DRM 호환성 모델에서의 컨텐츠 이용 기법

이병래, 장경아
삼성전자
{byungrae.lee, kachang}@samsung.com

Contents Usage Method in DRM Interoperability Model

Byung-Rae Lee*, Kyung-Ah Chang
Samsung Electronics

요 약

다양한 DRM 클라이언트들간의 컨텐츠 공유를 제공하기 위해서는 우선 DRM 기술에 대한 호환성의 보장이 필수적으로 이루어져야 한다. 그러나 다양한 DRM 서비스 제공자들이 존재하고 여러 DRM 기술이 존재하는 현재와 같은 상황에 있어서 DRM 클라이언트 디바이스들간의 호환성은 기대하기 어렵다. 본 논문에서는 도메인과 같은 다수의 디바이스들이 집합에서 서로간의 호환성을 보장하기 위한 DRM 모델을 제시하고 DRM 클라이언트에서의 컨텐츠 재생을 위한 라이센스 전송 프로토콜을 제안한다.

1. 서론

본 논문에서는 현존하는 여러 DRM (Digital Rights Management) 기술[1, 2]들에서 다양한 디바이스간의 상호 호환성을 보장하기 위한 구조를 제시하고 컨텐츠를 재생하기 위한 프로토콜을 제안한다.

현재와 같이 여러 DRM 서비스 제공자들의 DRM 기술이 다른 경우에 있어서 다양한 디바이스들간의 DRM 호환성은 보장이 되지 않는다.

본 논문에서는 DRM 디바이스들간의 호환을 위하여 아래와 같은 2 가지 제안을 한다.

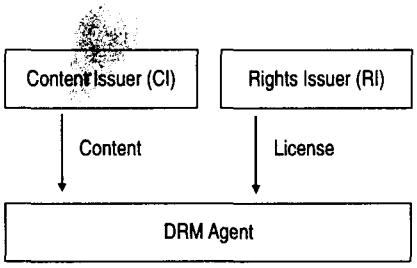
- DRM 호환에 있어서 핵심 요소인 컨텐츠(Content) 형식(Format)과 라이센스(License) 형식의 2 가지 요소를 제시하고 기본적인 구조를 나타내었다.
- DRM 클라이언트 디바이스와 DRM Proxy Server 간의 등록 프로토콜과 컨텐츠 재생을 위한 라이센스 전송 프로토콜을 제안하였다.

DRM 호환성에 있어서 가장 중요한 요소는 서로 다른 DRM 서비스 제공자들이 정의한 컨텐츠 형식(Content Format)과 라이센스 형식(License Format)을 DRM 클라이언트(Client) 디바이스(Device)들이 처리할 수 있는 단일 형식으로 변환을 해주는 것이다. 본 논문에서는 DRM Proxy Server 를 통하여 컨텐츠 및 라이센스 형식을 단일 형식으로 변환하여 DRM 클라이언트들간의 호환성을 보장해주는 구조와 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2 장에서는 일반적인 DRM 모델을 기술하고 3 장에서는 DRM 시스템간의 호환성을 위한 주요 요소를 제시한다. 4 장에서는 DRM 호환을 위한 기본 모델을 제시한다. 5 장에서는 DRM 클라이언트를 위한 등록 프로토콜을 제안한다. 6 장에서는 등록 프로토콜에 이어서 DRM 클라이언트 디바이스가 컨텐츠를 재생하는데 사용하는 라이센스 전송 프로토콜을 제안한다. 마지막으로 7 장에서는 결론을 제시한다.

2. DRM 시스템

일반적인 DRM 시스템은 다음과 같은 구조로 이루어진다.



<그림 1> 일반적 DRM 모델

각 참여자의 역할은 다음과 같다.

참여자	설명
CI	암호화된 컨텐츠를 DRM Agent 가 있는 디바이스에 제공
RI	암호화된 컨텐츠를 사용할 수 있는 라이센스를 DRM Agent 가 있는 디바이스에 제공
DRM Agent	CI 로부터 컨텐츠를 전송 받고 RI 로부터 라이센스를 전송 받아 컨텐츠를 재생

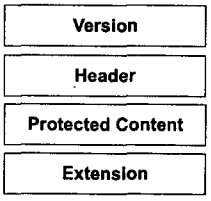
DRM Agent 가 있는 디바이스는 CI 로부터 컨텐츠를 얻을 수 있으며 RI 로부터 라이센스를 획득하여 컨텐츠를 재생할 수 있다.

3. DRM 시스템간의 호환성

본 장에서는 다양한 DRM 시스템간의 호환성을 이루기 위한 2 가지 요소를 제시한다.

