라이센스 기반 디지털 저작권 보호 시스템 설계 및 구현

정 연 정[†]·윤 기 송[††]·류 재 철[†††]

요 약

웹 기술의 발전에 따라 누구나 인터넷을 통하여 다양한 종류의 정보와 미디어를 액세스할 수 있게 되었으나 이러한 접근은 저작권과 소유권 침해를 유발할 수 있다. 콘텐츠가 다운로드된 이후에 콘텐츠를 보호할 수 있는 방안으로 콘텐츠에 대한 저작권을 보호하기 위해 DRM(Digital Rights Management) 기술이 연구되고 있는 상태이다. 본 논문에서는 인터넷 상에서 라이센스를 기반으로 하여 창조자, 배포자, 구매자 같은 유통단계의 각 참여자의 디지털 콘텐츠에 대한 저작권을 보호할 수 있는 시스템을 제안한다. 기존의 DRM 시스템이 배포자와 구매자사이의 유통을 지원하는 반면 본 시스템은 창조자에서 구매자로 이어지는 모든 유통 체인을 온라인으로 처리한다.

Design & Implementation of License-based Digital Rights Management System

Yeonjeong Jeong[†]·Kisong Yoon[††]·JaeCheol Ryu[†††]

ABSTRACT

The web-based technology allows anybody who has access to the Internet to get all kinds of information from the World Wide Web. It brings about issues regarding intellectual property and copyright threats. After content is downloaded, no further protection is provided on the content that has been accessed. DRM (Digital Right Management) technologies came out to ensure the protection of copyrighted content and information. In this paper, we propose architecture of license-based digital rights management system for protection of contents and principles' rights such as contents creators, providers, distributors, and uses in contents distribution value-chain over Internet. This system makes on-line processing of all value-chain from creator to purchaser possible, compared with existing DRM products only supporting only limited distribution between distributor and purchaser.

키워드 : 콘텐츠(Content), 저작권 보호(Digital Rights Management), DRM

1. 서 론

PC와 인터넷의 보급에 힘입어 기존에 아날로그 위주이던 콘텐츠는 디지털로 빠르게 전환되고 있다. 디지털 콘텐츠는 원본과 완벽히 동일한 품질의 복사본을 만드는 것이 가능하고, 빈번한 사용으로 인한 품질의 저하 현상이 발생하지 않기 때문에 새로 등장하는 콘텐츠는 물론, 기존의 아날로그 콘텐츠들도 디지털로 변환되고 있다[2, 5].

디지털 콘텐츠의 유통으로 고품질의 콘텐츠를 손쉽게 이용할 수 있게 되었지만, 콘텐츠 저작권자의 입장에서는 자신의 콘텐츠를 품질의 저하 없이 무단으로 복제하여 사용하는 사람이 생기기 때문에 저작권자로서의 권리가 침해당하는 결과를 낳기도 한다. 이러한 문제를 해결하기 위한 시도로서 암호화, 워터마킹, 식별자 시스템과 같은 여러 가지 방법의 저작권 보호 기술이 연구되고 있다[7, 8].

특히, 콘텐츠 암호화를 통하여 콘텐츠를 보호하려는 DRM 관련 기술은 현재 몇 가지 제품이 상용화 되어 서비스 되고 있는 상황이다[6, 9]. 하지만 현재의 기술은 최종 사용자로부터의 콘텐츠 보호에 중점을 두고 있어, 콘텐츠 제작자, 제공자, 분배자 등 콘텐츠 유통에 참여하는 주체들에게 호환성 문제, 저작권의 보호 및 관리 문제, 올바른 유통 체계 확립 문제 등을 효과적으로 해결할 수 있는 수단을 제공하지 못하고 있다. 콘텐츠의 전달 및 소비, 유통에 필요한 기술적 장치들이 마련되어야 하며 이러한 기술적 기반은 콘텐츠 제공자, 분배자, 사용자 등 모두에게 호환성 문제, 저작권의 보호 및 관리 문제, 올바른 유통 체계 확립 문제 등을 효과적으로 해결할 수 있는 수단을 제공해야 한다.

복잡하고 다양한 유통모델에서 DRM 시스템을 적용하기 위해서는 다양한 유통모델을 분석하고, 이를 뒷받침할 수 있도록 메타데이터, Secure Container, 라이센스 발급, DRM 클라이언트, 유통 서버 등을 설계하는 것이 필수적이다. 본

† 정 회 원 : 한국전자통신연구원 선임연구원
†† 정 회 원 : 한국전자통신연구원 책임연구원
††† 종신회원 : 충남대학교 정보통신공학부 교수
논문접수 : 2003년 10월 20일, 심사완료 : 2003년 12월 28일

논문에서는 라이센스 기반의 디지털 콘텐츠 저작권 보호를 위한 시스템을 설계하고 구현한다.

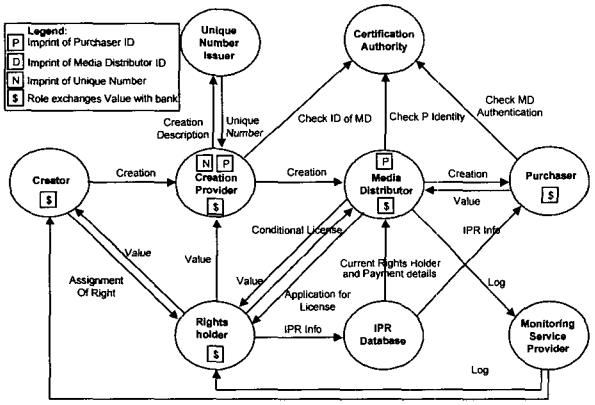
본 논문은 제2장에서 디지털 저작권 보호를 위한 관련 연구 현황에 대해서 알아보고, 제3장에서 디지털 저작권 보호 시스템을 살펴보고, 제4장에서 결론을 맺는다.

