8] Smart Card Security User Group, "Smart Card Security User Group Smart Card Protection Profile v3.0", 2001.9.9
[9] 국가보안기술연구소, "보호프로파일 보안요구사항 도출 방법에 관한 연구", 2006.10.
[10] S.R. Subramanya and Byung K. YI, "Digital rights management", Potentials, IEEE, 2006.3.
[11] Smart Card Security User Group, "Smart Card Security User Group Smart Card Protection Profile" version 3.0
[12] Karolina 또기두, "Mapping customer requirement to CC", Uppsalssa University, 2001.
[13] OMA, "Increasing revenue with secure mobile solutions", Sun Mircosystems, Inc, CoreMedia, 2003.
[14] Sonera MediaLap, "Mobile Digital Rights Management", Sonera MediaLab, 2003.
[15] F.Hartung, F.Ramme, "Digital rights management and watermarking of multimedia content for m-commerce applications", IEEE Communications Magazine, 2000.
[16] Jordan C. N. Chongy, Ren_e van Buurenz, Pieter H. Hartely, Geert Kleinhuisx, "Security Attributes Based Digital Rights Management", KPN Research, 2002.
[17] Apple Inc. "Common Criteria Certification:Apple's Ongoing Commitment to Security ", Whitepaper.
[18] Secure Digital Container, http://www.digicon.com
[19] Microsoft Windows Media Rights Manager, "http://www.microsoft.com/windows/windowsmedia/howto/articles/drmarchitecture.aspx"
[20] Advanced access content system, "http://www.aacsla.com/home".
[21] Open Mobile Alliance, "DRM Architecture Approved Version 2.0", 2006.
[22] PachyDRM, "http://www.pachydrm.com"
[23] R.H.Koenen, J.Lacy, M.Mackay, S.Mitchell, "The Long March to Interoperable Digital Rights Management", Proceedings of the IEEE, 92:883-897, 2004.

조 혜 숙

e-mail : hsjo@security.re.kr
2003년 한성대학교 멀티미디어정보처리과(학사)
2005년 성균관대학교 대학원 전자전기컴퓨터공학과(공학석사)
2006년~현 재 성균관대학교 대학원 전자전기컴퓨터공학과 박사과정
관심분야 : 정보보호, 보안성평가, 무선네트워크

이 광 우

e-mail : kwlee@security.re.kr
2005년 성균관대학교 정보통신공학부(학사)
2007년 성균관대학교 대학원 전자전기컴퓨터공학과(공학석사)
2007년~현 재 성균관대학교 전자전기컴퓨터공학과 박사과정
관심분야 : 암호이론, 정보보호, 네트워크 보안, 전자투표, 워터마킹

전 웅 렬

e-mail : wrjeon@security.re.kr
2006년 성균관대학교 정보통신공학부(학사)
2008년 성균관대학교 대학원 전자전기컴퓨터공학과(공학석사)
2008년~현 재 성균관대학교 전자전기컴퓨터공학과 박사과정
관심분야 : 보안성평가, 데이터베이스 보안

이 윤 호

e-mail : leeyh@security.re.kr
2003년 성균관대학교 정보통신공학부(석사)
2008년 성균관대학교 대학원 컴퓨터공학과(공학박사)
1993년 3월-2000년 4월 한국통신 연구개발본부 전임연구원
2000년 5월~2005년 1월 KBS인터넷(주) 기술지원팀장
2006년 6월~현 재 (주)애니온소프트 기술이사
관심분야 : 암호이론, 정보보호 응용, 전자투표, 워터마킹

김 승 주

e-mail : skim@security.re.kr
1994년~1999년 성균관대학교 정보공학과(학사, 석사, 박사)
1998년~2004년 한국정보보호진흥원(KISA) 팀장
2004년~현 재 성균관대학교 정보통신공학부 교수
2001년~현 재 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년~현 재 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년~현 재 교육인적자원부 유해정보차단 자문위원, 디지털콘텐츠유통협의체 보호기술워킹그룹 그룹장
2007년~현 재 대검찰청 디지털수사 자문위원, KISA VoIP 보안기술 자문위원, 기술보증기금 외부 자문위원, 전자정부서비스보안위원회 사이버침해사고대응 실무위원회 위원
관심분야 : 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET

원 동 호

e-mail : dhwon@security.re.kr

1976년~1988년 성균관대학교 전자공학과(학사, 석사, 박사)

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

2002년~현 재 대검찰청 컴퓨터범죄수사 자문위원, 감사원 IT 감사 자문위원

2007년~현 재 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, 정보통신대학원장

관심분야 : 암호이론, 정보이론, 정보보호