라이선스 보호를 위한 유,무선 디바이스와 Agent 기반의 DRM 시스템 설계

추연수*, 김정재**, 전문석***
*숭실대학교 컴퓨터학과
e-mail:lets-priase@hanmail.net

Design DRM System based on Wired, Wireless Device and Agnet for License Protection

Yeounl-Soo Choo*, Jung-Jae Kim**, Moon-Seog Jun***
Dept of Computer Science, Soong-sil University

요 약

최근 인터넷 사용의 증가로 디지털 컨텐츠의 사용과 유통이 보다 쉬워짐으로 인해 디지털 컨텐츠가 불법 복제와 불법 유통이 행해지고 있으며 이것은 컨텐츠 제작자들의 권리를 침해하고 있다. 이를 방지하고자 DRM(Digital Rights Management)시스템의 연구가 활발히 진행되고 있다. DRM 시스템은 정당한 사용자가 정당한 지불을 치루고 라이선스를 구입한 후 컨텐츠를 사용할 수 있게 하는 시스템으로 사용자 인증과 컨텐츠 보호를 위한 암호화, 복호화와 이를 위한 키 분배가 관건이다. 본 논문에서는 사용자 인증과 더불어 불법적인 사용자로부터 라이선스를 보호하기 위한 DRM 시스템을 제안하고자 한다.

1. 서론

최근 인터넷 사용의 증가로 디지털 컨텐츠의 사용과 유통이 용이해졌다. 또한 디지털 컨텐츠는 복제를 하여도 그 질이 떨어지지 않는다는 특성이 있다. 이러한 디지털 컨텐츠의 특성과 인터넷의 이점을 이용하여서 무분별한 디지털 컨텐츠의 불법 복제와 배포가 이루어져 많은 디지털 컨텐츠 제작자들이 그 저작권에 피해를 보고 있는 실정이다. 불법적인 디지털 컨텐츠의 배포로 인한 지적 재산권을 보호하고자 많은 DRM(Digital Right Management) 시스템들이 개발되고 있다. 제작자(Provider)에 의해서 제공된 컨텐츠를 사용자가 사용하기 위해서 라이선스가 필요하다.[4] 사용자는 정당한 지불을 통해 라이선스를 획득하게 된다. 라이선스를 가진 사용자만이 컨텐츠를 사용할 수 있도록 하기 위해서 컨텐츠 분배자는 컨텐츠를 가공하게 되고 분배자는 가공된 컨텐츠 사용여부를 가늠하는 키를 라이선스를 획득한 사용자에게 전송해준다.

이러한 DRM 시스템에서 불법적인 사용자가 정당한 사용자의 정보를 이용하여 컨텐츠를 사용할 수 있기 때문에 사용자 인증이 필요하다. 많은 DRM 시스템에서 사용자 인증을 위해서 개인 인증서를 사용하고 있다. 인증서는 개인과 사이트를 인증할 수 있는 기능을 가지고 있지만 휴대성에 있어서 제 3의 저장장치를 필요로하기 때문에 번거로움이 있다.

본 논문에서는 사용자 인증을 위하여 사용자의 모바일 폰을 사용하였고, 하드웨어 정보를 이용한 PC 인증을 추가하여서 좀 더 효과적인 DRM 시스템을 설계하였다.

본 논문의 구성은 다음과 같다. 2장에서는 DRM 기술 현황과 기능, OTP(One Time Password), 해쉬 함수를 소개하고 3장에서는 DRM 시스템의 필요요

건과 기존 DRM 시스템의 문제점에 대해서 알아보고 4장에서는 개선된 DRM 시스템을 제안하고 개선된 성능을 기술한다. 5장은 결론과 향후 연구방향을 기술한다.

2. 관련연구

2.1 DRM 기술 현황 및 기능

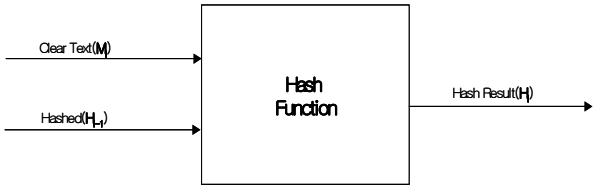
디지털 컨텐츠 저작권 보호를 위해서 많은 DRM 시스템이 개발되고 있다. DRM 시스템은 InterTrust사와 Microsoft사 등에서 개발되고 있으며, DOI(Digital Object Identifier)를 이용한 컨텐츠 식별을 통하여 DRM 시스템에 적용시키고 있다. XrML(eXtensible rights Markup Language)를 이용하여 저작권 정보를 명시하며 저작권 보호를 위한 시스템 개발에 노력하고 있다. [3][8][9]

