Domain DRM 시스템을 위한 License 공유 기술†

최동현, 최윤성, 이윤호, 이영교, 김승주, 원동호*

성균관대학교 정보통신공학부 정보보호연구소

A License Sharing Scheme for Domain DRM System†

Donghyun Choi, Younsung Choi, Yunho Lee, Younggyo Lee, Seungjoo Kim and Dongho Won*

Information Security Group, School of Information and Communication Engineering, SungKyunKwan University

요 약

디지털 기술의 발전으로 인해 원본과 동일한 품질을 가지는 디지털 콘텐츠의 무한한 복제가 가능할 뿐만 아니라 인터넷을 통해 전 세계 어디라도 전파될 수 있다. 이러한 디지털 콘텐츠의 불법복제에 따른 문제를 해결해 줄 수 있는 것이 바로 DRM(Digital Rights Management)이다. 하지만 현재의 DRM은 콘텐츠를 구매하여 License를 받은 최초의 디바이스에서만 사용이 가능하도록 설계 되어 있다. 이러한 방식은 콘텐츠를 구매한 사용자의 권리를 제한하는 것이다. 본 논문에서는 Home Network와 같은 특정 Domain영역 안에서만 콘텐츠의 사용이 가능한 DRM 시스템을 제안한다.

I. 서론

컴퓨터 기술의 발전으로 인해 우리는 고품질의 디지털 콘텐츠를 제작할 수 있게 되었다. 또한 인터넷의 확산과 통신 기술의 발전은 컴퓨터간의 상호연결성을 증대시켰다. 이러한 기술의 발전은 디지털 음악, 화상, 영상물, 출판물 등 멀티미디어 데이터에 대한 수요를 증대 시켰다. 하지만 디지털 기술의 발전은 원본과 동일한 품질을 가지는 디지털 콘텐츠의 무한한 복제가 가능할 뿐만 아니라 인터넷에 연결되어 있는 어디에서든지 불법으로 복제된 콘텐츠를 구할 수 있게 되었다. 이러한 문제는 디지털 콘텐츠시장의 성장을 가로막고 있다. 이러한 디지털 콘텐츠의 불법 복제 문제를 해결해 줄 수 있는 것이 바로 DRM 시스템이다[1][2][5].

현재의 저작권 보호 기술은 콘텐츠 판매자로부터 사용자가 디지털 콘텐츠를 구매, 그에 해당 되는 License를 License Server로부터 얻는다[8]. 사용자는 License를 받은 최초의 컴퓨터에서만 콘텐츠의 사용이 가능하도록 설계 되어 있다. 이 경우, 사용자는 자신이 구매한 콘텐츠를 자신이 소유하고 있는 다른 다비이스에서 사용을 할 수 없으며 이는 License를 구매한 사용자의 권리를 제한하는 것이다. 이러한 사용자의 권리 제한의 문제를 해결하기 위한 방법이 도메인 DRM을 이용하는 것이다[3][6][7].

본 논문에서는 디지털 콘텐츠를 사용자가 속한 특정 Domain 안에서 자유롭게 사용이 가능하도록 하는 License 공유 기술을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 대표적인 DRM시스템에 대해 설명하고, 3장에서는 제안하는 DRM 시스템에 대하여 기술하고, 기존의 DRM 시스템과 비교한다. 마지막으로 5

* 교신저자 : 원동호(dhwon@security.re.kr)

† 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터(ITRC) 육성·지원사업의 연구결과로 수행되었음.

장에서 결론을 맺는다.

II. 관련 연구

2.1 InterTrust의 DRM 시스템

InterTrust의 DRM은 저작물 보호를 위해 암호기술과 워터마킹 기술을 사용하며 저작물 사용규칙을 지정하여 사용내역의 수집 및 기록, 과금 처리를 수행하는 것이다. 저작물은 사전에 암호화 된 후 배포되므로 사용자의 컴퓨터에서 저작물을 사용하는 시점에서 License 에이전트가 License를 확인하고 지불정보를 전송하여 거래를 채결하도록 하였다. 또한 저작물이 암호화되어 보호되고 있으므로 사용자들 사이에 암호화된 저작물을 주고받을 수 있는 저작물 재분배(Super Distribution)를 실현하였다. 하지만 이 시스템은 License를 받은 사용자의 다른 장치에서는 플레이 할 수 없는 단점을 가지고 있다[9][10].

2.2 Microsoft의 DRM 시스템

Microsoft의 DRM시스템은 저작물 제공자에게 인터넷상에서 암호화를 통해 보호된 음악, 비디오 등 미디어를 배달한다. 각각의 서버 또는 클라이언트 인스턴트들은 개인화 과정을 통해 키 쌍을 할당받게 되며 크래킹 되었거나 안전하지 않다고 판단되는 인스턴스에 대해서는 인증서 취소목록을 이용하여 서비스 대상에서 제외시킨다. 인증서 취소목록은 Microsoft사의 웹사이트를 통해 배포된다. 키는 License에 포함되고 License와 저작물은 분리되어 분배된다. 하지만 이 시스템 역시 License를 받은 사용자 소유의 다른 장치에서 플레이 할 수 없는 단점을 가지고 있다[4][9][11].

