전자상거래를 위한 공개키 기반 AOD 시스템의 설계

김영준[0] 이윤정 박남섭 이병래 김태윤
고려대학교 컴퓨터학과
{dream[0], genuine, nspark, brlee, tykim}@netlab.korea.ac.kr

Design of AOD System based on PKI for e-Commerce

Young-Jun Kim[0] Yoon-Jung Rhee Nam-Sup Park Byung-Rae Lee Tai-Yun Kim
Dept. of Computer Science & Engineering, Korea University

요 약

최근 초고속 통신망을 이용한 인터넷의 대중화와 더불어 인터넷을 기반으로 하는 전자상거래가 활발해지고 있다. 특히 인터넷을 통한 MP3 데이터 등의 멀티미디어 컨텐츠의 유통은 많은 연구의 대상이 되고 있다. 하지만 기존의 AOD(Audio On Demand) 시스템들은 실질적인 불법복제방지와 저작권 보호에 미흡한 단점이 있다. 따라서 본 논문에서는 공개키 기반 구조(PKI: Public Key Infrastructure)[1,2]에 기초하여 실질적인 불법복제방지와 저작권을 보호하는 AOD 시스템을 제안한다. 제안된 기법은 사용자의 공개키를 이용하여 MP3 데이터를 전송함으로써 전송 도중 제 3자로부터의 공격에 대응할 수 있고, 정당한 사용자 외에는 MP3 데이터를 사용하지 못하도록 함으로써 사용자와 판매자의 권리를 보장한다.

1. 서론

인터넷을 통한 디지털 컨텐츠의 판매는 판매자의 입장에서는 저렴한 유통 방법에 의한 상품가격의 인하와 물류 및 유통망 비용 절감을 통한 가격 경쟁력 획득이라는 여러 가지 부가적인 이득을 가지고 있고[3] 구매자의 입장에서는 직접 매장에 가지 않고도 언제나 제품을 구입할 수 있으며 Try-Before-You-Buy, Pay-Per-Use 등 다양한 방법으로 구매할 수 있는 장점이 있다. 하지만, 이런 여러 가지 장점에도 불구하고 디지털 컨텐츠는 복제가 용이하고 복사본이 원본과 동일하기 때문에 인터넷을 통한 전자상거래에서는 디지털 컨텐츠의 대량 불법복제와 유통이 이루어질 수 있다. 따라서 디지털 컨텐츠의 저작권 보호와 사용자의 정당한 권리 보장을 위해서는 불법복제방지와 저작권 보호에 관한 연구가 이루어져야 할 것이다. 따라서 본 논문에서는 공개키 기반 구조(PKI: Public Key Infrastructure)[1,2]에 기초하여 MP3 데이터의 불법복제와 유통을 방지하고 사용자에게 보다 편리한 환경을 제공하기 위한 AOD 시스템을 제안한다.

본 논문의 구성은 다음과 같다. 2 장에서 MP3 저작권 보호를 위한 기술 동향에 대하여 소개하고 문제점을 제시하며 3 장에서 제안한 AOD 시스템을 설계한다. 4 장에서 기존의 AOD 시스템과 제안한 시스템의 성능을 비교 분석하고 5 장에서 결론 및 향후 연구 방향을 제시한다.

2. MP3 저작권 보호를 위한 AOD 모델

2.1 SecuMAX

SecuMax는 삼성의 MP3 미디어 데이터 유통 기술로서 사용자는 우선 MP3 디지털 컨텐츠 서비스 사이트에서 회원등록을 하게 된다 [4]. 회원 등록시 사용자의 ID, 패스워드, 주민등록번호를 SecuMAX 서버에 등록하게 되는데, 이것은 사용자 인증 역할을 수행하는 기초 자료로 활용된다. 회원 등록을 마친 후 암호 해독키와 전용 플레이어를 다운로드 받는데, SecuMAX 복호화 모듈이 내장된 music drive 가 들어 있다. 암호 해독키는 music drive 를 설치하는 과정에 등록하도록 되어 있으며, SecuMAX 를 지원하는 컨텐츠 서비스 사이트에서 sm3 파일을 제공받아 들을 수 있다 [4,5,6,7]. SecuMAX 는 저작권자에 대한 리포트를 해 주는 기능이 있고 불법복제를 어느 정도 차단할 수 있지만 키의 유출시 불법유통의 위험이 있다.

