컨텐츠 공유를 위한 DRM 호환 모델

박정석, 박명순
고려대학교 컴퓨터과학기술대학원
e-mail:parkjs@hec.co.kr, myongsp@korea.ac.kr

DRM Interoperability Model for Contents Sharing

Jung-Suk Park, Myong-Soon Park
Graduate School of Computer Science and Technology, Korea University

요 약

기업에서 적용하고 있는 문서보안 DRM 시스템에서 상이한 라이센스 정책을 사용하는, 다양한 기술 기반의 DRM Client 간에 컨텐츠를 공유하기 위해서는 DRM 기술에 대한 호환성이 보장되어야 한다. 여러 DRM 기술들이 시장에 공존하는 현재와 같은 상황에서는 DRM Client 간의 호환이 어려워 다양한 기술이 적용된 DRM Client가 사용자 라이센스 정보를 교환하여 컨텐츠를 공유하기란 어려운 일이다. 본 논문에서는 사용자 공인 인증 방식과 라이센스 공유 방식을 통해 DRM Client간 컨텐츠를 호환하는 모델을 제안한다.

1. 서론

컨텐츠의 디지털화와 인터넷을 통한 유통 환경이 발달됨에 따라 컨텐츠 저작권자의 권익을 사용자로부터 보호하기 위한 DRM(Digital Rights Management) 기술이 컨텐츠 유통시장에서의 필수 요건이 되었다. 아울러 DRM 기술을 보유한 여러 업체들 사이의 기술 표준화와 상호 호환성 문제가 또 다른 이슈가 되었고 각종 연구단체에서 표준화에 대한 연구가 진행되고 있다.

최근 들어 이 DRM 기술을 활용하여 기업(또는 기관)의 내부 기밀자료의 외부 유출을 방지하고 사용자 인증을 통하여 인증된 사용자만이 해당 자료를 열람하고 사용할 수 있도록 하기 위한 문서보안 시스템을 기업들이 앞 다투어 도입하고 있다. 이에 따라 문서보안 DRM 시장에서도 여러 업체들의 상이한 기술들이 혼재함에 따라 표준화와 호환성 문제가 대두되고 있다.

DRM 시스템에서 DRM Client(일명 DRM Agent)는 DRM 서버로부터 사용자가 요청한 컨텐츠의 암호화된 형태와 함께 사용자의 컨텐츠에 대한 권한을 넘겨받아 그 권한에 따라 컨텐츠를 사용자에게 제공한다. 만약 이때 상이한 기술 기반의 2개 이상의 DRM 클라이언트가 한 시스템에 존재하게 되면 DRM Client 간에 사전에 약속된 라이센스 교환 정책이 없는 한 각각의 DRM 서버로부터 다운받은 컨텐츠를 공유하기란 어렵다.

이에 본 논문에서는 사용자에 대한 공인 인증 방식과 라이센스 공유 방식을 통해 DRM Client 간에 컨텐츠를 공유하는 방안을 제안한다.

본 논문의 구성은 다음과 같다. 먼저 제 2장에서 DRM의 요소기술을 소개하고, 제 3장에서는 여러 DRM 간의 비호환성에 의해 발생 가능한 문제점을 기술한다. 제 4장에서는 DRM Client 간 컨텐츠 공유를 위해 사용자 중앙 인증 방식과 라이센스 정보 공유방식의 DRM 모델을 제시한다. 제 5장에서는 결론과 향후 연구 방향을 기술한다.

2. DRM의 요소 기술

일반적인 DRM 시스템을 구성하는 요소기술은 다음과 같다

2.1 암호화 기술

DRM은 컨텐츠를 암호화하여 사용자에게 전달하게 되고 사용자는 해당 컨텐츠를 사용하기 위해서 복호화 과정을 수행한다. 암호화 기술이란 컨텐츠 및 라이센스를 암호화하는 것을 말하며, 기본적으로 대칭 암호화 방식과 비대칭 암호화 방식이 있다.

