DRM 시스템에서 사용자 중심의 콘텐츠 사용을 위한 라이센스 모델에 관한 연구

왕보현, 류종화, 이병욱
경원대학교 전자계산학과
bhwang99@hanmail.net

A Strudy of License Method for User-oriented Use of Contents in DRM system

Bo-Hyun Wang, Zong-Hua Liu, Byung-Wook Lee
Dept of Computer Science, Kyungwon University

요 약

기존 DRM 시스템들은 콘텐츠 저작권자의 저작권을 배타적으로 보호한다. 이에 사용자들이 DRM 으로 보호된 콘텐츠를 사용할 때는 다소 제약이 가해진다. 최근 사용자 중심의 콘텐츠 사용 요구가 확산되고 있고 이에 대한 연구가 활발히 진행되고 있다. 본 논문에서는 사용자들의 콘텐츠 사용 유형을 분류하고 그에 따른 라이센스 모델을 제안한다. 제안된 라이센스 모델에서는 사용자 식별 정보를 이용하여 허가된 사용자만이 융통적인 콘텐츠 사용을 가능하게 한다. 이러한 라이센스 모델을 통해 DRM 시스템의 저작권 보호의 기본 원칙을 제공하며 사용자에게는 융통성 있는 콘텐츠 사용을 가능하게 한다.

1. 서 론

디지털 콘텐츠는 복제가 용이하고 복제된 콘텐츠의 질이 원본 콘텐츠와 거의 유사하다는 특징으로 인해 많은 불법복제가 이루어지고 있다. 이로 인해 콘텐츠 저작권자의 저작권이 침해되고 유통업자에게도 많은 손실을 가져왔다. 디지털 콘텐츠의 불법유통과 복제를 방지하고 지정된 소비자에게 주어진 범위 내에서 콘텐츠를 사용케 하여 디지털 콘텐츠 저작권이 보호되고 배포자의 이익 실현을 가능하게 하는 기술이 DRM 기술이다.

그러나 DRM 기술은 저작자의 저작권을 배타적으로 보호함으로써 콘텐츠 사용자에게는 다소 제약적이다. 이는 라이센싱 기법이 저작권자에 촛점을 맞추었기 때문이다. 현재 폭넓게 사용중인 MS사의 WMRM이나 표준으로써 넓기 채택되고 있는 OMA DRM의 라이센스 기법을 살펴보면 콘텐츠는 사용자가 다른 사용자에게 배포가 가능하지만 콘텐츠를 사용하기 위해서는 반드시 콘텐츠를 배포 받은 사람이 라이센스를 요청하고 발급받아야만 한다. 이는 라이센스 관리의 모든 기능을 라이센스 발급자가 가지고 있고 라이센스 요청자의 범위를 콘텐츠를 사용할 사람으로 국한시킴으로써 콘텐츠의 융통성 있는 사용을 어렵게 한다.

본 논문에서는 사용자들의 콘텐츠 사용 유형을 분류하고 그에 따른 라이센스 모델을 제안한다. 콘텐츠 사용의 유형은 크게 세 가지로 분류할 수 있으며 다음과 같다. 그룹에서의 콘텐츠 사용, 그룹이 아닌 사용자들 간의 재배포, 임의의 사용자가 소유한 디바이스들에서의 콘텐츠 사용이다. 이러한 콘텐츠 사용을 가능하게 하기 위한 제안된 라이센스 모델은 사용자 식별 정보를 이용하여 허가된 사용자를 인증한다. 사용자 식별 정보는 디바이스 정보를 사용함

으로써 허가된 디바이들에서 허가된 사용자가 콘텐츠를 자유롭게 실행시킬 수 있도록 한다. 또한 디바이스 정보를 콘텐츠 암호화 키를 보호하는데도 사용한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 기술하고 3장에서는 콘텐츠 사용 유형을 분류하고 4장에서는 라이센스 모델에 대해 제안하고 5장에서 결론을 맺는다.

2. 관련 연구

본 절에서는 기존 DRM 시스템에서의 라이센스 모델을 기술하고, 사용자 중심의 콘텐츠 이용이 정당하다는 것을 보여주는 법적 제도인 fair use doctrine에 대해 기술한다. 또, 사용자 식별 정보에 대한 내용을 기술한다.