2.2 Digicap

Digicap은 BR네트콤이 개발한 기술로서, 사용자는 회원으로 가입한 후 Token Manager, Winamp, Winamp Plug-in을 다운로드 받아 설치하고 가변형 개인 Key 형태인 토큰(Token)으로 사용자를 인증 한다. Token Manager에서의 인증 절차가 끝나면 수시로 로그인해서 MP3 Download 메뉴에서 원하는 MP3화일을 다운로드 할 수 있다 [8]. Digicap은 Token을 이용하여 사용자를 인증하고 불법복제를 방지하지만 악의적인 사용자가 다운로드 받은 파일을 불법으로 배포할 시에는 적절한 대응책이 없다.

2.3 DLC를 이용한 MP3 유통 시스템

동적 사용권 관리(DLC: Dynamic License Control) 기술을 이용한 MP3 유통 시스템은 판매자 시스템의 DLC 서버와 사용자의 PC에 설치된 DLC 클라이언트간에 통신

을 통하여 사용권을 관리하여 불법 복제를 방지하고 정품을 인증하는 기술이다 [6]. DLC 유통시스템은 불법복제 방지에 효율적이지만 사용권과 MP3 데이터를 전송하는 도중에 제 3 자의 공격에 대한 대응책이 미비하다.

3. 제안한 AOD 시스템의 설계

본 논문에서 제안한 시스템은 공개키 기반 구조(PKI)에 기초하여 MP3 데이터의 불법복제와 유통을 방지한다.

3.1 제안한 AOD 시스템의 구성

제안한 AOD 시스템에 참가하는 주체로는 음반업체, 판매자 시스템(SS: Seller System), 판매자 에이전트(SA: Seller Agent), 사용자 시스템(CS: Customer System), 사용자 플레이어(CP: Customer Player), 지불처리시스템(PG: Payment Gateway)이 있다. 제안한 AOD 시스템에서는 사용자에게 MP3 파일을 전송할 때 사용자의 공개키로 암호화 한 EMF (Encrypted Mp3 File)를 전송한다. 그림 1은 제안한 AOD 시스템의 전체 그림이다.

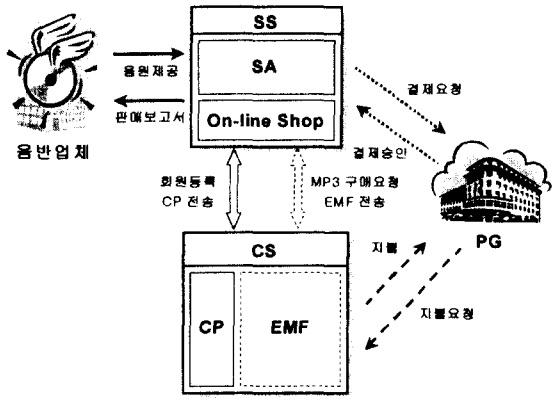

그림 1 MP3 유통 및 인증 관리 에이전트 시스템

■ **음반업체 (저작권자)**

① 음원을 판매자에게 제공한다.
② 판매자에게서 실시간으로 판매보고를 받는다.

■ **판매자 (SS)**

① 음반업체에게서 받은 음원을 MP3형태로 변환한다.
② 일정시간만 재생 가능한 샘플 MP3를 제작한다.
③ 소스(Source) MP3 파일은 판매자의 대칭키(Sym_{seller})로 암호화한다.
④ 샘플 MP3와 MP3 리스트를 홈페이지(*On-line Shop*)에 올린다.
⑤ 판매자 시스템의 에이전트는 판매와 회원관리를 대행한다. 새로운 회원이 등록하면 사용자 플레이어(CP)의 유무를 확인한 후 플레이어를 사용자의 시스템에 전송·설치한다.
⑥ 사용자에게서 구매요청이 들어오면 PG에 결제를 의뢰한다.
⑦ 결제가 승인되면 대칭키로 암호화된 해당 MP3 파일을 사용자의 공개키로 암호화하여 전송한다.
⑧ 판매상황을 실시간으로 음반업체에 통보한다.

■ **구매자 (CS)**

① 판매자의 홈페이지에 회원 등록을 하고 플레이어를 전송 받아 설치한다.
② 샘플 MP3 파일을 전송 받아 듣거나 원하는 곡을 고른 후 구매요청을 한다.
③ 지불을 완료한 후 암호화 된 MP3 파일을 전송 받아 감상한다.

■ **지불처리시스템 (PG)**

① 판매자에게서 결제요청을 받으면 해당 사용자에게 지불을 요청한다.
② 사용자의 지불이 완료되면 판매자에게 결제를 승인한다.

