情報保護學會論文誌
第16卷 第3號, 2006. 6

네트워크 상에서 디지털 콘텐츠 보호를 위한 DRM 프레임 설계*

김 종 우†, 양 원 일‡, 한 승 조
조선대학교

Design of DRM Frame for Digital Contents Protection in Network*

Jong-woo Kim†, Won-il Yang‡, Seung-jo Han
Chosun University

요 약

현재 무료로 이용하던 많은 디지털 콘텐츠들이 유료화되고 있으며, 저작권 보호를 위해 DRM등과 같은 불법사용방지기술이 이용되고 있다. 그러나 이러한 소프트웨어 저작권 보호 장치들을 무력화하려는 움직임은 소프트웨어 산업의 급성장과 비례해서 발전하고 있다. 본 논문에서는 DRM 시스템에 공개키 알고리즘과 하드웨어 바인딩을 적용하여 보다 안전하고, 콘텐츠 인증과 사용자 인증을 제공할 수 있는 방안을 연구하였다. 제안된 시스템은 콘텐츠 분배나 지적재산권을 보호하고, 투명하고 안전한 콘텐츠 분배에 관여하는 유통 당사자들 간의 상호운용에 관한 문제를 해결 수 있다. 또한 제안된 알고리즘은 DRM 유통 시스템의 투명성을 보장함과 동시에, 무단 배포를 방지할 수 있다.

ABSTRACT

This study is intended to provide more secure contents authentication and user authentication by applying public key algorithm and hardware binding to the DRM system. The proposed system is capable of protecting distributed contents and copyrights as well as resolving any interoperability issues among those involved in transparent and secure contents distribution. The proposed algorithm also affords transparency in the DRM distribution system and protection from unauthorized distribution.

Keywords : *DRM, Contents Protection*

Ⅰ. 서 론

20세기에 정보화를 위한 컴퓨터와 정보통신을 이용한 인프라가 구축되었으며, 21세기에는 구축된 인프라에 어플리케이션을 추가하는 단계로서 그 어플리케이션에 따라 수많은 분야가 빠르게 발생하고 있다.

90년대 말, 인터넷을 통한 디지털 콘텐츠 유통 산업이 새로운 모델로 부각됨에 따라 불법복제로 인한 저작권 침해를 방지하기 위해 InterTrust, ContentGuard, Reciprocal, LiquidAudio 등 많은 DRM 기술들이 발표되었다. 그러나, 초기 시장을 형성하던 디지털 음악 및 e-Book 시장의 침체와 저작권자 위주의 DRM 기술에 대한 사용자의 불만 증대, 그리고 상이한 DRM 기술들간의 상호호환성 결여 등의 이유로 매우 제한된 범위에서만 사용

접수일: 2006년 2월 16일; 채택일: 2006년 6월 8일
* 이 논문은 2006년도 조선대학교 학술연구비의 지원을 받아 연구되었음.
† 주저자, mmm@7.co.kr
‡ 교신저자, wiyang@chosun.ac.kr

되어 왔다.

그러나 2000년 이후, 전자상거래와 함께 인터넷 비즈니스의 양대 영역을 차지하게 될 디지털 콘텐츠가 급속히 활성화되고 있어, 이 같은 시장 수용에 대응할 통합적인 디지털 저작권보호 (DRM: digital right management) 솔루션 등의 저작권 보호 기술들이 개발되어야 한다. DRM은 암호화 기술과 권한제어 기능을 이용하여, 디지털문서를 권한 부여자만이 볼 수 있도록 하는 기술로서, 정보유출 및 저작권보호에 반드시 필요한 기술이다[1-3].

본 논문에서는 공개키 알고리즘을 이용한 콘텐츠 비밀키를 분배함으로써 보다 안전한 키분배가 가능하다. 또한 제안된 알고리즘은 콘텐츠 비밀키 노출을 통한 콘텐츠의 불법 복제를 방지할 수 있다.

본 논문에서는 DRM 유통 프레임워크를 설계하고, 이를 위한 인증 프로토콜 설계 후, 라이선스 및 암호화 메커니즘 설계, 그리고 패키징 메커니즘을 설계한다. 이러한 DRM 시스템을 Visual C++, Visual Basic, ASP, XML, ADSI 등을 이용하여 설계하고, DB 구축을 위하여 MS-SQL 2000을 이용한다.

Ⅱ. DRM 관련 기술

2.1 DRM의 정의

DRM(Digital Rights Management)은 디지털콘텐츠의 보호를 위한 암호화 및 사용자 인증키 관리, 디지털콘텐츠 유통 환경을 구성하는 주체들 간의 지적재산권 및 거래 규칙, 과금, 이용규칙에 대한 표현, 디지털콘텐츠의 이용 및 분배, 사용 및 접근 제어, 권한제어, 워터마킹, 불법복제 추적기술, 투명한 전자상거래를 위한 거래 내역의 관리 및 보고, 과금처리 등을 가능하도록 하는 디지털 저작권 관리에 대한 전반적인 기술이다. 즉, 콘텐츠의 암호화와 권한제어를 통해 콘텐츠에 권한을 가지고 있는 사용자들만이 그 권한에 따라 콘텐츠를 열어 볼 수 있도록 함으로서 콘텐츠의 불법사용 방지, 자동과금, 결재대행, 부가서비스 등 디지털 콘텐츠의 생성, 유통, 사용에 관련된 전 분야의 서비스를 제공하는 것이다[1-6].

DRM은 콘텐츠를 메타데이터와 함께 배포 가능한 단위(Secure Container)로 패키징하는 패키저(Packager)와 이렇게 배포된 콘텐츠를 사용하고자 하는 사용자의 플랫폼에서 콘텐츠의 이용권한을 통제하는 DRM Controller, 그리고 콘텐츠에 대한 배포 정책 및 라이선스를 발급 관리하는 Clearinghouse (DRM Server)로 크게 구분할 수 있다.

2.2 암호 보안 기술

90년대 중반부터 인터넷을 기반으로 한 전자상거래가 활발하게 진행됨에 따라 보안이 중요한 이슈로 떠오르게 되었다. 이러한 이유로 이전에는 국방 및 금융 분야에서 제한적으로 사용되던 암호화 관련 기술이 인터넷을 기반으로 하는 각종 전자상거래 시스템의 보안을 위하여 실용화되기 시작하였다. 암호 기술은 또한 디지털 콘텐츠의 불법복제 문제점을 해결하기 위한 수단으로 적용되기 시작 하였다.

DRM 시스템에서 전송될 콘텐츠는 암호 기술을 이용하여 암호화되며, 수신자는 암호화된 콘텐츠를 복호화하여 콘텐츠를 이용하게 된다[7]. 콘텐츠의 암호화는 수신자의 고유정보(예 : Public key 또는 Secret Token 등)을 이용하여 암호화되기 때문에 지정된 수신자 이외의 사람들은 비록 암호화된 콘텐츠를 입수하더라도 암호를 해독할 수 없게 된다. 이러한 방식은 'Secure Distribution(또는 Copy Protection)' 방식이라고 불리며, 콘텐츠의 전송 중 해킹 위협으로부터의 보호 및 허가되지 않은 사용자로부터의 접근 방지를 가능케 한다. 이 방식은 다음과 같은 기능을 제공한다.