2.1 컨텐츠 형식 (Content Format)

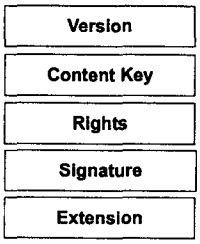
컨텐츠는 암호 기술에 의해서 보호를 받는다. 컨텐츠에 해당하는 라이센스가 없는 DRM Agent 는 컨텐츠를 재생할 수가 없다.



<그림 2> 컨텐츠 형식

2.2 라이센스 형식 (License Format)

라이센스에는 보호화된 컨텐츠를 재생할 수 있는 컨텐츠 키가 포함되어 있다.



<그림 3> 라이센스 형식

<그림 3>는 라이센스의 형식을 보여준다. 라이센스에는 컨텐츠 키와 권한의 두가지 중요한 요소가 있다.

- 컨텐츠 키(Content Key): 암호화된 컨텐츠를 복호화하는 역할을 한다. 컨텐츠를 사용할 수 있는 정당한 사용자 만이 컨텐츠 키를 통하여 재생할 수 있다.
- 권한(Rights): 컨텐츠를 사용하는 제약점으로서 사용자의 권리를 나타낸다.

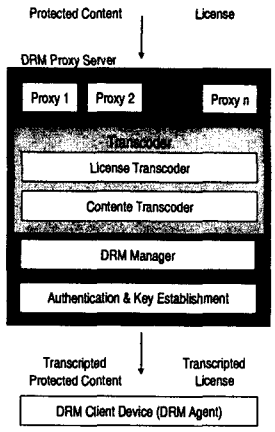
라이센스는 XML[3]로 인코딩 되어 진다. 대표적인 언어에는 ODRL (Open Digital Rights Language)[4], XrML (eXtensible Rights Markup Language)[5] 등이 있다.

라이센스는 라이센스를 발급한 RI 의 비밀키로 전자서명이 되어 질 수 있다. 이를 통하여 다음의 2 가지 사항이 확인 가능하다.

- 발급자인 RI 의 신원 파악
- 라이센스의 무결성 파악

4. DRM 호환 시스템 모델

본 논문에서는 서로 다른 형식을 갖춘 컨텐츠와 라이센스를 단일한 형식으로 변환해주는 DRM Proxy Server 에 기반한 호환 시스템 모델을 제시한다. <그림 4>는 DRM 형식 변환 모델을 보여준다.



<그림 4> DRM 형식 변환 모델

DRM 형식 변환을 통하여 DRM 클라이언트가 컨텐츠를 재생하는 과정은 다음과 같다.

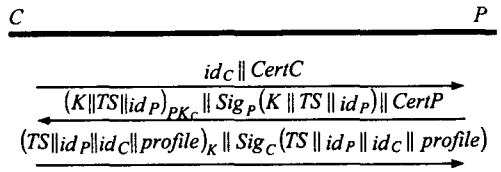
1. DRM 형식 변환 모델을 통하여 특정 DRM 보호된 컨텐츠와 라이센스 형식은 DRM Proxy Server 에 의하여 DRM 클라이언트에 적합한 단일 형식으로 변환되어 전달 된다.
2. DRM 클라이언트는 DRM Proxy Server 로부터 전달되어 온 변환된 형식의 컨텐츠와 라이센스를 수신한다.
3. DRM 클라이언트는 라이센스를 이용하여 컨텐츠를 재생할 수 있다.

DRM Proxy Server 에 의하여 변환된 단일 형식을 가지는 컨텐츠와 라이센스는 DRM 클라이언트에 전달되어 컨텐츠 재생이 될 수 있다.

5. DRM 클라이언트 등록 프로토콜

제안한 등록 프로토콜은 DRM 클라이언트 디바이스인 *C* 와 DRM Proxy Server, *P* 로 구성된다. 본 프로토콜에서 *P* 는 CI 를 통하여 DRM 보호된 컨텐츠를 받았으며 RI 를 통하여 컨텐츠에 해당하는 라이센스를 수신하였다고 가정한다. 공개키 암호 알고리즘으로는 RSA[6] 등이 사

용될 수 있다.



<그림 5> DRM 클라이언트 등록 프로토콜

등록을 원하는 C 는 자신의 신원 idC 와 $CertC$ P 에게 전송을 한다.

P 은 C 로 부터 전송 받은 $CertC$ 를 이용하여 C 의 공개키 PK_C 를 획득하고 이를 이용하여 생성한 세션 키 K, 시간 정보 TS, 자신의 신원 id_P 를 암호화 한 정보와 비밀키로 서명한 정보를 자신의 인증서, $CertP$,와 같이 전송한다.