2. 관련 연구

2.1 IMPRIMATUR 비즈니스 모델

IMPRIMATUR 비즈니스 모델은 저작권 관리 시스템 프레임워크에 대한 개념을 제공한다. (그림 1)은 IMPRIMATUR 비즈니스 모델을 나타내며 이 모델은 유통주체가 콘텐츠를 획득할 수 있는 유통경로를 제공하고 저작물에 대한 정보나 창조자, 제작자, 배포자 등 유통 참여자에 관한 정보 제공을 표현한다.

IMPRIMATUR 비즈니스 모델에서는 각각의 역할(Role)별로 창조자, 제작자, 분배자, 저작권자, 사용자, 인증기관 등으로 구분하고 이들 간의 저작물의 상거래, 저작물의 저작권 보호, 저작물에 대한 접근제어, 저작물과 관련된 저작자의 권리를 영역, 매체, 기간에 대해 표현 등의 기능을 제공하는 것을 목표로 하고 있다[1].

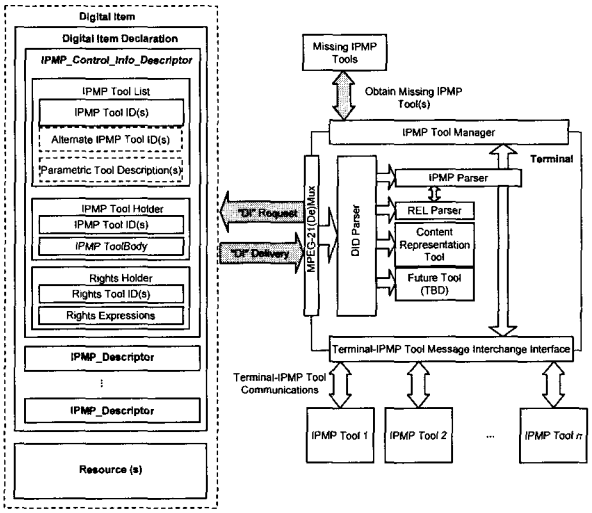


(그림 1) IMPRIMATUR 비즈니스 모델[1]

2.2 MPEG-21 IPMP

MPEG-21 IPMP의 목적은 모든 사용자가 디지털 아이템(Digital Item)에 대한 자신의 권리, 소유권, 계약을 표현할 수 있고 이러한 권리, 소유권이나 계약을 네트웍이나 디바이스 상에서 안전하게 관리하고 보호할 수 있는 프레임웍을 제공하는 것이다[4]. (그림 2)는 MPEG-21 IPMP 시스템 아키텍처를 나타낸다.

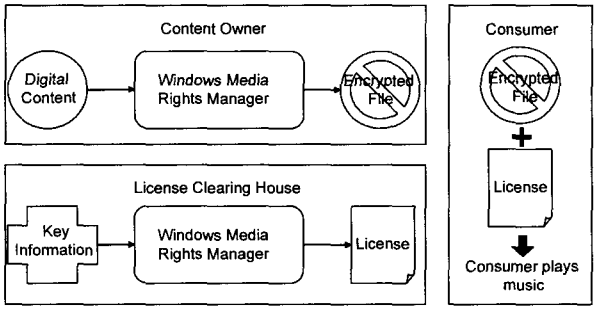
MPEG-21 IPMP 프레임웍은 RDD, REL과 IPMP 안전한 메시징 구조(IPMP Secure Messaging Architecture)를 구성요소로 포함한다[3]. 메시지 라우터(Message Interchange Interface)를 통해 IPMP 툴들간 또는 터미널과 IPMP 툴 사이의 메시지를 교환함으로써 호환성를 제공하려고 한다. 현재 RDD/REL로 표현된 IPMP 권리(Rights)를 보호하고 강제하도록 하기 위해 메시징 아키텍처를 개발 중이다.



(그림 2) MPEG-21 IPMP 시스템 구조 [4]

2.3 Microsoft DRM

Microsoft DRM 시스템은 아래 (그림 3)과 같이, 콘텐츠 소유주, License Clearing House, 소비자, 세 주체의 상호작용에 관여한다. Windows Media Rights Manager는 Microsoft DRM에서 가장 핵심적인 기능을 담당하는데, 기본적으로 패키징(Packaging), 유통, 라이센스 발급, 라이센스 획득, 콘텐츠 사용의 순서에 따라 프로세스가 진행된다[10, 11].



(그림 3) Microsoft DRM 개요[11]

Microsoft DRM에서는 라이센스와 미디어가 각각 분리되어 배포되며, 라이센스의 조건 변경이 쉽고, 대여 혹은 회원제 형태의 모델을 적용하거나, 프리뷰(Preview)의 제한, 투명한 라이센스 발급, 휴대용 SDMI 장치에 대한 전송 통제 등의 세부 기능이 있다.