- 콘텐츠의 비밀성 보장 :
  암호화(Encryption/Decryption)
- 콘텐츠의 위/변조 방지 :
  전자서명(Digital Signature)
- 허가되지 않은 사용자의 콘텐츠 이용 차단 :
  키관리(Key Management)

본 논문에서 제안된 인증 프로토콜에 사용되는 암호 알고리즘은 기존 시스템과의 호환성을 높이기 위하여 표준화되어 있고 범용으로 쓰이는 AES, SEED, RSA, SHA 등의 알고리즘을 이용하였다.

Ⅲ. 제안된 DRM 시스템 설계

본 논문에서는 인터넷 환경에서의 DRM 유통 프레임워크를 그림 1과 같이 설계한다.

본 논문에서는 인터넷 환경에서 콘텐츠의 창조자,

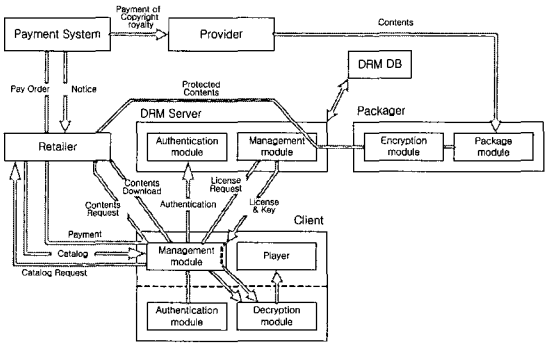

그림 1. DRM 유통 프레임워크

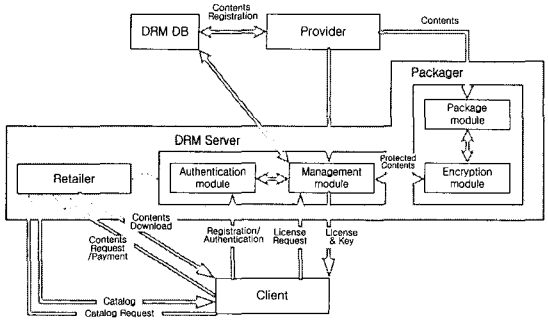

그림 2. DRM Clearinghouse 구조

저작권자, 제작자, 배포자, 사용자 등 유통 주체의 권리를 보호하고, 안전하고 투명한 콘텐츠 유통을 지원하는 유통 프레임워크를 설계하고자 한다.

유통 프레임 워크 설계 구현시 고려사항은 다음과 같다.

- 각 유통주체가 독립적으로 운영될 수 있는 형태
- 유통주체가 필요에 따라 결합 또는 분리될 수 있는 형태
- 각 유통 주체간 신뢰성 보장
- 라이선스 서버로부터 콘텐츠 보호
- 콘텐츠 종류, 메타데이터 및 시스템 확장 가능한 형태

3.1 DRM Clearinghouse 설계

DRM Clearinghouse는 콘텐츠의 안전한 유통을 위해 콘텐츠를 암호 알고리즘으로 패키징하는 패키저와 온라인 상의 각 사용자를 인증하는 인증 모듈, 콘텐츠 및 암호와 관련된 정보들을 관리하는 관리 모듈로 구성되어 있다. 각 모듈은 독립적이며 상호 연동되어 동작된다.

본 논문에서 제안한 DRM 시스템은 그림 2와 같이 하나의 서버에서 콘텐츠 생성 관리, 일괄 처리를 할 수 있도록 Packager와 Retailer의 기능을 DRM Clearinghouse에 포함을 시킨다. 그러나 Packager와 Retailer는 각 독립인 시스템으로 동작된다.

인증 모듈에서는 콘텐츠의 불법 사용을 방지하기 위하여 사용자의 인증 정보와 하드웨어 바인딩 기법으로 사용자의 하드웨어 정보를 이용하여 인증을 받는다. 본 논문에서는 사용자 단말기 네트워크 카드의 MAC Address를 해쉬 함수에 적용한 값을 이용하여 사용 가능한 단말기를 제한한다. 그리고 콘텐츠의 암호화와 패키징을 위하여 본 논문에서는 128 비트의 SEED 암호 알고리즘과 128 비트의 AES 암호 알고리즘을 사용할 수 있도록 설계한다.

3.1.1 DRM 서버 설계

DRM 서버는 콘텐츠 사용자가 해당 콘텐츠를 이용할 수 있는 라이선스를 내려주며, 이에 대한 라이선스 발급 내역 및 판매내역을 정산하는 기능을 한다. DRM 서버는 실제 라이선스를 발급해주는 LGS (License Generation Server)와 라이선스 발급에 필요한 키를 보관하고 있는 KMS(Key Management Server), 콘텐츠 패키징시 사용된 키를 저장해 줄 수 있는 KRS(Key Registration Server)로 구성된다[8].

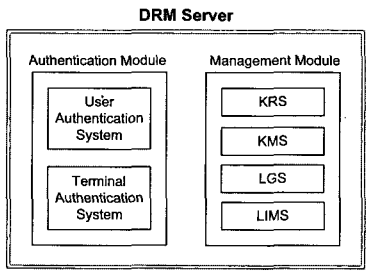

그림 3. DRM 서버 구성도

3.1.2 패키징 메커니즘

가. 시큐어 컨테이너

시큐어 컨테이너는 디지털 콘텐츠를 외부의 불법

침해로부터 방지할 뿐만 아니라 인터넷을 통해 손쉽게 이동할 수 있는 기술적 정보 구조체를 말한다. 이는 기존의 정보보호가 네트워크 전송 채널에서의 보호를 목적으로 한데 반해, 정보의 실사용자까지도 방어의 대상으로 하여 정보보호가 가능하도록 하는 개념이다. 본 논문에서는 시큐어 컨테이너를 클라이언트에 분배시 하드웨어 바인딩 정보를 이용하여 시큐어 콘텐츠를 이중 암호화함으로써 특정 단말기 인증 기능을 강화한다. 또한 클라이언트에서 콘텐츠 실행시 자동으로 실행이 되로록 EXE 파일로 리패키징을 하도록 설계한다.

나. 시큐어 컨테이너 설계

1) 파일 전체 구조

시큐어 컨테이너는 다음 그림 4, 5와 같은 구조를 가진다.