2.1 기존 DRM 시스템

대표적인 DRM 시스템인 MS사의 WMRM과 OMA DRM에서의 라이센스 모델에 대해 기술한다. MS사의 WMRM에서는 콘텐츠 사용의 한 유형인 재배포를 소매자(retailer)라는 개념을 이용하여 지원한다. 소매자는 배포자로부터 패키지된 콘텐츠를 받는다. 소비자 A가 소매자로부터 콘텐츠를 구매하고 소비자 B에게 재배포한다. 소비자 B가 콘텐츠를 실행하기 위해서는 클리어링 하우스로부터 라이센스를 요청하고 발급받아야 한다[5].

OMA DRM은 소비자가 자신의 단말에서 다른 소비자의 단말로 여러 채널을 통해 DRM 콘텐츠를 전송하는 것을 허용한다. DRM 콘텐츠를 전달받은 소비자는 DRM 콘텐츠 헤더에 명시되어 있는 사용권 발행자를 통해 별도의 사용권을 취득하도록 하는 방식이다. 이 방식은 콘텐츠의 이동 및 복사는 허용하되 사용 시점에서 사용권을 획득하여야만 콘텐츠의 이용이 가능하다. 위 가지 DRM 시스템에서는 모두 콘텐츠를 전달받은 사용자가 반드시 라이센스를 요청하고 발급받는다. 이러한 모델에서는 콘텐츠를 배포하는 사람의 다양한 콘텐츠 이용 유형을 지원하지 못한다[3].

2.2 Fair Use Doctrine

Fair use는 보호된 콘텐츠를 사용하는 개인들에 대한 권익 보호를 위해 존재하는 미국 저작권 법에서의 doctrine이다. Fair use doctrine하에서 방송, 교육, 비평, 평론, 새로운 보고서를 제외하고 연구나 교육과 같은 목적으로 콘텐츠를 사용하는 것은 저작권의 위배가 아니다. Fair use는 소비자가 구매한 콘텐츠를 재 판매하고 개인적인 용도로 백업하는 것을 허용한다.

Fair use doctrine과 DRM의 개념은 상반되지만 소비자 권익을 보호하고 사용자 중심의 콘텐츠 이용 측면에서 DRM 시스템은 fair use doctrine의 기본 방침을 지원하면서 안전하게 콘텐츠를 배포할 수 있는 기술적 지원이 필요하다[7].

2.3 식별자

디지털 콘텐츠 이용에 있어서 인증은 중요한 기술이다. 인증에는 사용자 인증과 디바이스 인증이 있다. 디바이스 인증은 주로 콘텐츠가 실행될 디바이스를 제한하고자 하는 것에 초점을 두고 있다.
사용자 인증을 위한 식별정보로는 ID/PASSWORD, 인증서의 공개 키, 이메일 주소 정보 등을 사용할 수 있다. 디바이스 인증을 위한 식별정보로는 SN(Serial Number), MN(Model Number) 그리고 MAC 주소등이 있다. SN은 주로 콘텐츠를 특정 디바이스에서만 사용하도록 규정할 때 사용된다[1]. MN(Model Number)는 디바이스와 디바이스에 설치된 소프트웨어의 버전을 식별할 때 사용된다. MAC(Media Access Control) 주소값은 모바일 기기 및 데스크 탑에서 사용할 수 있는 네트웍 카드의 48비트 하드웨어 주소를 말하며 모든 네트워크 카드가 유일한 값을 갖는다. 그러므로 네트워크가 가능한 모든 기기는 이 주소로써 식별가능하다.

3. 콘텐츠 이용 유형

현재 콘텐츠를 인터넷 상에서 구매하여 사용하는 경우 사용자들은 라이센스를 발급받은 후 콘텐츠를 실행할 수 있다. 또, 콘텐츠를 실행 가능한 기기는 라이센스를 발급받은 기기로 한정되어 있다. 이러한 경우는 사용자가 콘텐츠를 가족이나 이해관계가 있는 임의의 그룹에게 공유나 선물의 목적으로 콘텐츠를 배포 하더라도 콘텐츠를 전달받는 사람은 반드시 라이센스를 요청하고 다시 발급받아야 한다.

콘텐츠를 사용하기를 요구하는 유형과 필요한 기능을 기술하면 다음과 같다.