2.2 일회성 패스워드(One Time Password)

일회성 패스워드(OTP, One Time Password)는 한번 쓰고 버리는 일회용 패스워드이므로 기존의 패스워드가 스니핑에 의해 가로채여도 새로 생성된 패스워드를 사용하므로 안전하다. OTP는 Challenge Number를 생성하는 시기에 따라 Challenge-Response 방식과 Time Synchronos 방식이 있다. Time Synchronos 방식은 생성 주기 내에 인증 신청을 한 사용자는 모두 같은 Challenge Number를 받게 될 수 있으므로 Challenge-Response 방식만을 사용한다. 이러한 OTP는 사이트의 안전한 접속을 위해서 유용하게 사용된다.[7]

2.3 해쉬함수

해쉬함수는 입력되는 데이터의 크기와 관계없이 일정한 크기로 축약하며 단방향 함수의 특성상 역함수가 존재하지 않으므로 해쉬된 결과물에서 원본



[그림 1] 해쉬함수

의 데이터를 복원할 수 없고 또한 원본 데이터의 크기나 내용을 알 수 없다. 해쉬함수는 단독으로 사용하기 보다는 암호화 알고리즘과 복합되어 전자서명의 형태로 무결성을 입증하는데 사용되거나 주민번호, 신용카드 번호 같은 관리자도 알아서는 안되는 개인 신상 정보들을 저장하는데 사용된다. 대표적인 해쉬함수 알고리즘들로는 MD4, MD5, SHA-1과 같은 것들이 있다.

3.DRM 시스템의 필요요건, 문제점

DRM 시스템에서 디지털 컨텐츠 저작권을 보호하기 위한 여러 가지 기능들 가운데 가장 중요한 부분은 컨텐츠에 대한 암호화 방법과 사용자에 대한 인증 방법이다. 사용자가 정당한 지불을 통한 컨텐츠 사용을 위해서 제공자에 의한 합당한 Business Rule을 적용하는 것도 중요한 필요요건이다. 컨텐츠를 사용하기 위해서는 라이선스가 필요한데 라이선스를 안전하게 보호하는 것 또한 DRM 시스템에서 없어서는 안될 중요한 필요요건이다.

하지만 기존의 DRM 시스템은 추가 인증기관을 통한 인증의 번거로움이 있고 정확하지 못한 사용자 인증과 사용자의 변칙적인 사용으로 인해서 종종 저작권에 대한 확실한 보호를 수행하지 못하는 경우가 발생한다. 컨텐츠를 암호화하고 복호화 하는데 쓰이는 키를 안전하게 전달하지 못한다거나 정당한 사용자를 사칭하는 불법적인 사용자에게 키가 유출되는 키 분배에 대한 위험성도 가지고 있다. 이 때문에 DRM 시스템은 좀 더 안전한 키 분배 방법과 좀 더 확실한 사용자 인증이 필요하다.

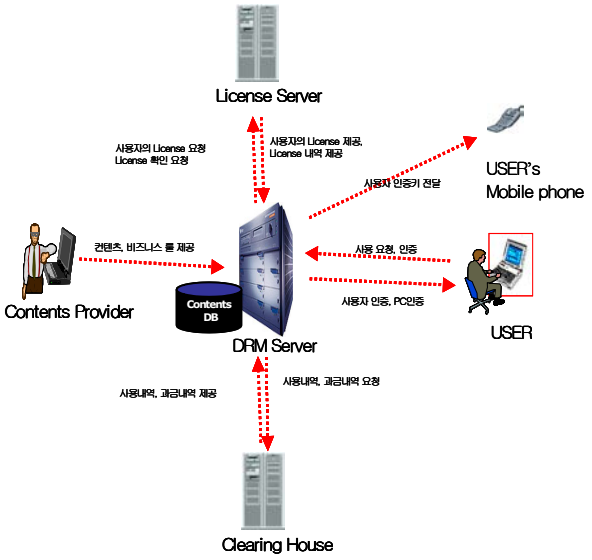
4.제안하는 DRM 시스템

4.1 라이선스

라이선스는 컨텐츠를 사용할 수 있는 PC의 계수를 적용하였다. 따라서 사용자는 사전에 라이선스를 구입할 때 사용자가 사용할 PC의 계수를 고려하여 라이선스를 구입하여야 한다. 이 라이선스 정책은 불법적인 사용자가 정당한 사용자의 정보를 이용하여 서버에 접속하더라도 Agent를 통한 하드웨어 정보를 서버에 전송받아 하드웨어 정보를 비교하기 때문에 컨텐츠 사용을 할 수 없게 만드는 기능을 한다. 또한 정당한 사용자가 다른 PC에서 컨텐츠를 사용하려한다면 제안한 인증 프로토콜을 다시 거쳐야 하며, 라이선스에 따라 컨텐츠를 사용할 수 있다.