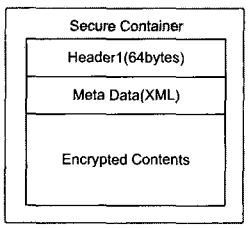

그림 4. 시큐어 컨테이너 구조

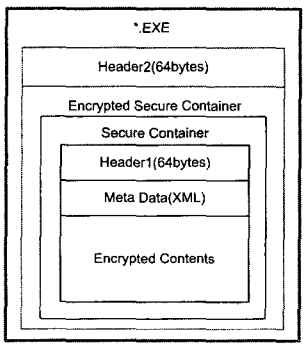

그림 5. 클라이언트 분배시 리패키징된 시큐어 컨테이너 구조

2) 세부 구조 설명

가) Header

Header1은 표 1과 같고, 시큐어 컨테이너 파일을 식별하기 위한 정보와 XML 부분의 길이 정보를 알려준다. Header2는 표 2와 같고, 사용자가 콘텐츠를 실행시 시큐어 컨테이너 복호화에 필요한 최소 정보를 담고 있다.

나) XML

시큐어 컨테이너 스키마(schema)에 의한 XML 문서이다.

다) 암호화된 콘텐츠

암호화된 콘텐츠를 파일의 끝부분에 붙인다. 콘텐츠의 마스터키를 이용하여 암호화되어 있다.

표 1. Header1의 구조

Identifier ISLAB Package	Container Format Version 1.0	XML 문서의 Size(Integer)	Reserved
16bytes	8bytes	4bytes	36bytes

필드명	설 명
Identifier ISLAB Package	클라이언트에서 파일을 읽을 때 이 값을 검사하여 컨테이너 파일이 맞는지 확인한다. default 값은 "ISLAB PACKAGE"이다.
Container Format Version	파일포맷의 버전을 나타낸다. 이 값에 따라 파일 전체 구조와 적용되는 XML 스키마가 달라질 수 있다.
XML 문서의 Size	파일내의 XML 부분의 길이를 나타낸다. 시큐어 컨테이너 파일의 65바이트부터 이 값만큼이 데이터가 XML이다.
Reserved	현재 버전에서 사용하지 않고 나중을 위해 예약된 공간이다.

표 2. Header2의 구조

Identifier ISLAB Repackage	Content_ID	User _ID	Encry -ption Algori-thm	Content Type	Rese-rved
8bytes	8bytes	8 bytes	4bytes	8bytes	28 bytes

필드명	설 명
Identifier ICLAB Repackage	클라이언트에서 파일을 읽을 때 이 값을 검사하여 컨테이너 파일이 맞는지 확인한다. default 값은 "ISLAB REPACKAGE"이다.
Content_ID	콘텐츠의 식별자 값이다. 콘텐츠의 고유 번호이다.
User_ID	사용자의 식별자로 본인에게 허락된 콘텐츠를 확인하기위한 값이다.
Encryption Algorithm	리패키징을 위하여 사용된 암호화 알고리즘 정보이다.
Content Type	이 정보를 이용하여 콘텐츠의 종류를 구분하여 응용프로그램에 연결한다.
Reserved	현재 버전에서 사용하지 않고 나중을 위해 예약된 공간이다.

3.2 클라이언트 설계

클라이언트는 다운로드 받은 콘텐츠의 실행을 위하여 어플리케이션 영역에서 복호화하고, 프레이어로 실행하는 기능을 가지고 있다. 클라이언트 장치는 컴퓨터, 셋탑 박스(set-top box), 게임 콘솔, PDA, 모바일 폰 등과 같이 다양한 장치가 있다.

DRM 시스템에서 클라이언트는 사용자 단말기에서 동작되므로 DRM 시스템에 손상을 가할 수 있다. 따라서 적절한 보안 레벨을 제공해서 클라이언트 환경을 안전하게 하고, 시스템을 손상시키려는 의도를 어렵게 해야 한다.

제안 DRM 시스템의 클라이언트는 다음 그림 6과 같이 구성된다. 임의의 공격자로부터 클라이언트 모듈내에 저장된 값들을 보호하기 위해 클라이언트 모듈에 저장되는 데이터는 모두 암호화된다. 클라이언트는 DRM 서버와 같이 인증 모듈, 관리 모듈, 암호 모듈 및 플레이어가 포함된다. 사용자는 실제 DRM 서버로부터 콘텐츠를 실행할 때, 콘텐츠에 대한 사용 규칙을 확인하고, 사용 권한에 대한 라이선스를 획득한다.

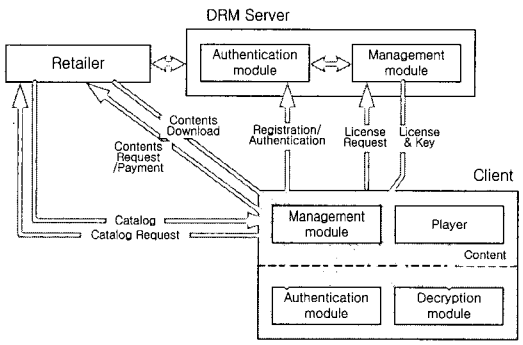

그림 6. 클라이언트 구조

3.3 인증 프로토콜 설계

본 논문에서는 보다 안전하고, 신뢰성 있는 디지털 콘텐츠 유통 및 인증을 위한 프로토콜을 제안한다. Retailer와 DRM 서버, Client간의 신뢰성 있는 디지털 콘텐츠 인증 프로토콜을 제안하고 있다. 공개키 암호 알고리즘을 적용하여 비밀키의 분배와 서명에 사용한다. 본 논문에서는 최소한의 정보만을 공개키 암호 알고리즘을 이용하여 암호화하고, 콘텐츠 및 다른 정보들은 일반적으로 관용암호 알고리즘을 사용하여 효율성을 고려한다.

본 논문에서 제안된 DRM 인증 프로토콜은 그림 4와 같은 DRM 서버, Retailer Packager, Client 간에 적용되는 프로토콜이다. 즉, 콘텐츠의 요청과 다운로드, 그리고 라이선스 발급 프로토콜을 제안한다.

3.3절에서 제안한 인증 프로토콜은 Retailer와 DRM 서버, Client간의 통신을 위하여 별도의 전문 형식을 만들어 소켓 통신을 하도록 설계한다. 사용되는 대칭키 암호 알고리즘은 AES와 SEED를 사용할 수 있게 설계하였고, 공개키 암호 알고리즘은 기본적으로 RSA를 사용하도록 설계한다. 그리고 해쉬 알고리즘으로는 SHA-1을 사용하도록 설계하였으나, 다른 알고리즘을 활용할 수 있도록 설계한다.

3.3.1 Contents Request(Message1) 소켓메시지 포맷

Contents Request(Message1) 소켓메시지 포맷은 표 3과 같고, 메세지의 각 필드는 다음과 같이 설명할 수 있다.