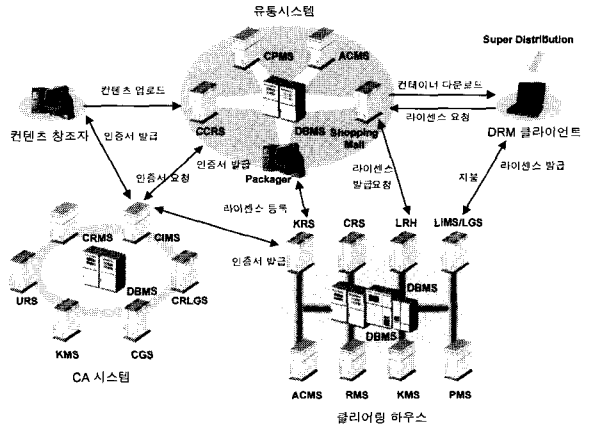
Microsoft DRM은 개별 프로그램이나 PC 혹은 단말기와 같은 장치위주로 구성되어 있고, DRM을 구성하는 여러 가지 프로세스 중에서 '패키징 - 라이센스 발급 사용'에 초점을 두고 있다. 하드웨어 ID를 이용한 유일한 DLL을 생성하여 사용자의 컴퓨터와 바인딩하는 개별화(Individualization)

이나, 운영체제, 사운드카드, 드라이버를 통해서 음악파일을 관리하는 SAP, 운영 체제의 커널 수준에서 작동하는 Protected Content Manager Exclusion 등의 요소는 Microsoft DRM 기술이 운영체제와 컴퓨터, 단말기 등의 장치 위주의 관리에 집중하고 있음을 보여준다. 한편, DRM을 실제 상황에 적용하기 위해서는 전역 식별자, 모니터링 및 추적, 계약, 그리고 IPR 데이터베이스 등의 요소가 함께 적용되어야 하는데, Microsoft DRM 기술에서는 이러한 요소가 나타나지 않고, 다만 콘텐츠 소유주가 패키징을 하여 유통시킨 후, 이에 대한 라이센스의 발급과 소비자의 사용에 대한 기술로만 구성되어 있다.

3. 시스템 개념 및 구조

현재 개발된 DRM 시스템들은 콘텐츠 유통업자와 구매자 사이의 단순한 유통 모델만 지원하도록 되어있어 콘텐츠의 유통에 관해서 누구나 쉽게 접근할 수 있는 환경이 제공되고 있지 않다. 본 논문은 창조자와 구매자 사이의 콘텐츠를 쉽고 안전하게 유통할 수 있도록 하며 콘텐츠 보호 및 유통을 온라인으로 처리하고 관리한다.

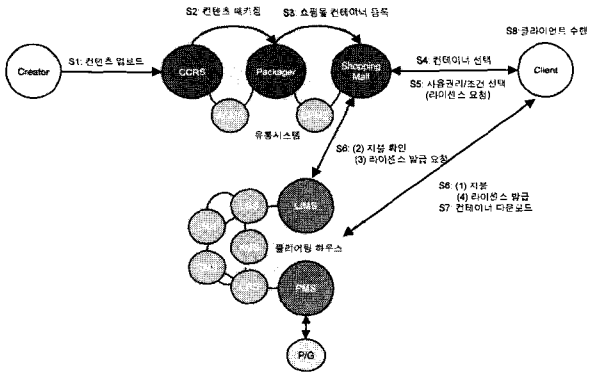
본 논문은 IMPRITUR 모델에서 역할(Role)별로 구분된 기능들을 (그림 4)와 같은 독립적인 모듈 단위로 구성하여 콘텐츠 유통 채널을 형성하고 콘텐츠 창조자에서부터, 유통업자, 구매자에 이르는 모든 콘텐츠 유통 채널에서 콘텐츠가 보호가 될 수 있도록 한다. 또한 각 모듈을 다시 세부 기능별로 컴포넌트화하여 지원 기능의 범위를 축소, 확대할 수 있도록 유연성(flexible)있는 구조를 가지는 라이센스 기반 디지털 저작권 보호 시스템을 제안한다. 제안된 시스템은 인터넷을 통하여 콘텐츠와 메타데이터, 창조자 정보 등을 입력 받아 이들 데이터를 암호화하고 패키징하여 안전하게 유통할 수 있는 콘텐츠로 만들고 라이센스 기반으로 유통될 수 있도록 하여 누구나 콘텐츠를 쉽게 유통할 수 있는 환경을 제공한다.



(그림 4) 라이센스 기반 디지털 저작권 보호 시스템 구성도

시스템의 구성은 콘텐츠를 암호화하여 보호할 수 있도록 패키징하여 콘텐츠(Secure Container)를 생성하는 패키저, 콘텐츠를 관리하고 유통 시키는 유통 서버, 라이센스 발급 및 과금 서비스, 리포팅 등을 담당하는 클리어링하우스, 컨테이너에 포함된 메타데이터를 해석하고 암호화된 콘텐츠의 복호화를 수행하며 사용자에게 발행된 라이센스를 관리하는 DRM 클라이언트로 구분된다. 본 논문에서 구현된 유통 서버와 클리어링 하우스는 Windows 2000 Server 및 리눅스 운영체제를 지원하며, 패키저와 DRM 클라이언트는 Windows 운영체제에서 작동한다.

본 시스템의 서비스 흐름을 (그림 5)에서 살펴보면 소비자는 콘텐츠 유통 시스템을 검색/조회하면서 자신이 원하는 콘텐츠를 선택하고 이에 대한 사용권한을 요청한다. 콘텐츠는 종류에 따라 다양한 사용규칙과 결제조건들이 제시되며, 소비자는 자신의 목적에 맞는 사용규칙과 결제조건을 선택한다. 소비자가 선택한 사용규칙과 결제조건에 따라 유통업체 시스템은 클리어링하우스로 결제 요청을 한다. 클리어링하우스는 결제 요청에 대한 처리를 수행하고 이에 대한 결과를 요청업체 시스템에게 전달한다. 결제처리가 정상적으로 완료된 건에 한하여 소비자에게 적절한 라이센스 발급이 될 수 있도록 유통업체 시스템은 클리어링하우스로 라이센스 발급요청을 한다. 라이센스 발급 시스템은 발급 요청된 라이센스를 요청된 사용규칙과 조건에 맞게끔 생성하여 소비자에게 전달한다. 소비자는 발급된 라이센스 범위 내에서 콘텐츠를 이용할 수 있게 된다.