- 원하는 디바이스들에서 콘텐츠를 자유롭게 실행하기를 원한다. : 콘텐츠가 실행될 디바이스에 대한 제한을 완화하고 실행할 수 있는 디바이스들을 라이센스로 관리할 수 있어야 한다.

• 자신의 콘텐츠와 실행 권리 일부를 타인에게 양도하고 싶다. : 배포 받는 사람의 라이센스를 요청할 수 있어야 하며 권리 양도 내용을 배포 받는 사람과 배포 하는 사람의 라이센스에 모두 반영하여야 한다. 또한 콘텐츠의 투명한 배포를 위하여 배포를 추적할 수 있는 기능이 필요하다.

• 교육 목적으로 임의의 그룹내에서 콘텐츠를 공유하기를 원한다.

4. 라이센스 모델

그림 1은 3절에서의 사용자 중심의 콘텐츠 사용 유형을 안전하게 지원하기 위한 라이센스 모델이다. 그림 1에서 배포자는 콘텐츠 서비스를 제공하는 시스템이며 라이센스 서버는 라이센스를 발급한다. 그림 1의 라이센스 모델에서 사용자 식별자로써 사용되는 하드웨어 식별자는 MAC 주소를 이용하고 HID로 나타낸다. 소비자 i는 배포자로부터 콘텐츠를 구매하고 소비자 i+1은 소비자 i로부터 콘텐츠를 배포 받고 소비자 i+2는 소비자 i+1로부터 콘텐츠를 배포 받는다.

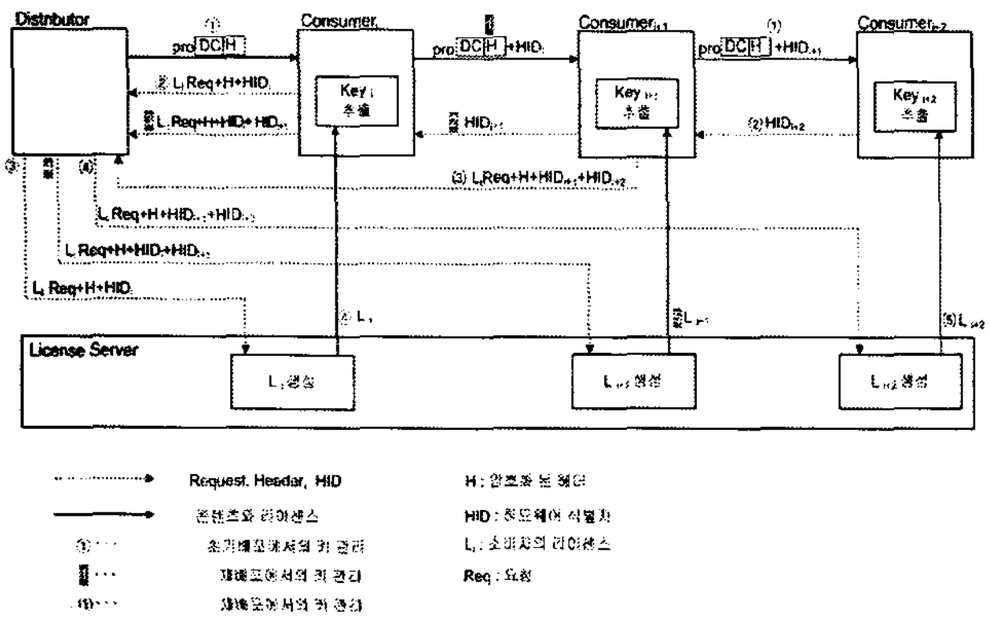

그림 1. 라이센스 모델

①부터 ④까지는 소비자 i가 콘텐츠를 구매했을 때 라이센스가 발급되는 과정을 나타낸다. ① 소비자 i가 콘텐츠를 구매하면 배포자는 암호화된 콘텐츠와 헤더를 소비자 i에게 전송한다. ② 소비자 i는 라이센스 요청과 함께 헤더 정보와 자신의 HID를 배포자에게 전송한다. ③ 배포자는 이들 정보를 라이센스 서버에게 전송하고 ④ 라이센스 서버는 수신된 정보를 이용하여 라이센스를 발급하여 소비자 i에게 전송한다. 라이센스에 포함된 키의 생성과 HID를 이용한 관리 기법은 다음 절에서 기술한다.