- OP code(2bytes) : 요청 패킷인지 다운로드 패킷인지를 나타내준다. message 1은 요청패킷이기 때문에 '01'값을 사용한다.
- Signature Algorithm(4bytes) : Binding ($E_{KUR}[E_{KRC}[User\_ID \| K_{BI}]]$)정보를 서명 및 암호화하기 위해 사용되는 알고리즘을 나타내는 필드이다. 기본적으로 RSA를 사용하기 때문에 '0001' 값을 사용한다. 다른 공개키 암호 알고리즘 사용시 필요한 필드이다.
- Hash Algorithm(2bytes) : Binding_Info 값을 적용하기 위하여 사용되는 해쉬 알고리즘의 종류를 나타내는 필드이다. 기본적으로 SHA-1을 사용하기 때문에 '01' 값을 사용한다.
- User_ID(8bytes) : Client의 고유 식별자이다. 상위 3bytes는 Retailer별로 분류된 값이고, 나머지 5bytse값은 Retailer별 고유 개인 식별자 값이다.
- Content_ID(8bytes) : 콘텐츠의 고유 식별자이다. 패키저에서 패키징될때 콘텐츠마다 생성된다. 상위 2bytes는 저작권자별로 분류된 값이고, 다음 1bytes는 콘텐츠의 종류, 나머지 5bytes는 콘텐츠의 고유 식별자 값이다.
- Nonce(8bytes) : 임시 비표값이다.
- Binding(20bytes) : $E_{KUR}[E_{KRC}[User\ ID \|$

표 3. Contents Request Message Format

OP code	Signature Algorithm	Hash Algorithm	User_ID	Content_ID	Nonce	Binding
2bytes	4bytes	2bytes	8bytes	8bytes	8bytes	20bytes

표 4. Contents Download Message Format

OP code	Length	Encryption Algorithm	Container_ID	Nonce	TS	Lifetime	Certificate	Encrypted Content
2bytes	4bytes	4bytes	8bytes	8bytes	2bytes	4bytes	variable	variable

표 5. License Request Message Format

OP code	Signature Algorithm	Hash Algorithm	User_ID	Retailer_ID	Content_Info	Binding	Certifiate
2byte	4byte	2byte	8byte	4byte	8byte	20byte	variable

표 6. License & Key Message Format

OP code	Signature Algorithm	Hash Algorithm	Encrytion Algorithm	User_ID	DRM Server_ID	Content_ID	License
2byte	4byte	2byte	4byte	8byte	4byte	8byte	variable

K_{BI}]]값이다. 사용자의 ID와 하드웨어정보가 Signature Algorithm 필드에 나타낸 공개키 암호 알고리즘으로 암호화되어 있는 값이다. K_{BI}는 Binding_Information으로 값은 Network Card의 MAC Address를 사용한다. 이 MAC Address 값을 해쉬 함수에 적용하여 나온 20bytes (160bits) 중 16bytes(128bits)만 사용한다.

3.3.2 Contents Download(Message2) 소켓메시지 포맷

Contents Download(Message2) 소켓메시지 포맷은 표 4와 같고, 메세지의 각 필드는 다음과 같이 설명할 수 있다.

- OP code(2bytes) : 요청 패킷인지 반환 패킷인지를 나타내준다. message 2는 다운로드 패킷이기 때문에 '02'값을 사용한다.
- Length(4bytes) : OP code~Certificate까지의 길이를 bytes 단위로 나타낸다.
- Encryption Algorithm(4bytes) : Content 암호화에 사용되는 알고리즘을 나타내는 필드이다. AES와 SEED를 사용한다. AES 알고리즘이 사용되면 '0001', SEED 알고리즘이 사용되면 '0002'값을 사용한다.
- Container_ID(8bytes) : 콘텐츠의 컨테이너 식별자로 라이선스를 발급 받기 위하여 저장되어 있는 DB에서 키값을 검색하기 위한 값이다.
- Nonce(8bytes) : 반환되는 임시 비표값이다.
- TS(4bytes) : Certificate가 발행된 시간이다.
- Lifetime(8bytes) : Certificate의 유효 시간으로 Not before 값과 Not after 값이 있다.
- Certificate : 라이선스를 얻기 위한 인증값 필드이다.
- Encrypted Content : 마스터키를 이용하여 암호화된 Content 필드이다.

3.3.3 License Request(Message3) 소켓메시지 포맷

License Request(Message3) 소켓메시지 포맷은 표 5와 같고, 메세지의 각 필드는 다음과 같이 설명할 수 있다.

- OP code(2bytes) : 요청 패킷인지 다운로드 패킷인지를 나타내준다. message 3은 요청패킷이기 때문에 '01'값을 사용한다.
- Signature Algorithm(4bytes) : Binding ($E_{KUR}[E_{KRC}[User\_ID \| K_{BI}]]$)정보를 서명 및 암호화하기 위해 사용되는 알고리즘을 나타내는 필드이다. 기본적으로 RSA를 사용하기 때문에 '0001' 값을 사용한다. 다른 공개키 암호 알고리즘 사용시 필요한 필드이다.

· Hash Algorithm(2bytes) : Binding_Info 값을 적용하기 위하여 사용되는 해쉬 알고리즘의 종류를 나타내는 필드이다. 기본적으로 SHA-1을 사용하기 때문에 '01' 값을 사용한다.
· User_ID(8bytes) : Client의 고유 식별자이다. 상위 3bytes는 Retailer별로 분류된 값이고, 나머지 5bytse값은 Retailer별 고유 개인 식별자 값이다.
· Retailer_ID(4bytes) : 판매자의 고유 식별자이다.
· Content_Info(8bytes) : 콘텐츠의 정보값으로 콘텐츠의 속성, 종류 등을 나타낸다.
· Binding(20bytes) : $E_{KUD}[E_{KRC}[User_ID \| K_{BI}]]$값이다. 사용자의 ID와 하드웨어정보가 Signature Algorithm 필드에 나타낸 공개키 암호 알고리즘으로 암호화되어 있는 값이다. Binding_Info 값은 Network Card의 MAC Address를 사용한다. 이 MAC Address 값을 해쉬 함수에 적용하여 나온 20bytes(160bits) 중 16bytes (128bits)만 사용한다.
· Certificate : 라이선스를 얻기 위한 인증값 필드이다.

3.3.4 License Download(Message4) 소켓메시지 포맷

License Download(Message4) 소켓메시지 포맷은 표 3과 같고, 메세지의 각 필드는 다음과 같이 설명할 수 있다.

· OP code(2bytes) : 요청 패킷인지 다운로드 패킷인지를 나타내준다. message 4은 다운로드 패킷이기 때문에 '02'값을 사용한다.
· Signature Algorithm(4bytes) : 라이선스 정보를 서명 및 암호화하기 위해 사용되는 알고리즘을 나타내는 필드이다. 기본적으로 RSA를 사용하기 때문에 '0001' 값을 사용한다. 다른 공개키 암호 알고리즘 사용시 필요한 필드이다.
· Hash Algorithm(2bytes) : 라이선스 정보를 적용하기 위하여 사용되는 해쉬 알고리즘의 종류를 나타내는 필드이다. 기본적으로 SHA-1을 사용하기 때문에 '01' 값을 사용한다.
· Encrytion Algorithm(4bytes) : 라이선스 암호화에 사용되는 알고리즘을 나타내는 필드이다. AES와 SEED를 사용한다. AES 알고리즘이 사용되면 '0001', SEED 알고리즘이 사용되면 '0002'값을 사용한다.
· User_ID(8bytes) : Client의 고유 식별자이다. 상위 3bytes는 Retailer별로 분류된 값이고, 나머지 5bytes값은 Retailer별 고유 개인 식별자 값이다.
· DRM Server_ID(4bytes) : 판매자의 고유 식별자이다.
· Content_ID(8bytes) : 콘텐츠의 고유 식별자이다. 패키저에서 패키징될때 콘텐츠마다 생성된다. 상위 2bytes는 저작권자별로 분류된 값이고, 다음 1bytes는 콘텐츠의 종류, 나머지 5bytes는 콘텐츠의 고유 식별자 값이다.
· License : 라이선스 데이터 필드이다.

