디지털 컨텐츠 저작권 보호를 위한 라이센스 분배 프로토콜

박복녕[0] 김태윤
고려대학교 컴퓨터학과
happy[0]@netlab.korea.ac.kr

License Distribution protocol for Digital Contents Rights Protection

Bok-Byong Park[0] Tai-Yun Kim
Dept. of Computer Science and Engineering, Korea University

요 약

인터넷의 발전을 통해 대량의 디지털 정보를 활용할 수 있는 기반이 형성됨에 따라 다양한 컨텐츠들이 인터넷 환경에서 이용 가능한 디지털 형태로 제작되어 활발하게 유통되고 있다. 그러나 인터넷을 통한 정보의 공유가 확산됨에 따라 컨텐츠 및 라이센스의 불법 사용 및 복제 등이 문제점으로 나타나게 되었다. 디지털 컨텐츠 유통에 있어서, 개별적인 컨텐츠를 보호할 수 있는 기술이 필수적으로 요구되고, 이러한 요구사항을 만족하기 위해 DRM 기술이 저작권 보호 기술로 이용되고 있다.

본 논문에서는 공개키 기반구조에 기초하여 저작권을 보호하고 관리하는 DRM 시스템에서의 라이센스 분배 프로토콜을 제안한다. 제안한 프로토콜은 Diffie-Hellman 키 생성 방식으로 세션키를 설정하여 라이센스를 암호화해서 전송하므로 컨텐츠의 불법사용과 유통을 방지한다.

1. 서 론

인터넷으로 인해 디지털 자원에 대한 유통 환경이 급속히 변화함에 따라 디지털 형태의 음악, 화상, 영상물, 출판물 등 멀티미디어 파일 형태의 상품 판매가 가능하게 되었다. 이러한 디지털 컨텐츠는 품질의 손상 없이 복제가 가능하기 때문에 이를 방지하기 위한 디지털 컨텐츠의 저작권 보호문제가 중요한 이슈로 대두되고 있다. 따라서 컨텐츠를 보호할 수 있는 기술이 필수적으로 요구되며, 이러한 요구 사항을 만족하기 위해 DRM 기술이 저작권 보호 기술로 이용되고 있다.

DRM (*Digital Rights Management*)은 암호화 기술을 이용하여 허가되지 않은 사용자로부터 디지털 컨텐츠를 안전하게 보호함으로써 저작권 관련 당사자의 권리 및 이익을 지속적으로 보호 및 관리하는 하드웨어와 소프트웨어를 포함한 포괄적인 저작권 관리 기술로 정의할 수 있다[1][2].

DRM 보호기술은 크게 나누어, 디지털 컨텐츠 자체에 대한 보호기술과 컨텐츠에 대한 접근을 보호하는 기술로 나눌 수 있다. 현재까지 개발된 DRM 기술은 주로 컨텐츠 자체에 대한 보호기술을 연구하여 디지털 워터마킹과 같은 보호기술이 발전하였으나, 컨텐츠 접근에 대한 보호기술에 대해서는 연구가 부족하였다. 컨텐츠 보호를 위하여 암호화 키 관리는 매우 중요하며, 암호화 키의 도난 방지를 위하여 엄격한 키 관리 및 분배 기술이 필요하다.

본 논문에서는 공개키 기반 구조(PKI : Public Key Infrastructure)[3]에 기초하여 디지털 컨텐츠의 저작권을 보호하고 자유로운 유통을 제공하기 위한 DRM에서의 라이센스 프로토콜을 제안한다. 라이센스를 안전하게 전송하기 위하여 객체간의 세션키 설정은 Diffie-Hellman[4] 키 설정 방식을 사용한다. 제안한 시스템에서는 컨텐츠를 사용하기 위한 소프트웨어 설치시 사용자의 PC에 DRM Client를 설치하여 DRM 서버와 상호 통신하여 작동함으로써 실시간으로 정보를 교환하고 컨텐츠 사용을 감시하여 컨텐츠 불법방지와 유통을 방지하여 제작자의 저작권을 보호한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 정보보호기술 및 디지털저작권 관리 기술을 소개하고, 3장에서는 논문에서 제안한 라이센스 분배 프로토콜을 기술한다. 4장에서는 프로토콜에 대한 성능 분석을 하고 5장에서는 결론 및 향후 연구 방향을 제시한다.