III. 제안하는 DRM 시스템

3.1 용어

- $E_K(A)$: A를 키 K로 암호화
- $D_K(A)$: A를 키 K로 복호화
- P : 공개키
- S : 비밀키
- K_C : Content Encryption Key
- DC : DRM Client
- DM : Domain Manager

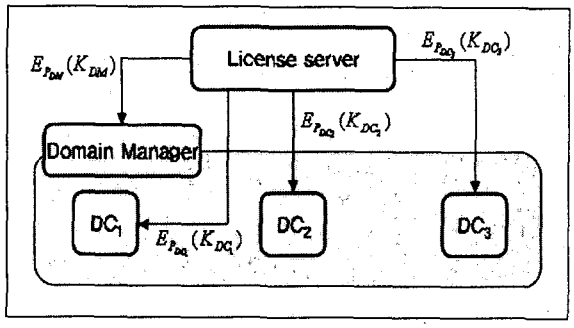
3.2 프로토콜

Step 1 : 디바이스 등록

License Server는 Domain Manager와 해당 Domain 속하는 Client에 키를 각각 할당한다. **<그림 1>**에서 처럼 키는 수신자의 공개키로 암호화 되어 License에 포함되어 전송된다.

License Server $\xrightarrow{E_{P_{DM}}(K_{DM})}$ Domain Manager

License Server $\xrightarrow{E_{P_{DC_i}}(K_{DC_i})}$ DC_i



<그림 1> 디바이스 등록 단계

Step 2 : 콘텐츠 사용

Client가 디지털 콘텐츠를 구매하면 해당 콘텐츠를 암호화한 키인 K_C를 License Server가 콘텐츠 Packager로부터 받게 되고, License Server는 이를 콘텐츠 구매자에게 전송한다. 제안하는 시스템에서 License Server는 K_C를 도메인 초기 등록과정에서 할당된 구매자의 키로 암호화한 후 암호화된 값을 다시 한 번 Domain Manager에게 할당한 키로 암호화 한다. 이때 사용하는 암호방식은 가환암호(Commutative encryption) 방식을 사용한다. 가환암호는 암호화 순서에 상관없이 복호화 할 수 있는 방식을 말한다.

License Server : $E_{DM}(E_{DC_2}(K_C))$

이렇게 생성된 값을 License Server는 콘텐츠의 구매자에게 전송한다.

$$\text{License Server} \xrightarrow{E_{DM}(E_{DC_2}(K_C))} DC_2$$

<그림 2> 에서처럼 콘텐츠 구매자 DC_2는 License Server로부터 받은 정보를 Domain Manager에게 전송한다. Domain Manager는 받은 정보를 자신이 License Server로부터 받은 키로 복호화 한다.

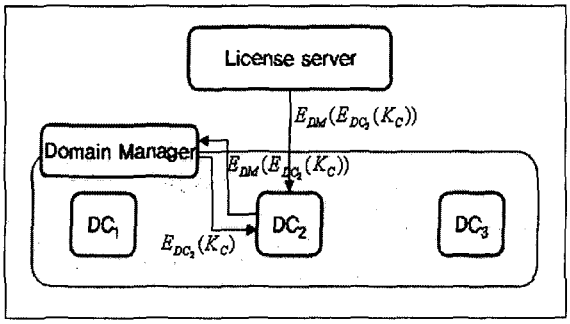
$$DC_2 \xrightarrow{E_{DM}(E_{DC_2}(K_C))} DM$$

$$DM : D_{DM}(E_{DM}(E_{DC_2}(K_C))) = E_{DC_2}(K_C)$$

이렇게 생성된 정보는 다시 DC_2에게 전송한다. DC_2는 초기 등록과정에서 License Server로부터 할당 받은 key로 복호화 하여 K_C를 얻고 콘텐츠를 사용한다.

$$DM \xrightarrow{E_{DC_2}(K_C)} DC_2$$

$$DC_2 : D_{DC_2}(E_{DC_2}(K_C)) = K_C$$



<그림 2> DC_2의 콘텐츠 사용 흐름

3.3 License 공유

같은 도메인 내에서 License를 공유 하기위해서 DC_2는 License Server로부터 받았던 License를 자신의 키로 복호화 한다.

$$DC_2 : D_{DC_2}(E_{DM}(E_{DC_2}(K_C))) = E_{DM}(K_C)$$

복호화된 값은 DC_3에게 전송한다.

$$DC_2 \xrightarrow{E_{DM}(K_C)} DC_3$$

해당 정보를 받은 DC_3은 이 정보를 다시 자신의 키로 암호화하여 Domain Manager에게 전송한다.