Ⅳ. DRM 시스템 구현 및 분석

4.1 DRM 시스템 구현

본 논문에서는 제안된 DRM 시스템을 설계 및 구현하였다. 구현된 DRM시스템은 크게 DRM 서버와 클라이언트로 구성된다. DRM 시스템의 개발 환경은 다음과 같다.

· Clearinghouse Operation System : Windows 2000 Server
· Client Operation System : Windows XP Professional
· Language : Visual C++, Visual Basic, ASP, XML, ADSI
· Program Tool : Visual Studio 6.0 SP5
· DBMS : MS-SQL 2000
· Program Technology : Data Shaping

4.2 DRM 서버 구현

그림 7은 구현된 DRM 서버의 로그인 화면을 나타낸다. DRM 서버에서 각 콘텐츠 별로 테이블간의 데이터 구조를 트리 구조로 구성하고 연관된 컬럼정보를 DB로 쉽게 구축할 수 있도록 설계 하였다. 그림 8부터 그림 10은 이러한 설정 화면을 나타낸 것이다.

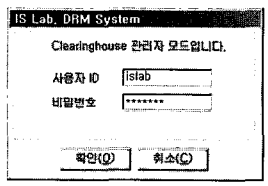

그림 7. DRM 서버 로그인 창

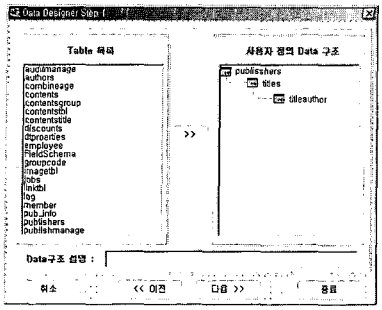

그림 8. Data Designer Step 1

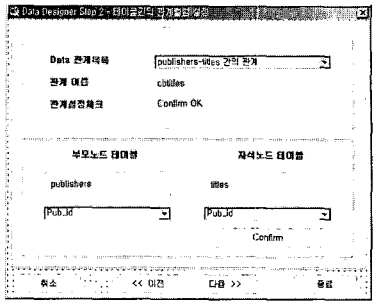

그림 9. Data Designer Step 2

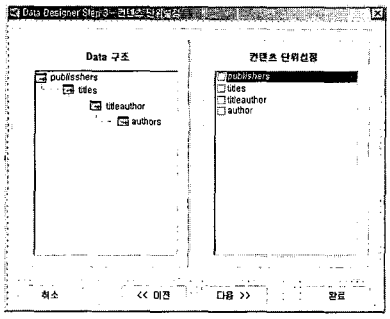

그림 10. Data Designer Step 3

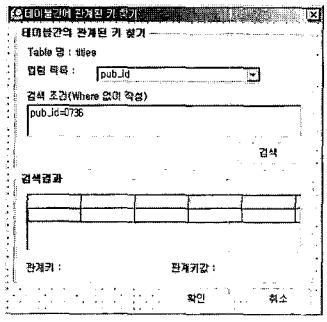

그림 11. 키관리 화면

그림 11은 콘텐츠 별 키를 관리할 수 있는 키 관리 모듈이다. 이 모듈은 KRS-KMS-LGS사이의 키 관리 통신을 지원한다.

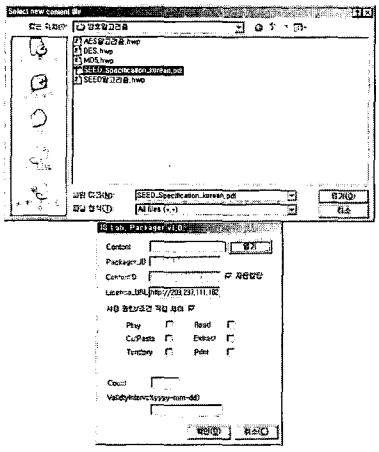

그림 12. DRM 패키징

그림 12는 콘텐츠 Packager 실행 화면이다. 패키징 대상파일을 한 개의 파일 또는 복수 개의 파일을 선택하여 생성할 수 있다. 패키징 옵션에는 사용권한 설정부분에서 패키징할 파일을 인쇄 혹은 원본 파일을 저장할 수 있게 할 것인가를 결정할 수 있다. 또한 횟수 제한 옵션을 이용하여 파일을 액세스할 때 사용할 수 있는 횟수를 제한할 수 있도록 설계 하였다. 기간제한 옵션은 선택하여 라이선스 유효 기간을 설정 할 수 있게 해준다. 또한 개봉 확인 옵션기능을 추가하여 클라이언트 시스템이 구현 되었을 경우 클라이언트에서 패키징된 파일을 받았을 경우 다시 통보할 수 있도록 설계하였다. 그림 13은 패키징된 콘텐츠의 정보를 확인할 수 있는 창이다.

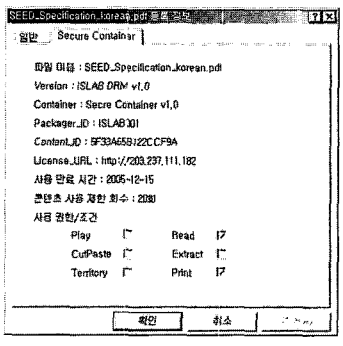

그림 13. DRM 패키징 정보

4.3 DRM Client 구현

DRM Client는 AES, SEED의 복호화 모듈과 SHA-1의 복호화 해쉬 모듈, 콘텐츠를 실행시킬 수 있는 Player나 View를 찾는 응용프로그램 링크 모듈, 인증을 받기 위한 인증 모듈, 그리고 이를 통합적으로 관리하는 관리 모듈로 구현하였다.

클라이언트는 Retailer에게 사용자 인증을 받기 위하여 일반적으로 사용하는 ID/Password 인증을 사용한다. 여기서 Password는 SEED로 암호화되어 전송된다.

다음 그림 14는 Retailer에 웹으로 접속하여 디지털 콘텐츠를 다운로드 받을 수 있도록 설계된 화면이다. XML을 이용하여 DRM DB와 연동할 수 있도록 설계하였고, ActiveX로 제작하여 웹과 연동하여 콘텐츠 다운로드 및 라이선스 발급을 위한 소켓메시지를 전달할 수 있도록 설계하였다. 다음 그림 14는 콘텐츠를 다운로드 및 라이선스 발급을 위한 브라우저 창과 설계된 drmclient.cab의 ActiveX 설치 화면이다.