1부터 5까지는 소비자 i가 소비자 i+1에게 콘텐츠를 재배포했을 때 라이센스 발급과정을 나타낸다. 1 소비자 i는 소비자 i+1에게 암호화된 콘텐츠와 헤더 그리고 자신의 HID를 전송한다. 2 소비자 i+1은 소비자 i에게 자신의 HID를 전송한다. 3 소비자 i는 소비자 i+1에 대한 라이센스 요청과 함께 헤더와 자신과 소비자 i+1의 HID를 배포자에게 전송한다. 4 배포자는 이들 정보를 라이센스 서버에게 전송하면서 라이센스를 요청한다. 5 라이센스 서버는 라이센스를 생성하여 소비자 i+1에게 전송한다.

(1)부터 (5)까지는 소비자 i+1이 소비자 i+2에게 콘텐츠를 재배포했을 때 라이센스 발급 과정을 나타낸다. (1) 소비자 i+1은 소비자 i+2에게 암호화된 콘텐츠와 헤더 그리고 자신의 HID를 전송한다. (2) 소비자 i+2는 소비자 i+1에게 자신의 HID를 전송한다. (3) 소비자 i+1은 라이센스 요청과 함께 헤더와 자신과 소비자 i+2의 HID를 배포자에게 전송한다. (4) 배포자는 이들정보를 라이센스 서버에게 전송하면서 라이센스를 요청한다. (5) 라이센스 서버는 라이센스를 생성하여 소비자 i+2에게 전송한다. 그림 1의 라이센스 모델은 콘텐츠를 배포한 사람이 배포 받은 사람의 라이센스를 요청할 수 있음으로써 콘텐츠 사용의 융통성을 제공한다. 또한 배포 하는 사용자는 배포자에게 배포 받는 사용자 정보를 전송하며 자신이 양도하기를 원하는 권리 정보도 함께 전송한다.

4.1 HID를 이용한 Key 저장 형태

그림 2는 그림 1의 라이센스 서버에서 라이센스를 생성할 때 키를 어떤 형태로 저장하는 가를 나타내는 그림이다.

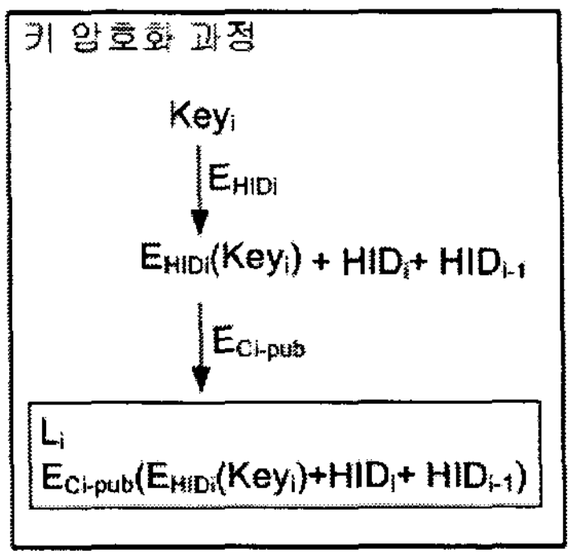

그림 2. 라이센스에 키 저장

제안된 라이센스 모델에서 라이센스에 키 가 저장될 때 키는 HID로 암호화 되고 암호화 된 키에 콘텐츠를 배포한 사용자와 자신의 HID가 연결되어 사용자의 공개 키로 암호화 된다.

4.2 Key 추출 과정

그림 3은 사용자가 라이센스를 발급 받고 라이센스로부터 키를 추출하여 복호화 하는 과정을 나타내는 그림이다.

라이센스로부터 사용자의 공개 키로 암호화 된 키와 배포한 사람과 배포 받은 사람의 HID를 소비자의 개인 키로 복호화 한다. 두 HID를 사용자의 디바이스에 포함된 두 HID와 비교한다. 콘텐츠를 배포한 사용자의 HID_{i-1}과 배포 받은 소비자의 HID_i가 일치하면 HID_i으로 암호화 된 키를 복호화 시킨다.