(그림 5) 서비스 흐름도

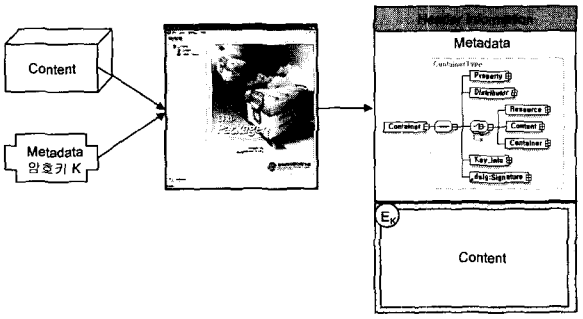
3.1 콘텐츠 패키저

콘텐츠 패키징은 Secure Container의 형식을 정의하고 그 형식에 따라 데이터를 채워 넣는 방법과 절차를 정의하는 것이다. 콘텐츠 패키징(Content Packaging)은 콘텐츠, 메타데이터, 비즈니스 룰 등 콘텐츠 보호와 유통에 관련되는 정보들로써 Secure Container를 구성하는 작업이며 콘텐츠 패키저(Content Packager)를 통하여 수행된다. (그림 6)에서 본 논문에서 제한하는 Secure Container의 구조를 볼 수 있

으며 (그림 7)에서 콘텐츠 패키저의 실행을 볼 수 있다.

Secure Container 설계시 고려해야 할 사항은 내부 데이터에 대한 계층적인 구조, 데이터 무결성, 암복호화 방법 정의, 내부데이터 인코딩/디코딩 방법 설계 등이 있으며 이러한 정보 구조체는 콘텐츠를 암호화할 뿐만 아니라, 콘텐츠 사용에 대한 비즈니스 모델 정보까지 포함하며 다음과 같은 특성을 갖는다[6].

- 기밀성(Confidentiality) : Secure Container에 포함된 정보에 대한 보안성 유지. 즉, 허락된 사용자에 대해서만 정보 접근을 허락하도록 함. 디지털 콘텐츠는 비즈니스 룰에서 정의한 조건에 따라 콘텐츠 사용이 허락됨. 대칭키 또는 비대칭키 암호화 기술 이용
- 무결성(Integrity) : Secure Container에 포함된 내용이 변경되지 않았음을 보장, 주로 해쉬(Hash) 함수를 이용한 암호화 기술 이용



(그림 6) 콘텐츠의 패키징 및 Secure Container 구조

콘텐츠 패키징의 결과로 생성되는 Secure Container는 다음과 같은 요소를 가진다.

- 대칭키로 암호화된 콘텐츠
- 메타데이터 및 비즈니스 룰
- 콘텐츠 암호화 키와 메타데이터의 해쉬값을 유통업체의 공개키로 암호화한 값
- Secure Container에 대한 전자서명

패키저 설계시 고려해야 할 사항은 패키저 실행 환경, 패키징을 지원하는 도구, 패키징의 결과물, 무결성 보장, 일괄처리 등이 있으며, 여기에서 무결성 보장은 메타데이터가 추가될 때 앞 유통주체의 권한을 어기지 않았는지, 그리고 클라이언트에서 메타데이터로써 권한을 확인할 때 콘텐츠에 대한 올바른 사용 권한을 가지고 있는지를 검사하는 것이다.

패키저를 구성하기 위한 내부 구성요소와 외부 구성요소는 다음과 같다.

① 메타데이터 작성기
사용자가 메타데이터를 입력하기 위한 도구이다. 필요에 따라 메타데이터의 일부분을 암호화하거나 전자서명을 추가 할 수 있다. 작성된 메타데이터는 일반적인 XML 문서이거나 인코딩된 문서이다.

② 메타데이터 템플릿 에디터
패키징하려는 콘텐츠의 종류에 따라 사용자는 메타데이터로부터 자신이 필요로 하는 요소들만을 선택할 수 있다. 메타데이터 템플릿 에디터는 이러한 작업을 위한 도구이다.

③ 사용자 인터페이스
메타데이터 입력을 위한 사용자 인터페이스이다. 메타데이터 템플릿에 따라 사용자가 입력해야 하는 요소들이 다르므로 사용자 인터페이스 또한 달라져야 한다. 따라서 메타데이터 템플릿의 내용에 맞는 사용자 인터페이스가 자동적으로 생성 가능해야 한다.

④ XML 생성기
사용자가 입력한 내용을 바탕으로 XML 형태의 메타데이터 문서를 생성한다.

⑤ 인코더/디코더
메타데이터 XML을 미리 정의된 규칙에 의하여 인코딩, 디코딩한다.

⑥ Secure Container 생성기
메타데이터와 콘텐츠를 하나의 Secure Container에 바인딩하는 도구이다. 콘텐츠는 필요에 따라 암호화될 수 있다.

⑦ Secure Container 템플릿 해석기
Secure Container 템플릿의 정보를 읽어 Secure Container 내부 데이터들을 구조화시킨다.

⑧ 룰(Rule) 생성기
메타데이터의 정보를 읽어 rule engine을 위한 규칙 집합을 생성해낸다.

⑨ 룰(Rule) 엔진
규칙 집합들을 입력으로 받아서 규칙들의 무결성을 검사한다.

⑩ 콘텐츠 암호화 모듈
대칭키를 사용하여 콘텐츠를 암호화한다. 콘텐츠를 여러개의 블록으로 나누고 각각 다른 키를 사용하여 암호화 가능하다.

⑪ 메타데이터 템플릿
사용자가 선택한 메타데이터 요소들에 대한 정보를 담고 있는 데이터이다.

⑫ Secure Container 템플릿
Secure Container의 내부 구조를 정의한 데이터이다.