2.2 키 관리 및 분배 기술

키 관리 및 분배기술은 암호화한 키에 대한 저장 및 배포기술을 말한다. 키 관리 방식은 중앙서버에서 관리하는 방식과 키를 컨텐츠와 함께 전송하여 Client에서 관리되는 방식으로 나눠진다.

키 분배 방식으로는 대칭키 방식과 공개키 방식이 있으며 대칭키 방식은 하나의 키 분배 서버를 통해 모든 컨텐츠 거래의 키 분배가 이루어진다. 반면 공개키 방식은 분산성, 확장성, 상호운용성 등에서 유리하나 공개키 기반 구조 PKI(Public Key Infrastructure)가 필요하다[1].

2.3 권한표현 기술

컨텐츠의 사용을 위해 부여된 사용권한 및 사용조건에 관한 정보단위를 라이센스라고 한다. 라이센스는 XML로 인코딩된다. 대표적인 라이센스 표현 언어에는 XrML[2](eXtensible rights Markup Language)이나 ODRL[3](Open Digital Rights Language), XMCL(eXtensible Media Commerce Language) 등과 같은 XML 기반의 언어들이 있다.

2.4 사용자 인증 기술

사용자별로 구별되는 라이센스를 컨텐츠에 적용하기 위해서는 사용자 인증 과정이 필요하다. 일반적으로 사용자 인증 처리를 위해 사용되는 기술은 ID/Passwd, Digital Certificate, SSO(Single Sign On), 생체인식, 디바이스 인증 기술이 있다.

DRM은 특정 인증 기술에 종속될 필요는 없지만 적용되는 응용 애플리케이션이나 도메인에 따라 상이한 인증 기술을 사용하므로 다른 시스템의 인증체계와의 연동이나 통합을 고려할 필요가 있다[4].

2.5 라이센스 전송 방식

라이센스 전송 방식은 크게 3가지로 구분된다.

Forward-lock 방식은 컨텐츠 사용권한에 따른 통제를 특별히 하지 않고 컨텐츠가 사용자에게 전송된 후 제 3의 디바이스로 전송되지 못하도록 하는 방식이다.

Combined Delivery 방식은 암호화된 컨텐츠에 라이센스가 포함되어 전송되는 방식으로 사용권한에 따른 다양한 통제가 이루어진다. 이 방식은 Forward-lock 방식에 비해 보안성이 높고 다양한 사용권한 통제가 가능하지만 컨텐츠 자체가 특정 사용자에게 종속되어 암호화되므로 컨텐츠 유통 측면에서는 한계가 있다.

Separate Delivery 방식은 암호화된 컨텐츠와 라이센스를 별도로 분리하여 처리하는 방식으로 전송된 컨텐츠를 사용하는 시점에서 라이센스의 취득 유무를 판단하고 취득된 라이센스에 따라 컨텐츠 사용을 통제하게 되므로 컨텐츠의 재배포를 통하는 경우에도 원활한 보호 및 통제가 가능하다. 본 논문에서는 separate delivery 방식에 의한 모델을 제시한다.

3. DRM 간의 비호환성

본 장에서는 DRM 시스템간의 비호환성에 따른 현상 및 문제점을 기술한다.

하나의 사용자 디바이스에 서로 다른 DRM 기술이 적용된 DRM Client A, B가 공존하는 경우 다음과 같은 상황이 발생 가능하다.