4.2 제안하는 DRM 시스템의 구조

본 논문에서 제안하는 DRM 시스템은 [그림 2] 와 같다. DRM 서버는 CP(Contents Provider)로부터 컨텐츠를 제공받고 Business Rule을 합의한다.

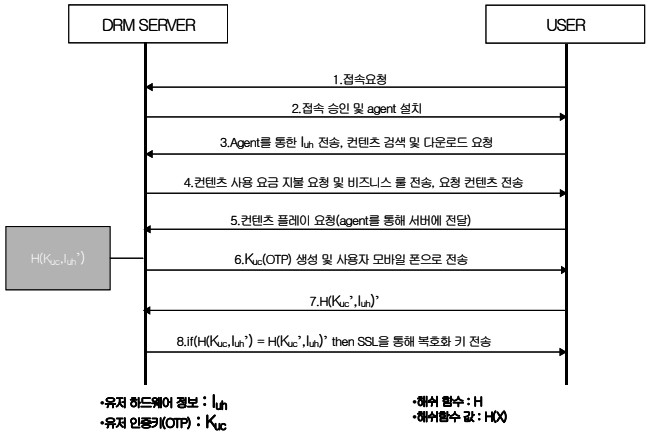


[그림 2] 제안하는 DRM 시스템 구조

서버는 제공받은 컨텐츠를 암호화하여 DB에 저장한다. 사용자는 컨텐츠를 검색, 선택, 지불 과정을 거친 후 전용플레이어를 통하여 컨텐츠 실행을 요청한다. 서버는 사용자의 지불내역을 Clearing House를 통해 제공받고 라이선스 서버에 라이선스를 요청한다. 서버는 Agent를 통한 사용자의 PC 인증과 사용자의 모바일 폰을 이용한 사용자 인증을 거친 후 SSL을 통하여 컨텐츠 복호화 키를 전송하고 라이선스 서버와 Clearing House에 사용자의 컨텐츠 사용내역을 전송한다. 서버로부터 복호화 키를 전송받은 사용자는 키를 이용하여 컨텐츠를 사용할 수 있다.

4.3 제안하는 인증 프로토콜

기존의 인증은 사용자 인증으로써 공인된 CA(Certificate Agent)를 통해 개인이 정당한 사용자인지를 인증하였지만, 제안하는 프로토콜에서는 사용자뿐만 아니라 사용자의 PC까지 인증함으로써 정당한 사용자의 라이선스를 불법적인 사용자가 불법적으로 획득하여서 사용하는 것을 막을 수 있다. 또한 라이선스를 타 사용자에게 양도하는 것도 막을 수 있다. 인증을 위한 프로토콜은 다음 [그림 3] 과 같다.



[그림 3] 제안하는 인증 프로토콜

서버는 사용자가 서버에 접속할 때 사용자 PC에 Agent, 전용 플레이어를 설치한다. Agent는 설치되어진 사용자 PC의 하드웨어 정보를 서버로 전송하고 사용자가 컨텐츠 실행 요청을 할 때 사용자 인증키를 요구한다. 이 때 사용자는 자신의 모바일 폰으로 전송받은 인증키를 입력한다. Agent는 입력받은 인증키와 수집한 하드웨어 정보로 해쉬값을 생성한다. 또한 생성된 해쉬값을 서버에게 전송하는 역할을 한다.

서버는 사용자의 컨텐츠 사용 요청이 있으면 Clearing House에 지불 현황을 요청, 제공받은 후 라이선스 서버에 라이선스를 요청한다. 그 후, 서버는 사용자의 모바일 폰으로 전송할 인증키(OTP, One Time Password)를 생성하고 사용자에게 전송한다(단, 모바일 폰은 사용자 본인이 소지한다는 가정). 이로서 서버는 사용자가 정당한 소지자라는 것을 인증하게 된다. 또한 Agent가 보내온 하드웨어 정보와 생성된 인증키를 해쉬하여 해쉬값을 생성한다. 해쉬값은 단방향 함수 값이기 때문에 Agent가 보내온 해쉬값과 같으면 Agent에게 복호화 키를 SSL을 통해 전송한다. Agent는 전송받은 복호화 키를 이용해 컨텐츠 복호화에 사용하고 폐기한다. 이와 같은 인증 프로토콜을 거쳐 사용자는 원하는 컨텐츠를 사용할 수 있다. 제안하는 프로토콜은 기존의 인증 방식에서의 불편함을 줄이고 불법적인 사용자에게 라이선스가 노출되는 것을 방지하였다.