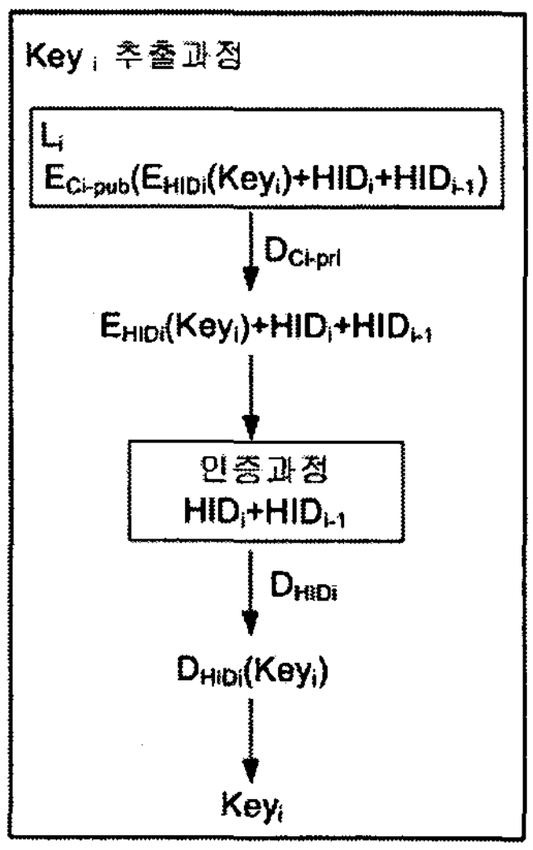

그림 3. 키 추출 과정

키를 추출하여 복호화 하는 과정에서 두 HID의 비교는 다음과 같은 의미를 나타낸다.

첫째, 콘텐츠를 배포한 사용자와 배포받은 사용자가 허가된 사용자임을 확인할 수 있다. 라이센스에 포함된 HID_{i-1}와 HID_i이 사용자 i에 있는 HID_{i-1}와 HID_i과 일치한다는 것은 사용자 i가 받은 콘텐츠가 정당한 사용자 i-1로부터 전달되었으며 콘텐츠가 정당한 사용자 i에게 수신되었다는 것을 의미한다.

둘째, HID들의 확인 과정 후 자신의 HID로 암호화된 비밀키를 복호화 함으로써 허가되지 않은 사용자에게 키가 유출되는 것을 막고 허가된 디바이스에서만 콘텐츠가 실행될 수 있도록 한다.

5. 결론

본 논문은 사용자 중심의 콘텐츠 사용의 유형을 나누었고 그러한 유형에서 안전하게 콘텐츠가 배포될 수 있는 라이센스 모델을 제안하였다. 제안된 라이센스 모델에서는 콘텐츠를 배포한 사용자와 배포 받은 사용자의 디바이스 식별자를 이용하여 배포한 사람과 배포 받은 사람이 허가된 사용자임을 인증한다. 또한 자신의 디바이스 식별자로 콘텐츠 암호화 키를 암호화 함으로써 허가된 사용자의 허가된 디바이스 에서만 콘텐츠가 실행되도록 하였다.

참고문헌

[1] Thomas S. Messerges, Ezzat A. Dabbish. "Digital Rights Management in a 3G Mobile Phone and Beyon", ACM Workshop DRM '03 October 27, 2004

[2] Sam Michiels, Kristof Verslype, Wouter Joosen and Bart De Decker. "Towards a Software Architecture for DRM", ACM Workshop DRM '05 November 7, 2005.

[3] Open Mobile Alliance, "DRM Architecture", OMA-DRM-ARCH-V2_0-20 040820-C, Draft Version 2.0-20 August 2004, http://www.openmobilealliance.org

[4] Bogdan C. Popescu, Bruno Crispo, Andrew S. Tanenbaum. "A DRM Security Architecture for Home Networks", ACM Workshop DRM '04 October 25, 2004

[5] Windows Media Rights Management, http://www.microsoft.com/windows/windowsmedia/

[6] 장혜진, "DRM 기술로 보호된 콘텐츠의 융통성 있는 공유를 위한 멤버/그룹 라이선스 메커니즘", 『한국정보처리학회 논문지 C』 VOL. 11-C No. 06 2004.12 pp.739~746

[7] Title 17-Copyrights, Chapter 1-Subject Matter And Scope of Copyright, Sec.107-US Code Collection. Legal Information Institute. http://www4.law.cornell.edu/uscode/107.html