그림 15는 다운로드 받은 콘텐츠의 정보를 확인하는 화면이다. 콘텐츠의 메타데이터와 인증 정보 및 라이선스 획득 정보 등을 확인할 수 있도록 설계 하였다. 그림 16은 1.mp3라는 음악콘텐츠를 DRM 서버에서 패키징 및 리패키징 하여 다운로드 받은 후, 클라이언트에서 실행 시킨 정상적인 디지털 콘텐츠의 실행화면이고, 그림 17은 하드웨어 정보, 즉 네크워크 카드의 MAC Address가 일치하지 않아, K_{BI}값을 이용하여 콘텐츠를 복호화하지 못하였을 때의 에러창이다. 그림 18은 라이선스가 없거나, 기한의 종료, 잘못된 라이선스 값일 때의 에러창이다.

4.4 DRM 시스템 분석

4.4.1 프로토콜의 보안 서비스 분석

3.3절에서 제안된 프로토콜은 디지털콘텐츠 보호와 안전한 유통을 위하여 설계된 프로토콜이다. 설계된 프로토콜은 콘텐츠의 기밀성, Client 인증, 단말기 인증, 재전송 공격 방지, 안전한 키분배 및 라이선스 배포 등의 보안 서비스를 제공하도록 설계하였다. 보안 서비스를 제공하기 위한 각 소켓메시지의 필드를 분석하면 다음과 같다.

가. Contents Request(Message1) 소켓메시지

· Noncel 필드 : 응답이 올바른 것이고 침입자에 의해 재전송된 것이 아니라는 것을 보증하기

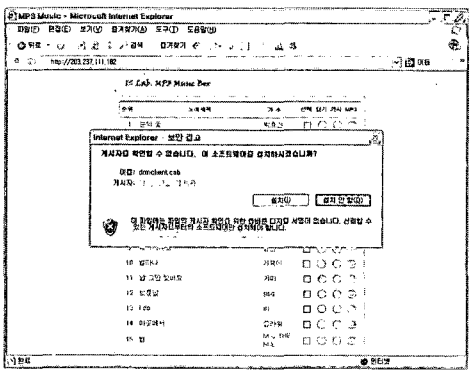

그림 14. 웹을 이용한 접속화면과 ActiveX 설치 화면

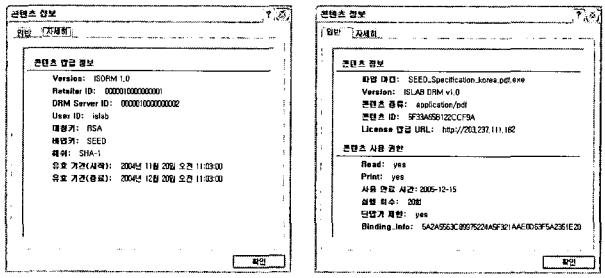

그림 15. 다운로드 받은 콘텐츠 정보 확인

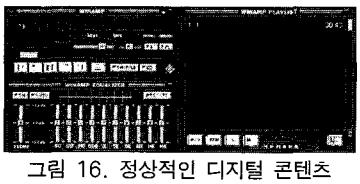

그림 16. 정상적인 디지털 콘텐츠 실행 화면

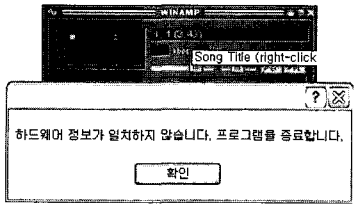

그림 17. 하드웨어 정보 에러

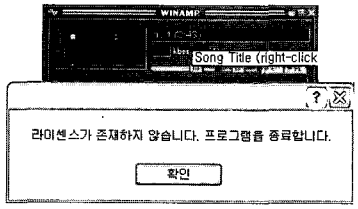

그림 18. 라이선스 에러

위해 메시지 2에서 반복되는 난수 값이다.

- Binding 필드 : Binding 필드는 $E_{KUR}[E_{KRC}[User_ID \| K_{BI}]]$값으로, K_{BI} 값은 라이선스를 발급받은 정당한 단말기에서만 콘텐츠를 실행하기 위한 단말기 인증을 위한 값이다. Client 인증을 위하여 $User\_ID \| K_{BI}$ 값을 Client의 개인키인 K_{RC}로 암호화하여 서명한다. K_{BI}는 후에 비밀키로 사용되기 때문에 서명된 값을 Reatailer의 공개키인 K_{UR}로 암호화하여 K_{BI}의 기밀성을 보장한다.

나. Contents Download(Message2) 소켓메시지

- TS, Lifetime 필드 : Certificate의 발행시간과 유효기간을 전송함으로써 재전송 공격을 방지한다
- Certificate 필드 : Certificate 필드는 $E_{KUD}[E_{KRR}[K_{R.D}]] \| E_{KR.D}[Content_ID \| User_ID \| Retailer_ID \| K_{BI} \| TS_1 \| Lifetime]$값이다. Content_ID, User_ID, Retailer_ID, K_{BI}, 인증서 발행 시간 TS_1, 유효시간 Lifetime의 정보가 세션키 $K_{R.D}$로 암호화한 값을 가지고 있다. 그리고 세션키 $K_{R.D}$의 안전한 분배를 위하여 공개키 알고리즘을 적용하였는데 $K_{R.D}$를 Retailer가 생성하였다는 것을 증명하기 위하여 Retailer의 개인키 K_{RR}로 서명한 후, 기밀성을 유지하기 위하여 DRM Server의 공개키 K_{UD}로 암호화하였다.
- Encrypted Content 필드 : Packager에서 콘텐츠 마스터 비밀키 K_{CON}으로 암호화한 값을 다시 K_{BI}로 암호화하여 전송한다. K_{BI}를 이용하여 콘텐츠를 암호화함으로써 제한된 단말기내에서만 콘텐츠가 실행될 수 있도록 할 수 있다. 즉, Hardware로부터 구한 값이 다르면 콘텐츠 자체를 실행할 수 없게 된다.

다. License Request(Message3) 소켓메시지

- Binding 필드 : Binding 필드는 $E_{KUD}[E_{KRC}[User_ID \| K_{BI}]]$값이다. 라이선스 요청을 위해 클라이언트가 서명한 User_ID와 K_{BI}값을 기밀성을 위해 DRM 서버의 공개키로 암호화한다.
- Certifiate 필드 : Message2에서 Retailer에게 전송받은 인증서로, DRM 서버만이 세션키 $K_{R.D}$를 회수하여 내용을 볼 수 있도록 설계하였다. 라이선스를 발급받기위한 티켓으로 사용된다.