기존의 인증방식은 불법적인 사용자가 불법적인 방법으로 라이선스를 획득하였을 때 해당 컨텐츠를 사용할 수 있었다. 하지만 본 논문에서 제안하는 DRM 시스템은 사용자 인증이 사용자가 항상 소지

하고 있는 모바일 폰을 사용하여 이루어진다. 또한 사용자 PC의 하드웨어 정보를 통하여 PC인증도 이루어지기 때문에 불법적인 사용자가 사용자 정보를 획득하더라도 사용자 PC와 다른 PC에서는 컨텐츠 사용을 할 수 없게 된다.

복호화 키는 Agent가 보내오는 해쉬값이 서버에서 생성한 해쉬값과 같아야만 전송된다. 하드웨어 정보가 제 3자에게 유출되더라도 매번 바뀌는 인증키(OTP)를 알 수 없기 때문에 복호화 키는 제 3 자에게 전송되지 않는다. 제안하는 본 DRM 시스템에서는 인증을 이중으로 하기 때문에 보다 안전하게 라이선스를 보호할 수 있다. 사용자가 불법적인 목적을 위해 사용 PC에서 Agent가 실행되는 것을 중단하려 한다면 Agent는 이를 감지하여 PC전원도 동시에 shutdown되도록 설계하여 Agent가 없는 상황에서 저작물이 실행되거나 변조되는 일을 방지하였다.

CP를 통해 제공 받은 컨텐츠는 대칭키 암호화 방식으로 암호화되어 사용자에게 전송된다. 또한 복호화 키는 사용자 PC로 전송될 때 SSL을 통해 전송되기 때문에 불법적인 사용자로부터 안전하다. 전송된 복호화 키는 1회 사용 후 폐기되기 때문에 사용자 PC에서 복호화 키를 획득하는 일은 불가능하다.

또한 본 논문에서 제안하는 시스템은 컨텐츠를 대칭키 암호화 방식으로 암호화하기 때문에 복호화 키가 필요하다. 복호화 키는 라이선스를 구입해야만 서버에서 전송되어지기 때문에 제안하는 DRM 시스템은 SuperDistribution이 가능하다.

5.결론

본 논문에서는 라이선스를 보호하기 위해 사용자의 모바일 폰과 사용자의 하드웨어 정보를 이용하여 DRM 시스템을 제안하였다. 사용자 인증을 위해 요즘 누구나 가지고 있는 모바일 폰에 인증번호를 전송하였고, PC 인증을 위해 사용자의 PC 하드웨어 정보를 서버에 전송하였다. 사용자 인증과 PC인증을 통해 라이선스를 효과적으로 보호할 수 있는 DRM 시스템을 설계하였다.

이 시스템은 제 3자에게 개인 정보가 유출됨으로 인한 제작자의 저작권 침해와 사용자의 피해를 방지할 수 있을 것으로 기대된다.

본 논문은 유선 환경을 고려한 시스템이며 무선 환경에서도 적용될 수 있도록 연구가 필요하며, 인증을 위해서 모바일 폰을 이용한 인증키 전송 시간과 해쉬함수의 처리시간, 복호화 키를 전송하기 위해 SSL 세션을 맺는 시간을 어떻게 단축하느냐가 연구되어져야 할 것이다.

참고문헌

[1] 김지홍, 이만영, 류재철, 송유진, 염흥렬, 이임영, 전자상거래 보안기술, 생능출판사, 2001.

[2] 박재표, 이광형, 김원, 전문석, “라이선스 에이전트를 이용한 디지털 저작권 보호를 위한 멀티미디어 데이터 관리 및 감시 시스템의 설계”, 컴퓨터산업교육학회 논문지, 제5권, 제2호, pp281-292, 2004

[3] 박복넝, 김태윤 “디지털 컨텐츠 저작권 보호를 위한 라이센스 분배 프로토콜”, 한국정보과학회 2002년 추계학술대회 2002

[4] 박재표 “동영상 데이터 보호를 윈한 공유키 풀 기반의 DRM 시스템의 설계”, 한국 정보처리학회 C권 4C11-166e

[5] 이덕규, 박희운, 이임영, “Agent 기반 불법 복제 방지 DRM모델”, 정보과학회 2001 추계학술대회, 제 28권, 제2호, pp682-684, 2001

[6] 이용효, 황대준, “에이전트 기반의 동적 디지털 저작권관리 시스템 설계 및 구현”, 한국정보처리학회 논문지 D, 제8-D권, 제5호, pp613-622, 2001

[7] IETF, RFC2289 A One-Time Password System, 1998

[8] Intertrust : http://www.intertrust.com/main/overview/drn.html

[9] Microsoft : http://www.microsoft.com/windows/windowsmedia/drm.asp