$$DC_3 : E_{DC_3}(E_{DM}(K_C))$$

$$DC_3 \xrightarrow{E_{DC_3}(E_{DM}(K_C))} DM$$

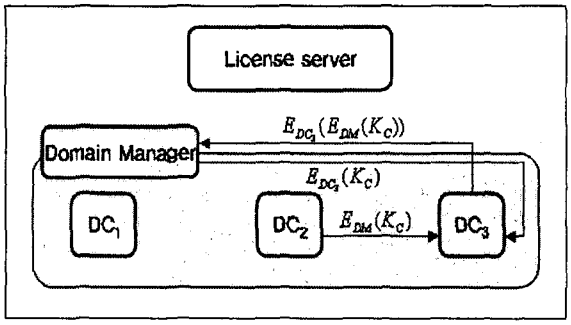
Domain Manager는 자신의 키로 복호화 하여 다시 DC_3에게 전송한다.

$$DM : D_{DM}(E_{DC_3}(E_{DM}(K_C))) = E_{DC_3}(K_C)$$

이를 수신한 DC_3은 초기 등록과정에서 License Server로부터 할당 받은 key로 정보를 복호화 하여 K_C를 얻고 콘텐츠를 재생한다.

$$DM \xrightarrow{E_{DC_3}(K_C)} DC_3$$

$$DC_3 : D_{DC_3}(E_{DC_3}(K_C)) = K_C$$



<그림 3> DC_2 와 DC_3의 License 공유

DC_1의 경우 위에서 진행한 동일한 방법을 반복하여 License를 공유 할 수 있다. 또한 패키징된 콘텐츠는 Super Distribution에 의해서 디바이스가 쉽게 얻을 수 있다.

3.4 다른 DRM 시스템과의 비교

[표1]에서 보여지는 바와 같이 제안하는 DRM 시스템은 기존의 DRM 시스템과 동일한 기능을 수행함과 동시에 License를 구매한 사용자가 자신이 속한 도메인 영역 내의 다른 디바이스에서도 사용이 가능하다. 만일 사용자의 디바이스가 도메인 영역을 벗어난다면 Domain Manager로부터 복호 화된 키를 받을 수 없기 때문에 콘텐츠의 재생이 불가능해 진다.

[표 1] 제안하는 방식과 기존 DRM기술의 비교

	License	저작물 재분배	도메인 영역에서 콘텐츠 공유
제안하는 방식	콘텐츠와 분리	가능	가능
InterTrust	콘텐츠와 분리	가능	불가능
Microsoft DRM	콘텐츠와 분리	가능	불가능

IV. 결론

디지털 콘텐츠는 품질의 손실 없이 원본과 동일한 콘텐츠를 무한이 복제가 가능할 뿐만 아니라 인터넷을 통해 전 세계 어디라도 빠른 시간 안에 전송될 수 있다. 디지털 콘텐츠가 가지는 이러한 특성 때문에 콘텐츠의 불법 복제가 빈번히 발생하고 있다. 이러한 불법복제를 막기 위해 DRM 기술은 연구 되어오고 있다.

본 논문에서 제안한 DRM 시스템은 디지털 콘텐츠 사용에 있어서 일반 사용자들이 한번 구매한 License를 최초 장치가 아닌 다른 장치에서도 사용 가능하도록 설계 하였다. License를 구매한 사용자는 등록된 도메인 내에서 구매한 콘텐츠를 자유롭게 사용할 수 있다.

향후 과제는 이러한 License를 다른 사용자와 거래 하거나 혹은 상속시켜줄 수 있는 DRM 시스템 설계에 관한 연구가 필요하다.

[참고문헌]

[1] Q.Liu, R. Safavi-Naini, and N. P. Sheppard, "Digital rights management for content distribution", proceedings of the Australasian information security workshop conference on ACSW frontiers 2003, Vol.21 Jan,. 2003

[2] ISO/IEC JTC 1/SC 29/WG 11 MPEG/N5235 Draft Requirements for MPEG-21, Intellectual Property Management and Protection. 2002

[3] B. Popescu, B. Crispo, A. Tanenbaum, F. Kamperman, "Systems and architectures: A DRM security architecture for home networks," Proceedings of the 4th ACM workshop on Digital rights management, October 2004.

[4] Andrea Pruneda, Microsoft Digital Media Division, " Security Overview of Microsoft Windows Media Rights Manager", October 2001

[5] S. Michiels, K. Verslype, W. Joosen, B. De Decker. Towards a Software Architecture for DRM. In Proceedings of the Fifth ACM Workshop on Digital Rights Management (DRM'05), pp. 65-74. Alexandria, Virginia, USA (co-located with CCS 2005). November, 2005.

[6] 강호갑, "DRM 최신 국제표준 기술사양 분석 및 세계 유명제품 동향과 전망에 관한 연구", 2004

[7] 주학수, "디지털 저작권 관리 시스템(DRM)의 개발현황", 정보보호학회지, 2003.4

[8] Yu Zheng, Dake He, Hongxia Wang, Xiaohu Tang, Secure DRM scheme for future mobile networks based on trusted mobile platform, Wireless Communications, Networking and Mobile Computing, 2005. Proceedings. 2005 International Conference on, Publication Date: 23-26 Sept. 2005, Volume: 2, On page(s): 1164- 1167

[9] Susanne Guth, "A Sample DRM System." Digital Rights Management 2003: 150-161

[10] http://www.intertrust.com/, InterTrust

[11] http://www.Microdoft.com/, Microsoft