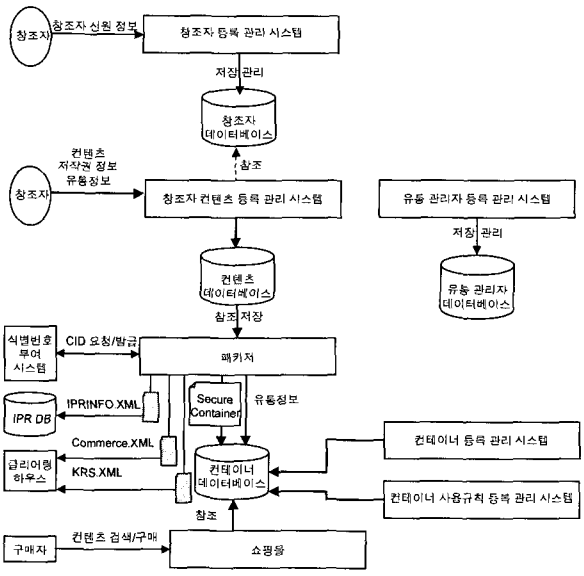
(그림 7) 콘텐츠 패키저 실행 화면

3.2 유통 서버

현재 개발된 DRM 시스템들은 콘텐츠 유통업자와 구매자 사이의 단순한 유통 모델만 지원하도록 되어있어 창조자와 유통업체 사이의 콘텐츠와 메타데이터 전달에 대해 고려하지 않았다. 콘텐츠의 제작은 제작 도구나 컴퓨팅 파워가 발전함에 따라 누구나 쉽게 제작할 수 있는 환경이 제공 되고 있지만, 제작된 콘텐츠의 유통에 관해서 누구나 쉽게 접근할 수 있는 환경이 제공되고 있지 않다.

본 유통 서버는 인터넷을 통하여 콘텐츠와 메타데이터, 창조자 정보 등을 입력 받아 누구나 콘텐츠를 쉽게 유통할 수 있는 환경을 제공 한다. 안전한 콘텐츠 유통을 위해 콘텐츠에 대한 보호는 기본적으로 제공되고 있으며, 콘텐츠를 쉽게 유통하기 위해 유통 서버에서 콘텐츠, 창조자와 콘텐츠에 관한 메타데이터, 창조자와 유통업자 사이의 유통정보 등의 콘텐츠 유통에 관한 데이터를 시스템적으로 처리하고 관리한다.

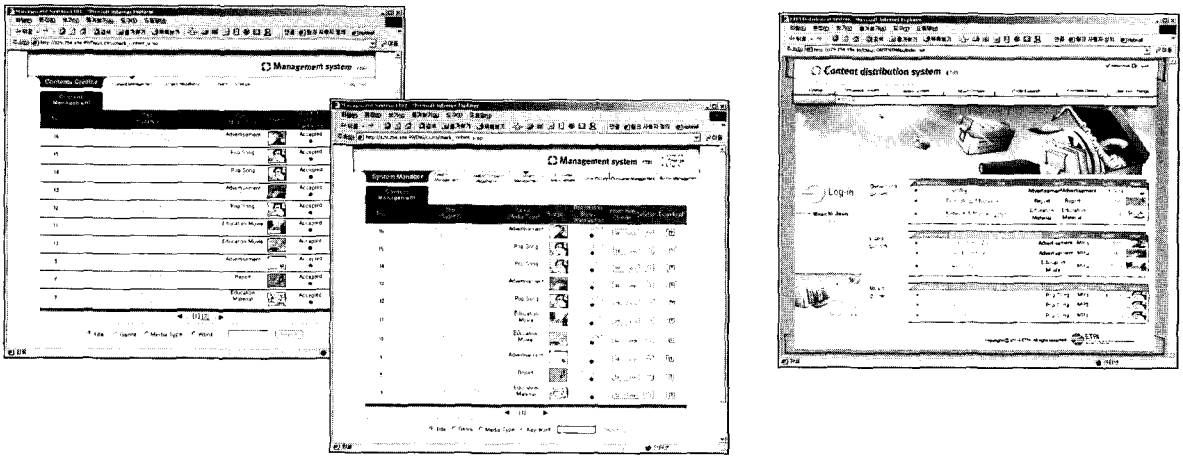
유통 서버는 창조자로부터 콘텐츠를 등록 받는 단계에서부터 이를 유통시키기 전까지의 유통 전처리 과정과 소비자로부터 콘텐츠 구매요청 및 라이센스 발급까지의 유통 본처리 과정, 그리고 라이센스 재발급등과 같은 유통 후처리 과정으로 나누어 처리한다. 아래 (그림 8)에서 유통 서버의 구성을 볼 수 있다. 유통 서버는 창조자 등록 관리, 창조자 컨텐츠 등록 관리, 유통 관리자 관리, Secure Container 등록 관리, Secure Container 사용규칙 등록 관리, 쇼핑몰로 구성된다.



(그림 8) 유통 시스템 구성도

3.3 클리어링 하우스

라이센스 기반 디지털 저작권 보호 시스템은 라이센스를 기반으로 하여 콘텐츠에 대한 사용권리를 제어하고 나아가 콘텐츠를 보호한다. 유통 서버는 구매자로부터 콘텐츠에 대

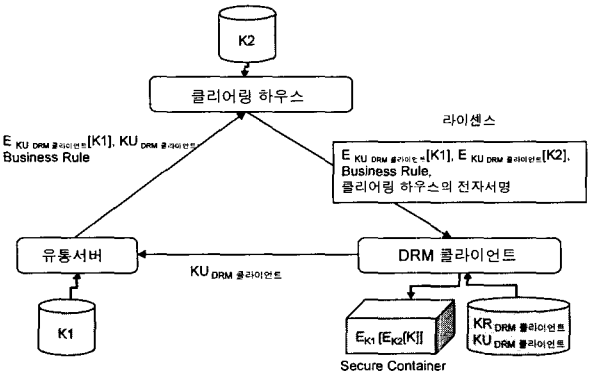


(그림 9) 유통 시스템 실행 화면

한 사용권한을 요구 받고 그 권한에 대한 라이센스 발행을 클리어링 하우스에 요청한다. 유통 서버는 콘텐츠 패키징시 발생하는 암호화키를 DRM 클라이언트의 공개키로 암호화하고 라이센스에 포함될 권한 정보를 클리어링하우스에 보내어 라이센스가 클리어링하우스로부터 DRM 클라이언트에 발행되도록 한다.