- 라이센스 교환 및 인식문제 : 두 Client간 사전 약속된 라이센스 교환 정책 또는 호환 방안이 없을 경우 라이센스를 교환하거나 공유할 수 없고 라이센스 표현방식이 다를 경우 인식도 불가능하다. 따라서 DRM 서버 A로부터 다운로드 받은 문서는 Client A를 통해서만 라이센스를 전송받아 복호화 할 수 있으며 Client B에 의해서는 복호화 되어 질 수 없다.
- 사용자 인증문제 : 기존 DRM 시스템의 경우 DRM 서버와 DRM Client가 한 쌍을 이루어 서버와 해당 Client간의 통신으로만 인증이 이루어지는 방식이다. 이 경우 하나의 사용자 디바이스에 존재하는 두 개의 Client가 서로 다른 인증방식을 사용하게 되면 각 Client는 한 사람의 사용자를 서로 다른 사용자로 인식하게 된다. 따라서 각 DRM Client는 각각의 DRM 서버와의 별도 인증을 거쳐야 한다.
- 컨텐츠 사용상 문제 : DRM의 컨텐츠 보호라는 기술 특성상 컨텐츠 사용을 위한 Viewer 프로그램(또는 특정 application)이 실행되는 과정을 항상 DRM Client가 모니터링하고 통제를 하게 되므로 서

로 다른 DRM Client가 서로의 구동을 억제하는 상황이 발생한다. 본 논문에서는 하나의 Client로 사용자 인증 및 문서 복호화를 하여 Client 서로 간의 간섭을 피하는 방법으로 해결책을 제시하고자 한다.

이러한 제약점들은 컨텐츠의 전자상거래에서와 마찬가지로 기업의 문서보안 DRM 시스템에 있어서도 향후 기업과 기업 간의 업무를 위한 전자문서의 전달에 있어서 문서의 보안이란 측면과 문서의 원활한 교환이라는 측면을 모두 고려한다면 해결되어야 하는 과제이다.

4. 문서보안 DRM의 호환을 위한 제안 모델

4.1 DRM 호환 모델

본 논문에서 제시하는 DRM 호환 모델은 앞서 2장에서 제시한 여러 기술 내용들 가운데 다음과 같은 사항을 준수한다. (표 1 참조) 그리고, 모든 시스템의 특성을 결정짓기 위하여 다음과 같이 몇 가지 가정을 도입한다.

- 각 참여자는 PKI를 통한 기존의 공인 인증 방식을 사용하여 인증된 공개키-개인키 쌍과 공개키 인증서를 소지하고 있다.
- 각 DRM 시스템은 상호 호환되는 권리표현 언어를 사용하여 라이센스를 표현하여 서로 인식이 가능하다.
- 각 DRM 시스템은 컨텐츠 암호화시 동일 메커니즘을 사용한다.
- 각 DRM 서버에서 생성되는 컨텐츠의 고유ID는 DOI(Digital Object Identifier)와 같은 표준 식별체계에 의해 생성된 컨텐츠ID를 이용하여 Unique하게 관리된다. (컨텐츠 ID 부여 시스템을 별도로 두어 컨텐츠 ID를 관리하는 방법이 있다[5].)

표 1. 설계 모델의 사양 정의

내용	Specification
라이센스 전송 방식	separate delivery 방식
키 분배 기술	PKI기반의 공개키 암호화 방식
키 관리 기술	중앙 인증서버 공유
인증 방식	중앙 서버 공인 인증 방식

위에서 제시한 사항 및 가정에 따라 본 논문에서 제안하는 공인 인증 방식과 라이센스 공유 방식을 사용하는 DRM 시스템을 그림 1에서 나타낸다.

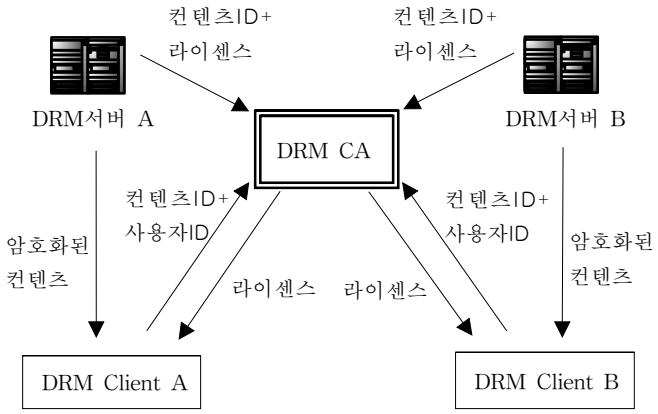

그림 1. DRM 모델

그림 1 DRM 모델의 동작순서는 아래와 같다.