라. License Download(Message4) 소켓메시지

- License 필드 : License 필드는 발급되는 라이선스 데이터로 $\{E_{KBI}[E_{KUC}[K_{CON}] \| TS1 \| Lifetime \| Option \| Condition] \| E_{KRD}[H[User_ID \| DRMServer_ID \| Content_ID \| E_{KUC}[K_{CON}]]]\}$값이다. Client에서는 $License_C$의 서명값을 확인하여 라이선스 발급이 정확히 이루어졌는지 검사한다. 그리고 자신의 하드웨어 정보(Binding)에서 비밀키 K_{BI}를 구해서 $E_{KBI}[E_{KCON}[Content]]$를 해독하여 $E_{KCON}[Content]$를 구해낸다. 그 다음 자신의 개인키 K_{RC}로 $E_{KUC}[K_{CON}]$를 복호화하여 K_{CON}을 구해낸다. 그러나 반드시 K_{CON}값은 TRM내에서만 존재하게 하여, User는 이 값을 직접 취하지 못하도록 설계되었다. 최종적으로 K_{CON} 값을 이용하여 Content를 실시간 복호화하여 Content를 사용한다. 복호화된 Content 정보도 반드시 TRM내에서만 존재하여야 하며, 이를 위해 Memory Hooking 기술이 적용하였다.

4.4.2 기존 DRM 시스템과 비교

다음 표 7은 제안된 DRM 시스템과 기존 DRM 시스템과의 비교를 나타낸다[9,10]. 비교 대상인 기존 DRM 시스템은 다음과 같은 특징을 가지고 있다. ContentGuard는 초기에 InterTrust와 같이 선도기술을 보유하여 DRM 시장을 리드해 왔으나, 최근에는 Vender DRM(기존의 자신의 제품에 DRM을 추가하는 시스템을 의미)이 나오면서 새로운 DRM 시스템들이 개발되고 있다. MS의 Microsoft Media Player가 대표적인 Vender DRM으로서, MicroSoft의 DRM 기술인 WMRM(Windows Media Right Manager)은 MicroSoft Media Player에 WMT(Window Media Technology)라는 DRM 기술이 추가되어 윈도우 미디어 파일의 유통 및 보안을 위해 개발되었다[11]. 전자책 시장의 사실표준으로 자리 잡고 있는 Acrobat Reader역시 Vender DRM으로 볼 수 있으며, Adobe PDF 기반의 DRM인 ACS(Acrobat Content Server)를 개발하였다.

본 논문에서 설계 및 구현한 DRM 시스템은 라이

선스 보안 측면에서는 다른 시스템에 비하여 하드웨어 바인딩 정보인 K_{BI}로 라이선스를 암호화함으로써 라이선스 자체의 변경 및 불법 사용자의 도용, 위조를 방지할 수 있다. 하지만 라이선스의 2중 암호화라는 라이선스 발급 서버의 처리 용량을 증가시킬 수 있다는 단점이 있다. 또한 라이선스 발급 방식은 MicroSoft WMRM과 같이 별도로 다운로드 받는 방식을 이용하였다. 콘텐츠에 라이선스를 포함하는 방식은 오프라인 상으로 라이선스의 권한을 부여받을 수 있기 때문에 공격이 쉬워진다. 본 논문의 방식은 콘텐츠의 메타정보에 라이선스를 발급 받기 위한 URL을 정의함으로써 다른 시스템의 콘텐츠에 라이선스를 포함하는 방법보다 안전하다고 볼 수 있다.

또한 복호화 키의 관리 기법 중 다른 시스템의 라이선스에 포함되는 기법은 라이선스가 크랙 되면 콘텐츠의 마스터키가 노출됨으로 콘텐츠의 불법 유통은 걷잡을 수 없게 된다. 하지만 제안된 DRM 시스템에서는 콘텐츠의 복호화 키를 라이선스에 포함되어 있는 마스터키와 클라이언트의 하드웨어 바인딩 정보 2개를 이용함으로써 제3자가 라이선스 값을 획득하여도 콘텐츠를 복호화할 수 없게 된다.

또한 블록암호 알고리즘인 AES, SEED를 이용하였기 때문에 실시간으로 콘텐츠를 실행할 수 있는 스트리밍 서비스도 지원 가능하다. 또한 기존의 DRM 시스템은 자사의 콘텐츠를 보호하고 유통하기 위하여 개발되었기 때문에 자사의 콘텐츠 및 제한된 콘텐츠 타입을 지원하고 있다. 하지만 본 논문에서 제안된 DRM 시스템은 모든 콘텐츠를 패킹할 수 있도록 설계되어 있고, 또한 콘텐츠 실행시 확장자를 이용하여 응용프로그램을 자동 링크하기 때문에 클라

표 7. 기존 DRM 시스템과 제안된 DRM 시스템의 비교

	MicroSoft WMRM	Adobe PDF Merchant DRM	ContentGuard	제안한 DRM 시스템
라이선스에 대한 보안	· 다른 PC로 복제 방지 · 기간/횟수 조작 방지 · Tampering 방지	· 다른 PC로 복제 방지 · 기간/횟수 조작 방지 · Tampering 방지	· 다른 PC로 복제 방지 · 기간/횟수 조작 방지 · Tampering 방지	· 다른 PC로 복제 방지 · 기간/횟수 조작 방지 · Tampering 방지 · 라이선스에 하드웨어 바인딩 기법 적용
Super Distribution	지원	미지원	미지원	지원 가능
암호화된 콘텐츠 구성	암호화+메타정보(URL)	암호화+라이선스	암호화+라이선스	암호화+메타정보(URL)
패키징시 비즈니스룰 지정	미지정	지정	지정	지정
암호화 키 관리	서버+암호화된 콘텐츠 파일 내 속성	서버	별도파일(Rights-Label)	서버+클라이언트 (하드웨어 바인딩 정보)
복호화 키 관리	라이선스 내에 포함	라이선스 내에 포함	라이선스 내에 포함	라이선스 내에 포함 클라이언트 정보
메타데이터 저장 위치	암호화된 콘텐츠 파일 내 속성	라이선스 내에 포함(암호화된 콘텐츠와 독립)	라이선스 내에 포함(암호화된 콘텐츠와 독립)	암호화된 콘텐츠 파일내 속성
라이선스 관리	· 한 파일로 관리 · plain text · key만 암호화	· 한 파일로 관리 · plain text · key만 암호화	· 라이선스마다 다른 파일 · plain text · key만 암호화	· 라이선스마다 다른 파일 · xml 문서 · key만 암호화 · 전자 서명 기능
서비스 방법	다운로딩	다운로딩	다운로딩	다운로딩+ 스트리밍 지원 가능
콘텐츠 지원 타입	Audio, Video	PDF, EBX	HTML, XML, ASCII, PDF, MS Office 등	모든 콘텐츠 지원

이언트에 콘텐츠 View가 설치되어 있다면 모든 콘텐츠가 지원 가능하다. 하지만 파일의 크기가 크고 시스템 점유율이 큰 콘텐츠, 즉 예를 들면 동영상 같은 파일은 시스템의 부하가 많이 걸릴 수 있다. 하지만 이러한 콘텐츠는 부분(구간) 암호화 기법을 적용하여 해결할 수 있다.