클리어링 하우스는 패키저로부터 콘텐츠를 암호화하는데 사용한 암호키와 암호정보를 등록받는 키 등록 서버, 키 등록 서버에 등록된 암호키와 암호화 정보를 안전하게 저장 관리하는 키 관리 서버, 라이센스 발급을 요청 받아 라이센스를 생성하여 DRM 클라이언트에 라이센스를 발급하는 라이센스 발급 서버로 구성된다.

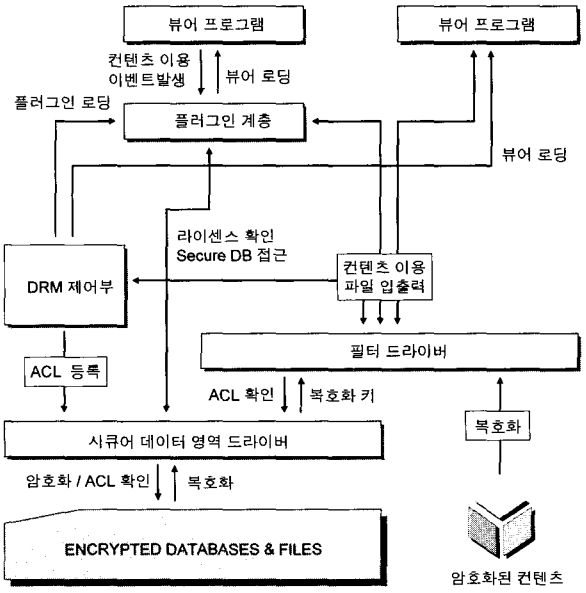
라이센스 발급 과정은 아래 (그림 10)과 같으며 안전한 데이터 전달을 위해 DRM 클라이언트의 공개키로 데이터와 콘텐츠 암호에 사용된 대칭키를 암호화하여 전달한다.



(그림 10) 라이센스 기반 암호화 키 전달 흐름

3.4 DRM 클라이언트

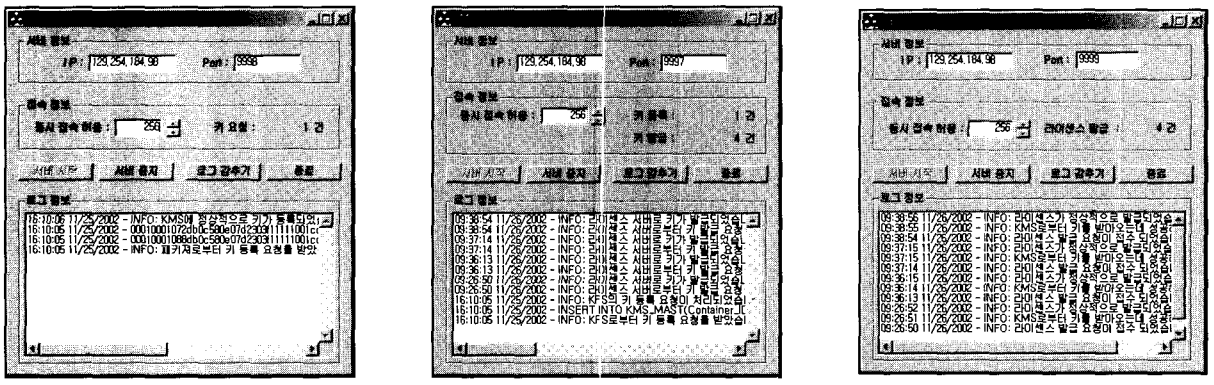
DRM 클라이언트의 설계에 있어서 기존의 뷰어 프로그램 지원, 새로운 콘텐츠 타입과 뷰어를 지원 용이, 모듈간의 투명한 상호 연동, 모듈간의 상호 인증과 권한 설정을 통해 악의적 공격에 대한 기본적인 대응을 할 수 있도록 한다. 아래 (그림 12)과 (그림 13)은 본 논문에서 제안하는 DRM 클라이언트의 구성과 실행 화면을 나타낸다