2. 관련 연구

2.1 암호화

암호화는 전자서명 및 정보보호를 위한 기본적인 기술이라고 할 수 있다. 암호화란 어떤 자료나 정보에 대하여 타인이 식별할 수 없도록 기술적 조치를 취하여 암호문으로 바꾼 것으로, 데이터를 암호화하는 방식은 대칭 암호화방식과 비대칭 암호화 방식의 두 가지 기본적인 형태가 있다[4].

컨텐츠 암호화에 사용되는 키는 안전하게 보호하기 위해서 정당한 사용자만이 접근 가능하도록 가공하여 컨텐츠 복호화 정보를 생성한다. 메타데이터에는 컨텐츠 유통 및 사용에 관한 비즈니스 규칙이 설정되어 있고 이 규칙 또한 위조 될 수 없도록 암호학적으로 보호된다.

2.2 키 분배 및 관리

DRM 키 분배 방식은 대칭키 방식과 공개키 방식으로 구별될 수 있다. 대칭키 방식은 하나의 키 분배 서버로 모든 부하가 집중되고 모든 컨텐츠 거래에 키 분배 서버가 관여해야한다. 반면 공개키 방식을 사용할 경우 분산성, 확장성, 상호운영성 등에서 많은 장점을 갖게되나 PKI가 필요하다는 부담이 있다. 그러므로, 컨텐츠의 특성 및 적용 환경에 따라 적절한 키 관리 매커니즘을 선택하는 것이 바람직하다.

2.3 DRM 시스템 구조

DRM 시스템은 디지털 컨텐츠 보호와 사용 규칙 관리 및 과금 체계 관리 구조로 구성된다. 그림 1은 일반적인 DRM 이용한 컨텐츠 유통 흐름도를 나타낸다[5].

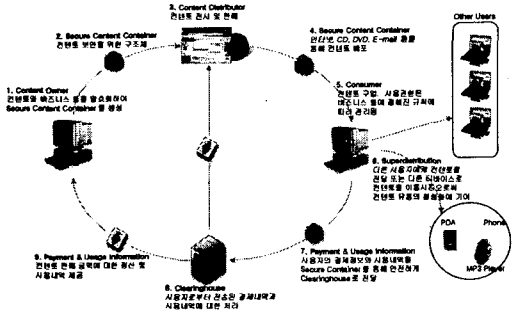

그림 1. DRM 흐름도

일반적으로 컨텐츠 보호는 디지털 컨텐츠 생성에서 배포, 사용, 폐기에 이르는 전 과정에 대해 암호화를 이용하여 가능하게 한다. 사용 규칙의 관리는 디지털 컨텐츠의 유통과 사용시 각 개인의 사용 규칙 및 권한을 정의한 것으로, 등록된 사용자는 허가된 규칙에 의해서만 컨텐츠를 사용하도록 제어할 수 있다. 마지막으로, 과금 체계 관리는 디지털 컨텐츠의 수익성을 지원하기 위해 디지털 컨텐츠의 사용 내역 관리와 이에 대한 과금 및 결재 관리 기능을 수행한다.

2.4 DRM 시스템의 요구 사항

DRM 시스템은 다음과 같은 요구 사항을 만족해야 한다[2].

① 컨텐츠 보호/인증
② 사용자 인증
③ Usage/Business Rule 적용
④ 라이센스 보호
⑤ 하드웨어 바인딩
⑥ Superdistribution

3. 제안한 라이센스 분배 프로토콜

3.1 제안한 DRM 시스템 구조

본 논문에서 라이센스 분배 프로토콜을 적용할 시스템은 그림 2에서 나타낸다.