V. 결 론

본 논문에서는 개방형 네트워크 상에서 콘텐츠의 창조자, 저작권자, 제작자, 배포자, 사용자 등 유통 주체의 권리를 보호하면서도 안전하고 투명한 콘텐츠 유통을 지원하는 통합 솔루션 설계하였다. 제안된 시스템은 유무선 네트워크 환경을 지원하는 유통 플랫폼과 저작권 정보 위조/변조/해킹을 방지하기 위한 DRM 기반 소프트웨어를 이용하여 각 유통 주체의 권리를 보호하며 클리어링 센터 시스템을 통해 투명한 콘텐츠 유통을 지원한다. 또한 다양한 응용 서비스 플랫폼에서 상호 호환성을 위한 저작권 정보표현 및 콘텐츠 사용규칙 및 유통 주체와 클리어링 센터간에 교환되는 정보 표현을 설계하였다.

본 논문에서는 DRM 유통 프레임워크를 제안한 다음, 크게 클리어링하우스 설계와 DRM 클라이언트 설계, DRM 인증 프로토콜 설계를 하였다. 클리어링하우스는 DRM 서버와 Packager를 하나의 시스템에 포함하여 설계하였다. DRM 서버에서 키 관리는 XML형식의 문서와 소켓 통신을 이용하여 KRS와 KMS, LGS 간의 데이터 교환의 효율성을 높였다. Packager의 패키징에 사용된 암호 알고리즘은 표준 암호 알고리즘이 AES와 SEED를 적용하였다. DRM Client는 자체 블록 보호 기법 및 동적 디코딩 기법을 활용하여 클라이언트 및 콘텐츠 보안을 강화하였다. 또한 콘텐츠의 복호화를 위해 AES와 SEED의 복호화 모듈, 메타데이터 해석기 등을 설계하였다. 또한 이러한 DRM 시스템의 유통 구조의 신뢰성을 위해 인증 프로토콜을 제안하였다. 하드웨어 바인딩 기법과 공개키 암호 알고리즘, 관용 암호 알고리즘, 해쉬 알고리즘을 적용하여 Client의 인증과 라이선스 획득을 위한 프로토콜을 제안하였다.하드웨어 바인딩 기법을 이용하여 단말기 인증과 실행 단말기 제한을 제공하도록 설계하였다. 또한 콘텐츠의 기밀성, Client 인증, 재전송 공격 방지, 안전한 키분배 및 라이선스 배포 등의 보안 서비스를 제공할 수 있는 시스템을 설계하였다.

본 논문에서 제안한 DRM 시스템은 콘텐츠의 창조자, 저작권자, 제공업자, 유통업자, 사용자 등 유통 주체 모두가 안전하고 효율적이면서 경제적인 방법으로 콘텐츠를 제작 유통, 소비할 수 있는 기반이 되며 콘텐츠 유료화에 다른 과세/통계 처리 등을 위한 투명한 전자 상거래 인프라로 활용되어 디지털 콘텐츠 제작과 전자상거래 분야의 활성화뿐만 아니라 콘텐츠 유통과 관련된 산업 전 분야에 활용될 수 있을 것으로 기대된다. 나아가 무선 시스템으로의 접목을 통하여 모바일 시대의 콘텐츠 문화 사업에 활용할 수 있을 것이다.

참 고 문 헌

[1] Intel, "Content Protection in the Digital Home", Volume 06, Issue 04, *Intel Technology Journal*, 2002/11/15

[2] Y.Jeong, K. Yoon, J. Ryou, "A Trusted Key Management Scheme for Digital Rights Management", *ETRI Journal*, Vol.27, No.1, Feb., 2004

[3] G. Hanaoka, K. Ogawa, I. Murota, G. Ohtake, K. Majima, S. Gohshi, K. Oyamada, S. Namba, and H. Imai, "Managing Encryption and Key Publication Independentaly in Digital Rights Management Systems", *IEICE TRANS. FUNDAMENTALS*, Vol.E87-A, No.1, Jan., 2004

[4] Michael Ripley, "Utilizing Content Protection Technologies", *Intel Developer Forum*, 2002/09/12

[5] Intel, "Advanced Digital Set Top Box Design - White Paper Revision 1.0", 2003/09

[6] Ahmet M. Eskicioglu, "MULTIMEDIA PROTECTION IN DIGITAL NETWORKS", *CNIS 2003*, 2003

[7] 최종욱, "기업내 디지털정보보호 기술", 상명여자대학교, 2001.

[8] ETRI, "DRM기반 하의 디지털 컨텐츠 유통 솔루션 개발", 정보통신부, 2003.

[9] DRM 포럼 운영, 정보통신표준화전략포럼 최종연구보고서, Dec, 2002.

[10] 이진홍, 김태정, 박지환, "컨텐츠 스트리밍을 위한 안전한 DRM 시스템 설계 및 구현", *정보보호학회논문지*, 제13권, 제4호, 2002. 8.

[11] Microsoft : http://www.microsoft.com/windows/windowsmedia/forpros/drm/default.mspx

〈著者紹介〉

김 종 우 (Jong-woo Kim) 정회원
1998년 2월 : 조선대학교 전자공학과 학사
2000년 8월 : 조선대학교 대학원 전자공학과 석사
2005년 2월 : 조선대학교 대학원 전자공학과 박사
2005년 4월~2006년 2월 : 조선이공대학 인터넷정보과 전임강사
2005년 2월~현재 : (주)일우통신 이사
2003년 3월~현재 : 조선대학교 정보통신공학과 외래교수
〈관심분야〉 통신보안시스템설계, 네트워크 보안, DRM, 무선 네트워크 보안

양 원 일 (Won-il Yang) 정회원
1972년 2월: 조선대학교 전기공학과 학사
1982년 2월: 조선대학교 전기공학과 석사
2001년 2월: 동신대학교 전기전자공학과 박사
1983년 3~현재 : 조선대학교 전자공학과 교수
〈관심분야〉 이동통신, 위성통신, 무선통신시스템, 멀티미디어 통신

한 승 조 (Seung-Jo Han) 정회원
1980년 2월 : 조선대학교 전자공학과 학사
1982년 2월 : 조선대학교 대학원 전자공학과 석사
1994년 2월 : 충북대학교 대학원 전자계산학과 박사
1998년 12월~ 2000년 12월 : (주)소프트프로텍 대표이사
2000년 11월~2002년 3월 : (주)소프트프로텍 북미지사장
1986년 5월~1987년 3월 : Univ. of New Oleans 객원교수
1995년 2월~1996년 1월 : Univ. of Texas 객원교수
2000년 12월~ 2002년 2월 : UC 버클리대학 객원교수
1997년~ 현재 : 조선대학교 정보통신공학과 교수
〈관심분야〉 통신보안시스템설계, 네트워크 보안, ASIC설계, DRM