3.2 MP3 데이터의 상품 작성 및 수행

본 논문에서 제안한 시스템은 음반업체에게서 받은 음원을 MP3 형식으로 변환한 뒤 사용자에게 샘플을 제공하기 위한 샘플 MP3 데이터를 작성하고 원래의 MP3 데이터는 판매자의 대칭키로 암호화 시킨다. 사용자가 구매요청을 할 경우에는 대칭키로 암호화된 MP3 데이터에 사용자의 공개키로 암호화한 EMF 를 전송한다. 사용자가 사용자 플레이어(CP)를 통해 전송받은 EMF 를 재생시키면 CP 는 EMF 를 사용자의 비밀키와 판매자의 대칭키로 복호화하여 MP3 를 재생한다. 그림 2 는 MP3 데이터의 상품 작성과 수행을 나타낸다.

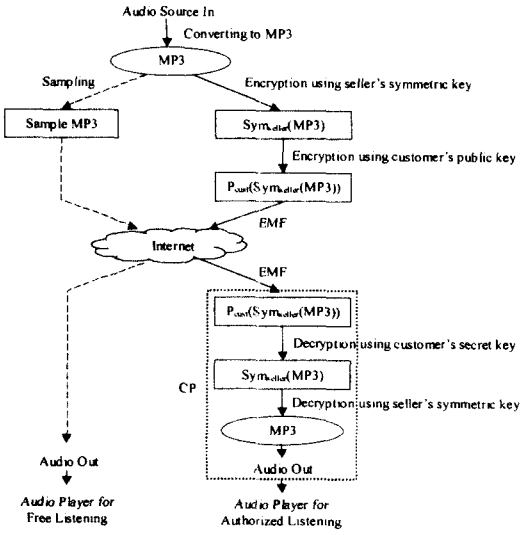

그림 2 안전한 MP3 상품 작성 및 수행 과정

3.3 MP3 데이터의 재생

본 시스템에서 판매자는 MP3 데이터를 전송할 때 제3자의 조작을 막기 위해서 판매자의 대칭키로 암호화 한 후 전송 중 공격에 대비해서 구매자의 공개키로 다시 암호화하여 전송한다.

표 1 MP3 데이터의 암/복호화에 사용되는 알고리즘

알고리즘	설 명
Sym_{seller}	판매자의 대칭키를 이용하여 평/암호문을 암/복호화한다.
P_{cust}	구매자의 공개키를 이용하여 평/암호문을 암/복호화한다.
S_{cust}	구매자의 비밀키를 이용하여 평/암호문을 암/복호화한다.

사용자가 전송 받은 EMF 를 재생하면 사용자 플레이어는 $P_{cust}(Sym_{seller}(MP3))$를 사용자의 비밀키인 S_{cust}로 복호화하여 $Sym_{seller}(MP3)$를 얻고 다시 판매자의 대칭키인 Sym_{seller}로 복호화하여 MP3 를 얻는다. 일련의 과정이 제대로 마쳐지면 사용자 플레이어는 복호화한 MP3 파일을 재생한다. 그림 3 은 MP3 데이터의 재생에 사용되는 복호화 프로토콜이다.

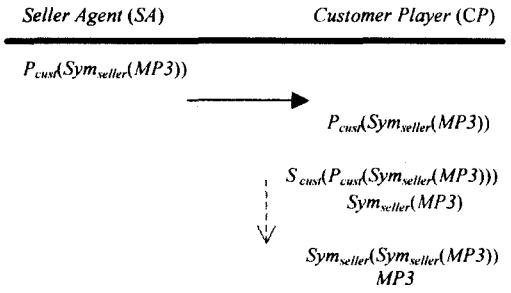

그림 3 MP3 데이터의 재생을 위한 복호화 프로토콜

4. 성능 평가 및 분석

본 장에서는 제안한 기법을 적용한 AOD 시스템과 기존 AOD 모델간의 성능을 비교 분석하여 평가한다.