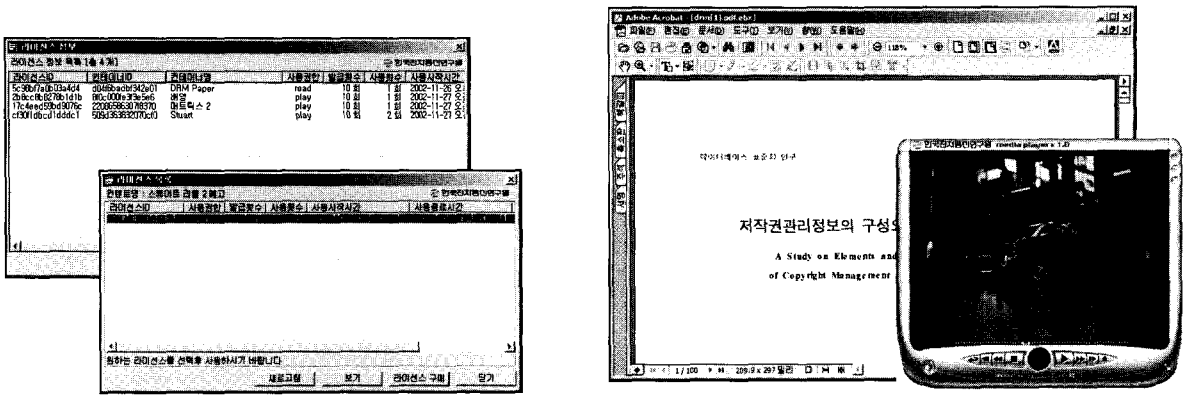
(그림 12) DRM 클라이언트 구성도

DRM 클라이언트는 일반 사용자뿐만 아니라 악의적인 사용자에게도 노출된 환경에서 동작하기 때문에 다양한 공격에 대한 강인성과 함께 사용자의 편의성을 고려한 유연한 구조도 가져야 한다. PDF, 워드, 엑셀 파일과 같이 널리 이용되나 특정 업체의 소프트웨어에 종속된 콘텐츠를 지원하는 경우, 사용자의 편의성을 위해서는 해당 업체의 전용 소프트웨어를 이용할 수 있게 해야 한다. 하지만 포맷이 공개되지 않은 파일의 경우 타 업체에서 이를 지원하기가 쉽지 않다는 문제가 있다. 이를 위해 클라이언트 환경에서 DRM 정책을 결정하는 제어부와 뷰어 프로그램을 분리하고, 그 사이에 플러그인 계층을 두어 DRM 제어부의 결정에 따라 뷰어 프로그램을 제어하도록 한다. DRM을 염두에 두지 않고 만들어진 뷰어 프로그램을 DRM 제어부의 정책에 따라 제어하기 위해서는 몇 가지 구현 기술이 필요하다.

먼저, Acrobat Reader와 같이 플러그인을 허용하는 소프



(그림 11) 클리어링 하우스 실행 화면



(그림 13) DRM 클라이언트 실행 화면

트웨어의 경우는 이를 통해 DRM 정책을 적용시킬 수 있으며, 두 번째로 소프트웨어가 Active X 컨트롤로 제공되는 경우에는 OLE 컨테이너의 형태로 플러그인 계층을 구성하여 제어할 수 있다. 세 번째로 외부에서 개입될 여지를 남기지 않고 완전히 독립적으로 동작하는 소프트웨어의 경우는 운영체제와 소프트웨어 사이에 오고 가는 메시지를 가로채어 DRM 정책을 적용시킬 수 있다.

암호화 기술은 최종 사용자 환경에서 모든 복호화 키가 존재해야만 하기 때문에 라이센스의 형태로 발급받은 복호화 키는 사용자의 PC에 안전하게 보관되어야 한다. 실제로 이를 가장 안전하게 구현하기 위해서는 스마트카드와 같은 안전한 물리적인 저장 장치를 사용해야 하나, 현실적인 어려움으로 인해 하드디스크 내에 저장을 하되 악의적인 사용자의 공격으로부터 복호화 키를 보호할 수 있는 장치를 마련해야 한다.

본 논문에서는 커널 레벨의 드라이버를 이용해 가상 드라이브와 같은 데이터 영역을 만들고, 이 안에 복호화 키를 비롯한 중요 정보들을 암호화 하여 저장하는 방법을 이용하였다. 암호화는 사용자 PC에 종속된 하드웨어 정보와 DRM 클라이언트의 설치시에 생성된 난수를 조합하여 이용한다. 저장영역 내에는 이 공간에 접근이 허용된 프로세스의 목록이 포함되어 있다. 이 목록에는 기본적으로 DRM 제어부와 필터 드라이버만이 포함되어 있으며, 유효한 라이센스를 가진 프로세스가 콘텐츠를 이용하기 위해 로딩될 때 DRM 제어부는 이 프로세스를 접근 허용 목록에 추가하고, 프로세스가 종료하거나 라이센스가 만료되면 목록에서 삭제한다.

필터 드라이버는 커널 레벨의 드라이버로, 어떤 프로세스가 암호화된 콘텐츠에 접근할 경우에 해당 프로세스가 콘텐츠에 접근할 수 있는 권한이 있는지의 여부를 확인한 후 복호화하여 넘겨주는 역할을 한다. 접근하는 프로세스는 콘텐츠가 암호화 되어 있는지의 여부를 알지 못하고 일반적인 파일 입출력 함수를 이용하며, 필터 드라이버는 이를 가로채어 동작한다. 필터 드라이버가 복호화를 수행할 때 필요한 키는 시큐어 데이터 영역에 저장되어 있고, 매번 입출력이 발생할 때마다 해당 프로세스의 접근 허용 여부를 시큐어 데이터 영역의 접근 허용 목록에서 확인한 후에 복호화를 수행한다.

DRM 제어부는 클라이언트 프로그램의 가장 중심이 되는 모듈로 라이센스 서버와 통신하여 라이센스를 전송받고, 이를 시큐어 데이터 영역에 저장하며, 콘텐츠에 대한 이용 요청이 발생했을 경우 라이센스를 확인하여 플러그인을 통해 뷰어를 실행해 준다. 유효한 라이센스를 가진 프로세스가 실행될 때 이를 접근 허용 목록에 추가해주며, 프로세스의 종료나 라이센스의 만료시에 이를 다시 삭제해주는 역할도 한다.