C 는 자신의 비밀키를 이용하여 P 가 전송한 암호화된 세션 키, K 를 복호화하고 시간 정보 TS 를 확인하여 메시지가 최근에 온 것 인지 확인한다.

C 는 마지막으로 자신과 P 의 신원 정보, id_C , id_P , P 로부터 받은 시간 정보 TS 를 세션 키, K 로 암호화한 것과 비밀키로 전자 서명한 것을 P 에게 전송한다.

마지막 메시지에서 C 는 P 에게 자신의 디바이스 특성, *profile* ,을 P 에게 같이 전송한다. P 가 고려해야 할 디바이스의 특성에서 *profile* 이 가지고 있어야 하는 정보는 아래와 같다.

- 디바이스 모델
- 프로세싱 능력 (CPU 성능, 메모리 사이즈)
- 화면 크기
- 저장 장치의 크기

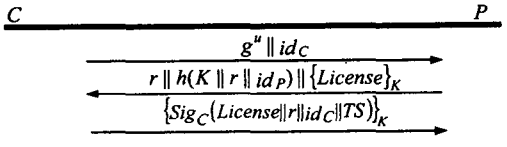
P 는 DRM 클라이언트의 특성에 기준하여 적합한 컨텐츠를 전송한다.

6. 라이센스 전송 프로토콜

6.1 라이센스 전송

컨텐츠에 대한 재생을 원하는 DRM 클라이언트 C ,는 DRM Proxy Server P ,에게 컨텐츠 재생 요청을 한다. 요청을 받은 P 는 C 에게 컨텐츠 재생을 할 수 있게 하는 라이센스, *License* 를 전송한다.

아래의 프로토콜에서 C 와 P 는 Diffie-Hellman[7] 방식에 의하여 공유되는 세션키 K 를 생성한다.



<그림 6> 라이센스 전송 프로토콜

프로토콜(<그림 6>)이 시작되면 C 는 세션키 설정을 위한 공개키 g^u 와 신원 id_C 을 P 에게 보낸다.

P 는 난수 r 을 생성하여 세션키 $K = h(g^{vu} \| r)$ 를 생성하고, r 과 P 의 신원 id_P, 난수 r 을 해쉬 함수 h 로 처리하여 생성한 세션키 K 로 암호화한 라이센스와 같이 C 에게 전송한다.

C 는 마지막으로 수신한 라이센스, *License* 와 난수, r, 자신의 신원, id_C 을 타임스탬프, TS 와 같이 전자서명을 하여 P 에게 전송한다.

6.2 컨텐츠 전송

DRM 암호화된 컨텐츠는 DRM 클라이언트의 저장 장치에 있거나 다른 디바이스 또는 DRM Proxy Server 로부터 전송 받을 수 있다. 컨텐츠는 암호화되어 있으므로 자유롭게 이동이 가능하다.

7. 결론 및 향후 연구 과제

본 논문에서는 DRM 클라이언트 디바이스들간의 호환성을 보장하기 위한 필요 요소를 파악하였다. DRM 서버에서 전송해주는 DRM 컨텐츠와 라이센스를 DRM 클라이언트 디바이스들에게 호환 가능한 형식으로 DRM Proxy Server 가 변환을 해주는 역할을 한다. DRM 클라이언트 디바이스는 DRM Proxy Server 와의 인증을 통하여 컨텐츠를 재생할 수 있는 라이센스를 획득할 수 있게 된다.

향후 연구 과제로 여러 DRM 클라이언트 디바이스들은 그룹을 이루어서 컨텐츠 공유를 진행하는 방법에 대한 연구가 필요하다. 동일한 컨텐츠 키를 공유하기 위해서는 DRM Proxy Server 가 키를 선정하여 멀티캐스트와 같은 방식으로 전송하는 방법이 있으며 또는 그룹 키 설정 (Group Key Agreement)[8] 방식으로 키를 생성할 수 있는 방법이 있다.

참고문헌

[1] OMA DRM WG, http://www.openmobilealliance.org
[2] Microsoft DRM, http://www.microsoft.com/windows/windowsmedia/drm.aspx
[3] XML (eXtensible Markup Language), http://www.w3c.org
[4] ODRL (Open Digital Rights Language), http://odrl.net
[5] XrML (eXtensible rights Markup Language), http://www.xrml.org
[6] R. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," CACM, Feb. 1978.
[7] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol.22, pp.644-654, Nov. 1976.
[8] M. Steiner, G. Tsudik, and M. Waidner, Diffie-Hellman Key Distribution Extended to Group," Third ACM Conf. Computer and Comm. Security, pp.31-37, Mar. 1996.