① 각각의 참여자는 DRM CA(Certificate Authority, 공인인증센터)에 공개키를 등록하고 인증서를 발급받는다.

② DRM Client는 해당 DRM 서버로부터 암호화된 컨텐츠를 다운로드한다.

③ DRM 서버는 해당 컨텐츠에 대해 생성된 고유 컨텐츠ID와 함께 라이센스를 DRM CA에 전송한다.

④ 사용자의 컨텐츠 사용 시점에서 DRM Client는 DRM CA에 해당 컨텐츠ID와 사용자ID를 보내고 라이센스를 요청한다.

⑤ DRM CA는 사용자에 대한 인증을 거친후 라이센스의 변경여부를 컨텐츠를 제공한 DRM 서버에게 요청하여 확인 후 라이센스를 사용자에게 전송한다.

⑥ DRM Client는 제공받은 라이센스로부터 컨텐츠의 복호화 키를 추출하여 컨텐츠를 복호화한다.

4.2 라이센스 전송 프로토콜

다음은 DRM의 호환 모델에 있어서 라이센스 공유를 위한 DRM CA와 Client 간의 라이센스 전송 프로토콜을 살펴보기로 한다.

DRM Client(C)는 DRM CA(A)에게 라이센스 전송을 요청한다. 요청을 받은 A는 C에게 라이센스($License$)를 전송한다. 프로토콜에서 C와 A는 Diffie-Hellman 방식으로 공유되는 세션키 K를 생성한다.

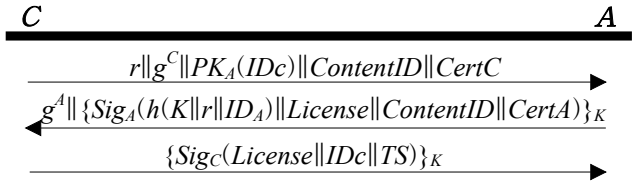

그림 2. 라이센스 전송 프로토콜

프로토콜(그림 2)이 시작되면 사용자는 난수 C를 생성하여 세션키 설정용 임시 공개키 g^C 를 계산하고 세션키 생성에 사용할 난수 r과 사용자 ID(ID_C)를 A의 공개키(A의 공개키 PK_A와 ID ID_A는 상호 인증을 통해 확인한 상태로 가정)로 암호화한 값 $PK_A(ID_C)$를 해당 컨텐트의 ID(*ContentID*), *CertC*와 함께 A에게 보낸다.

A는 임의의 난수를 생성하여 세션키 설정용 임시 공개키 g^A 를 계산하여 C로부터 전송받은 난수 r과 C의 임시 공개키 g^C를 이용하여 C와 공유하는 세션키 $K=h((g^A)^C||r)$을 생성하고, K와 r, ID_A 를 해쉬함수 h로 처리한 값과 *License*, *ContentID*, *CertA*를 세션키 K로 암호화한 값을 g^A와 함께 C에게 전송한다. (라이센스 변경 여부의 실시간 확인을 위한 DRM 서버와의 통신 프로토콜은 생략한다.)

C는 메시지를 복호화하여 *License*를 확인하고 전송받은 $h(K||r||ID_A)$가 K, r, ID_A를 해쉬 처리한 값과 일치하는지 확인하여 A의 실체를 검증한다. 마지막으로 수신한 라이센스(*License*)와 자신의 신원(ID_C)을 타임스탬프(*TS*)와 같이 전자서명하여 A에게 전송한다.

라이센스의 전송이 성공하면 컨텐츠 복호화 키를 생성할 수 있는 키 값을 추출하고 라이센스의 사용규칙에 따라 컨텐츠를 사용하도록 한다.