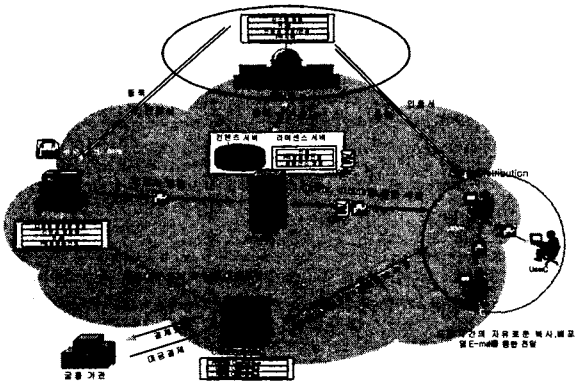

그림 2. DRM 시스템 모델

각각의 참여자는 CA에 공개키를 등록하고 인증서를 발급받는다. Publisher는 컨텐츠 Provider에게 컨텐츠를 암호화 하여 전송한다. User는 컨텐츠를 Provider의 웹 서버에서 제공받으며, 제공받은 컨텐츠는 암호화되어 있기 때문에 라이센스 없이 사용할 수 없다. 사용자는 지불 처리 후에 라이센스를 발급 받은 다음 컨텐츠를 사용할 수 있다. 클리어링하우스(Clearinghouse)는 지불 업무를 수행하고 사용자 컴퓨터의 DRM Client로부터 사용내역을 보고 받는다.

3.2 제안한 라이센스 분배 프로토콜

본 논문에서는 라이센스와 컨텐츠를 따로 분리하여 분배한다. 라이센스를 따로 분배 하기 때문에 컨텐츠의 재분배를 요구하지 않고 자유로이 라이센스 기간이나 규칙 등을 변경할 수 있다.

라이센스 분배 프로토콜은 라이센스 획득과 라이센스 인증 단계로 이루어진다. 사용자는 라이센스 서버와 라이센스 획득 프로토콜을 수행시킴으로써 라이센스를 얻게 된다. 라이센스 획득 단계 다음에 수행되는 라이센스 인증 단계에서는 사용자가 소유한 라이센스가 정당한 라이센스인지 확인한다.

제안하는 프로토콜에서 *U*는 사용자, *LS*는 라이센스 서버를 의미한다. 각 참여자와의 세션키 설정은 Diffie-Hellman 키 설정 방식을 사용한다.

프로토콜에 수행되기에 앞서, 각각의 참여자 모두는 공개키-개인키 쌍과 함께 인증서를 소지한다고 가정한다. 따라서 모든 프로토콜 메시지 교환에 있어서 부인방지(non-repudiation)의 기능이 추가되어 진다.

3.2.1 라이센스 획득 프로토콜

그림 3은 사용자 *U*가 다운로드한 컨텐츠에 대해 사용료를 지불 한 후에 *LS*에 라이센스를 요청하여 획득하는 프로토콜이다. 사용자 *DID*는 지불단계에서 등록된다.

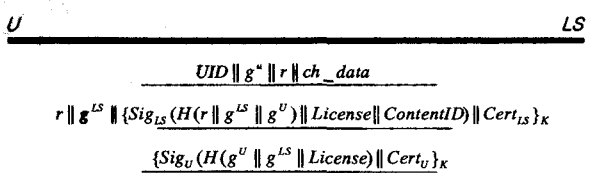

그림 3. 라이센스 획득 프로토콜

먼저 사용자는 난수 U를 생성하여 키 설정용 임시 공개키 g^U를 계산한 후 키 생성에 사용할 난수 r을 생성하고, 자신의 신원 UID, 그리고 지불에 관련된 데이터인 ch_data를 전송한다. UID는 $H(DID)$로 구성된다. DID는 사용자의 하드웨어 장치 ID로 사용자에 대한 식별자료로 이용되며 사용자의 익명성을 보장한다.

LS는 U로부터 메시지를 받아 $H(DID)$를 확인하여 U가 등록된 사용자인지 확인하고, 지불 정보를 확인하여 이에 해당하는 라이센스를 발급한다. LS는 임의의 난수를 생성하여 키 설정용 공개키를 계산하여 U로부터 전송받은 난수 r과 공개키를 이용하여 U와 공유하는 세션키 $K=H((g^{LS})^U\|r)$를 생성하여 메시지와 자신의 증명서를 생성한 세션키로 암호화하여 사용자로부터 받은 난수 r과 키생성용 임시 공개키 g^{LS}를 U에 전송한다.

라이센스를 획득한 U는 사용자의 공개키 인증서와 함께 $Sig_U((H(g^U\|g^{LS}\|License))$를 LS에 전송한다.

3.2.2 라이센스 인증 프로토콜

라이센스를 획득한 사용자가 컨텐츠를 복호하기 위해서는 라이센스를 인증받고 컨텐츠 복호키를 생성할 수 있는 KID를 LS로부터 전달 받아야한다. 라이센스 인증 프로토콜 수행 전에 U와 LS는 비밀 세션키 K를 소유하고 있다고 가정한다.