새로운 콘텐츠 타입을 지원하기 위해서는 적절한 뷰어 프로그램이 있어야 하고, DRM 정책을 기반으로 뷰어를 제어하기 위한 플러그인이 있어야 한다. DRM 업체마다 DRM 정책의 기술방법이 다르고, 뷰어 프로그램마다 동작 방식이 서로 다르기 때문에 현재는 DRM 업체에서 새로운 콘텐츠 타입의 추가시마다 직접 뷰어나 플러그인을 개발하고 있다. 또한, 클라이언트-플러그인-뷰어의 명확한 계층구조를 가지지 않고, 뷰어에 클라이언트의 기능이 통합되어 있기도 하며 플러그인 계층 없이 클라이언트에서 바로 제어하기도 하므로 표준화가 쉽지 않다. 본 연구에서는 클라이언트와 뷰어를 완전히 분리하고, 그 사이에서 DRM 정책에 따라 뷰어를 제어하는 역할로 플러그인을 이용하기 때문에 클라이언트와 플러그인이 통신하기 위한 표준 API 집합을 개발하였다. 이를 이용하면 서드파티 업체가 특정 콘텐츠 타입과 뷰어 프로그램을 지원하는 플러그인을 제작하여 클라이언트와 연동시킬 수 있다.

4. 결 론

현재 콘텐츠에 대한 보호 및 유통은 최종 구매자로부터의 콘텐츠 보호에 중점을 두고 있어, 콘텐츠 제작자, 제공자, 분배자 등 콘텐츠 유통에 참여하는 주체들에게 저작권의 보호 및 관리를 효과적으로 해결할 수 있는 수단을 제

공하지 못하고 있다.

본 논문에서는 창조자, 유통업자, 구매자, 클리어링 하우스가 참여하는 유통모델에서 디지털 콘텐츠의 안전한 유통을 위한 콘텐츠와 메타데이터에 대한 보호 방법과 유통 방법을 연구하고 이를 위한 라이센스 기반 디지털 저작권 보호 시스템을 제안한다. 본 논문에서는 콘텐츠의 전달 및 소비되는 유통 환경을 분석하여 복잡하고 다양한 유통모델에서 DRM 시스템을 적용하기 위한 메타데이터, Secure Container, 라이센스, DRM 클라이언트, 유통 서버, 클리어링 하우스 등을 설계한다.

본 논문에서 제안하는 시스템은 콘텐츠 유통에 참여하는 유통주체의 저작권을 보호하고 소유권 침해 방지를 위해 콘텐츠에 대한 암호화를 수행하고, 암호화시에 발생하는 키를 관리하며 이 키를 이용하여 라이센스가 발행될 수 있도록 한다. 또한 창조자와 유통업체 사이의 콘텐츠와 메타데이터 전달과 콘텐츠에 대한 사용권한을 생성 및 관리하며 콘텐츠 유통이 쉽게 발생하고 구매자가 편리하게 콘텐츠를 구매할 수 있는 환경을 제공한다.

현재 콘텐츠에 대한 저작권 보호는 유통업자와 구매자 사이를 중심으로 연구되고 있다. 콘텐츠 유통의 활성화와 콘텐츠 보호 영역을 넓히기 위해 B2B 영역에서의 콘텐츠 보호와 P2P 환경에서의 콘텐츠 보호 방안에 대한 연구가 필요하다.

참 고 문 헌

[1] IMPRIMATUR 비즈니스 Model, Version2.1, Available at http://www.imprimatur.net, June, 1999.

[2] Seongoun Hwang, Kisong Yoon, Changsoon Park, "Design and Implementation of a Licensing Architecture for Distribution of Copyright-Protected Digital Contents," Telecommunications Review, Vol.12, No.5, October, 2002.

[3] ISO/IEC JTC 1/SC 29/WG 11 MPEG/ N3939 Information technology- Multimedia framework(MPEG-21)- Part 1 : Vision, Technologies and Strategy, Jan., 2001.

[4] ISO/IEC JTC1 SC29/WG11 MPEG, MPEG-21 Requirements v 1.0, N4681, March, 2002.

[5] Frank Hartung, Friedhelm Ramme, "Digital Rights Management and Watermarking of Multimedia Content for M-Commerce Applications," IEEE Communications Magazine, pp.78-84, November, 2000.

[6] 강호갑, "DRM 기술동향", 계간저작권, 2001.

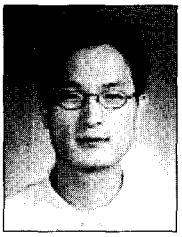
[7] Marc. A. Kaplan, "IBM Cryptolopes, SuperDistribution and Digital Rights Management," http://www.research. ibm.com/people/k/kaplan/cryptolope-docs.crypap.html.

[8] Olin Sibert, "DigiBox : A Self-Protecting Container for Information Commerce," 1st USENIX Workshop on Electronic Commerce, 1995.

[9] http://www.intertrust.com.

[10] http://www.microsoft.com/windows/windowsmedia/drm.asp.

[11] http://www.microsoft.com/windows/windowsmedia/wm7/drm/architecture.aspx.



정 연 정

e-mail : yjjeong@etri.re.kr

1994년 부산대학교 전자계산학과(학사)

1996년 부산대학교 대학원 전자계산학과 (석사)

1996년~현재 한국전자통신연구원 선임연구원

관심분야 : 정보 보호, 저작권 보호

윤 기 송

e-mail : ksyoon@etri.re.kr

1984년 부산대학교 조선공학과(학사)

1988년 City University of New York 전산학(석사)

1993년 City University of New York 전산학(박사)

1993년~현재 한국전자통신연구원 책임연구원

관심분야 : 정보 보호, 저작권 보호, 분산 처리

류 재 철

e-mail : jcryou@home.cnu.ac.kr

1985년 한양대학교 산업공학과(학사)

1988년 Iowa State University 전산학과 (석사)

1990년 Northwestern University 전산학과 (박사)

1991년~현재 충남대학교 정보통신공학부 교수

관심분야 : 정보 보호, 인터넷 보안