제안된 모델을 이용하면 사용자에 대한 인증이 공인인증서를 통하게 되므로 DRM 시스템별로 별도의 인증이 불필요하며, 라이센스 관리가 DRM CA를 통해 공유됨으로써 컨텐츠의 공유가 가능해진다.

4.3 사용이력 로깅

문서보안 DRM의 경우 보안사고 예방을 위해 컨텐츠 사용자의 사용이력에 대한 지속적인 시스템 감시가 필요하다. 그러므로 다음과 같이 사용이력에 대한 관리가 필요하다. DRM Client는 사용자의 컨텐츠 사용이력을 DRM CA에 전달하고 각 DRM 서버는 자신으로부터 배포된 컨텐츠ID에 대해 주기적으로 해당 컨텐츠에 대한 사용이력을 추출하여 사용자의 컨텐츠 사용내역을 모니터링 하도록 관리자에게 제공한다.

4.4 제안 시스템의 고찰

제안된 DRM 모델은 컨텐츠와 라이센스를 분리하고 라이센스를 중앙의 공용 서버에서 관리토록 함으로써 DRM Client가 해당 DRM 서버와의 통신을 통해서만 컨텐츠를 이용할 수 있다는 제약을 개선하여 특정 DRM 서버에 종속되지 않게 하였다.

라이센스를 중앙 인증서버에 공유함으로써 라이센스 교환 및 인식문제를 개선하고 공인인증서를 사용한 인증 방식을 사용하여 각 시스템별 별도의 인증이 불필요하도록 개선하였다. 또한 DRM Client간의 충돌문제는 하나의 클라이언트에서 여러 DRM 서버의 컨텐츠를 사용하게 함으로써 충돌문제를 원천적으로 피하도록 하였다.

5. 결론 및 향후 연구

본 논문에서는 서로 다른 DRM 기술 및 라이센스 정책을 사용하는 DRM Client가 하나의 사용자 디바이스에 공존할 경우 한번의 인증만으로 각 DRM 시스템으로부터 전송된 컨텐츠를 공유하는 모델을 제안하였다. 기업의 문서 외부 유출 방지를 위한 문서보안 DRM 시장은 현재 기업 내부로부터의 요구에 의해 점차 확대되고 있는 상황이다. 여러 문서보안 DRM 제품이 시장에 존재하는 상황에서 기업(혹은 기관)과 기업이 서로 간에 전자문서를 교환하는 과정에서 발생할 수도 있는 비호환성 문제를 해결하기 위해 사용자의 공인 인증 방식과 컨텐츠 라이센스를 공유하는 방식의 DRM 모델을 제안하였다. 향후 전달받은 라이센스를 사용자 디바이스의 비밀영역에 보관하여 DRM Client 간에 공유하는 방식이 연구될 수 있으며, 하나의 DRM 클라이언트만을 사용하면서 여러 문서보안 DRM 서버로부터 다운 받은 컨텐츠를 DRM CA와의 인증을 통해 사용하는 식의 연구가 진행되어 DRM Client는 하나로 통일하고 DRM 서버는 컨텐츠를 분배하는 역할로서만 존재하는 모델도 연구될 필요가 있다.

참고문헌

[1] 박복녕, 김태윤, “디지털 컨텐츠 저작권 보호를 위한 라이센스 분배 프로토콜”, 한국정보과학회 가을 학술발표논문집 Vol. 29. No. 2, 2002

[2] http://www.xrml.org

[3] http://odrl.net

[4] 강호갑, “지식정보관리시스템의 DRM역할과 통합방안”, 파수닷컴기술문서, http://www.fasoo.com

[5] ETRI, "디지털 콘텐츠 요통기술 동향 및 전망“, Digital Content Conference 서울 2003 발표자료, http://www.dc.or.kr/down/20031204/320-1%20dcc발표자료.pdf