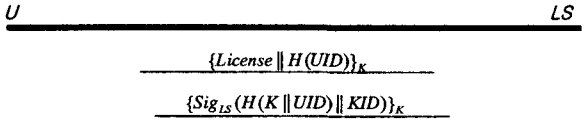

그림 4. 라이센스 인증 프로토콜

프로토콜(그림 4)이 시작되면, U는 $License$와 UID를 해쉬처리한 $H(UID)$를 LS에 전송한다.

LS는 U로부터 전송받은 메시지를 복호하여 $License$를 확인하고 전송받은 $H(UID)$가 저장되어있는 UID를 해쉬처리한 값과 일치하는지 확인한다.

$License$와 $H(UID)$를 확인하여 합법적인 사용자임이 검증되면 LS는 자신의 실체를 확인할 수 있는 정보와, KID를 세션키 K로 암호화해서 U에 전송한다.

U는 세션키를 계산하여 메시지를 복호한 후 서명을 검증하여 자신이 가지고 있던 정보와 $H(K||UID)$를 확인하여 LS의 실체를 인정하고, KID를 얻어낸다. U에서 KID는 컨텐츠 복호화 키 $Key=H(UID||KID)$를 생성하여 컨텐츠를 복호화하여 사용하게 된다.

4. 성능 분석

- 불법 유통 방지 : 제안한 프로토콜에서 사용하는 DID는 하드웨어 바인딩을 위해 추출한 사용자 장치의 고유키이다. 불법적인 사용자는 등록된 장치키와 동일한 키를 추출하지 못하므로 $H(DID)$ 값을 생성할 수 없어 라이센스를 인증 받지 못하므로, 타 장치에서 사용을 제한하여 라이센스의 불법 유통을 방지한다.
- 사용자 인증 : 라이센스 획득 프로토콜의 두 번째 메시지의 $H(r\|g^{LS}\|g^U)$를 통하여 U는 자신이 보낸 값과 일치하는지를 확인하여 서버와 동일한 세션키를 가지고 있다는 확신을 가지게 되고 결국 서버에 대한 실체인증이 포함되어 진다.
- 저작권 보호 : 제안한 프로토콜은 라이센스를 세션키로 암호화하여 전송하고 라이센스 내의 서버의 서명을 통해 라이센스의 위조 및 변조를 방지하여 라이센스를 보호하고, 라이센스의 불법 사용을 막아 디지털 컨텐츠 제작자의 저작권을 보호한다.
- Superdistribution : 제안한 프로토콜은 컨텐츠는 대칭키 방식을 사용하여 암호화하고, 라이센스는 공개키 방식으로 암호화함으로써 컨텐츠의 Superdistribution을 제공한다.

5. 결론 및 향후 연구

컨텐츠가 디지털화되고 인터넷이 발전하면서 디지털 컨텐츠의 불법 사용과 유통으로 인한 저작권 보호 문제가 발생하였다. 본 논문에서는 저작권 보호를 위해 PKI를 이용한 라이센스 분배 프로토콜을 제안하였다. 제안한 프로토콜은 Diffie-Hellman 키 설정 방식을 사용하여 라이센스를 암호화 함으로써, 라이센스를 안전하게 분배하여 라이센스의 불법 사용과 유통을 방지한다. 또한 하드웨어 바인딩을 이용하여 등록된 장치에서만 사용할 수 있도록 하여 제작자의 저작권을 보호한다.

향후 연구 과제로는 On-line 뿐만 아니라 Off-line에서도 저작권 보호가 가능한 연구를 할 것이다.

참고 문헌

[1] J. Dubl, "Digital Rights Management : A Definition", IDC, 2001

[2] J. Dubl, S. Kevorkian, "Understanding DRM System : An IDC White paper", IDC, 2001

[3] PKI Technical Specifications(Ver 2.0), 1996

[4] W. Diffie, M. Hellman, "New directions in cryptoraphy", IEEE Transactions on Information Theory, Vol. IT-22, No. 6, pp.472-492, Nov. 1976

[5] 강호갑, "소프트웨어 저작권 보호기술", 파수닷컴 기술문서, http://www.fasoo.com

[6] Schneier. Bruce, "Applied Cryptography, Second Edition", Essential reference for cryptographic engineers by the foremost pundit in the field, Wiley, 1996.