표 2 제안한 시스템과 기존의 AOD 시스템과의 성능비교

비교항목 \ 적용시스템	SecuMAX 시스템	Digicap 시스템	DLC 시스템	제안한 시스템
인증 방식	개인용암호키	Token	동적사용권	공개키방식
MP3 불법 복제 방지	○	○	○	○
MP3 불법 유통 방지	×	×	△	○
샘플 MP3 제공	×	×	×	○
MP3전송시노출위험에대한대책	○	×	○	○
Key전송시노출위험에대한대책	×	×	×	○

(○: High △: Low ×: None)

표 2 는 제안한 시스템과 기존의 AOD 모델의 성능을 비교 분석한 것이다. 기존의 AOD 모델들은 MP3 파일의 불법복제는 막을 수 있지만 정식으로 구매한 사용자가 악의적으로 MP3 데이터나 키를 유포할 시에는 방지할 수 있는 대책이 미비하였다. 하지만 제안한 시스템에서는 현실적으로 제 3 자에게 배포가 있을 수 없는 개인의 비밀키를 이용하기 때문에 MP3 데이터의 불법 유통을 방지할 수 있다. 기존의 AOD 시스템은 사용자에게 구매전에 사용해 볼 수 있는 기회를 제공하지 못했으나 제안한 시스템은 샘플 MP3 를 제작하여 제공함으로써 사용자의 만족도를 높였다. Digicap 시스템은 암호화된 MP3 파일을 전송할 때 네트워크 상에 노 출되어 있기 때문에 해당 시스템의 재생 소프트웨어를 갖고 있는 attacker 는 전송되는 MP3 파일을 intercept 하여 사용할 수 있다. 하지만 제안한 시스템은 구매자에게 EMF 를 전송할 때 해당 구매자만 재생할 수 있도록 구매자의 공개키인 P_{cust}로 암호화하여 전송하기 때문에 attacker 는 전송되는 EMF 를 intercept 하여도 재생하여 들을 수 없다.

SecuMAX 와 Digicap, DLC 시스템은 사용자 인증을 위한 키를 전송할 때도 또한 키가 네트워크상에 노출되어 있기 때문에 attacker 가 중간에서 intercept 하여 사용할 수 있다. 하지만 제안한 시스템은 사용자 인증을 구매자의 비밀키인 S_{cust}를 이용하기 때문에 attacker 가 중간에 intercept 하여도 복호화하여 사용할 수 없다.

5. 결론 및 향후 연구 과제

현재 인터넷상에는 MP3 데이터를 무료로 제공하는 사이트들이 많이 있다. 사용자들의 입장에서 단기적으로는 이득인 것처럼 보이나 장기적으로 볼 때 생산자가 제공하는 제품에 대해 정당한 대가의 지불 없이 불법 사용이 만연한다면 그 결과는 전체 음악산업의 위축으로 이어져 결국 사용자들에게 불이익으로 돌아오게 될 것이다. 이러한 시점에서 전자상거래에 필수적인 저작권 보호라는 문제를 해결하는 것은 중요하다. 본 논문에서는 PKI 를 기반으로 한 MP3 데이터의 불법복제방지와 저작권이 보호되는 AOD 시스템을 설계하였다. 제안된 기법은 사용자의 공개키를 이용하여 MP3 데이터를 전송함으로써 전송도중 제 3 자로부터의 공격에 대응할 수 있고 정당하게 구매한 사용자 외에는 MP3 데이터를 사용하지 못하도록 함으로써 사용자와 판매자의 정당한 권리를 보장하였다. 향후 연구 과제로는 정당한 구매자의 MP3 사용장소의 제한을 없애고 서로 다른 불법복제 방지 시스템간의 호환성을 위한 연구가 이루어져야 할 것이다.

참고 문헌

[1] Perlman, R., "An overview of PKI trust models", IEEE Network, Vol.13 No.6, pp.38-43, 1999

[2] Oppliger, R., "Authorization Methods for E-Commerce Applications", Proceedings of the 1999 18th IEEE Symposium on Reliable Distributed Systems, pp.366-371, 1999

[3] 윤우성, 김태윤, "UML을 이용한 불법 복제 방지를 위한 ESD 서버 설계", 정보처리학회 춘계학술발표 논문집, 제7권, 제1호, 2000

[4] SecuMAX, "http://www.secumax.com/"

[5] http://www.hackersnews.org/data/2001/04/0425_21.html

[6] 강우준, 김응모, "디지털 저작권 관리 기술을 이용한 MP3 디지털 음악의 온라인 유통", 정보처리학회 논문지, 제7권 제11호, 2000. 11

[7] 강상승 외, "MP3 미디어 데이터의 온라인 유통 기술", 한국전자거래학회/한국정보시스템학회 종합학술대회 논문집, pp589-600, 1999

[8] Digicap, "http://www.digicaps.co.kr"