X9.59를 이용한 DRM 기반 컨텐츠 유통 시스템 설계 및 구현

김환조, 채종우, 정목동
부경대학교 컴퓨터공학과

Design and Implementation of DRM-based Contents distribution System using X9.59

Hwan-Jo Kim, Jong-woo Chae, Mokdong Chung
Dept. of Computer Engineering, Pukyong National University

요 약

인터넷의 고속화, 대용량화로 디지털 컨텐츠의 사용이 증가하고 있다. 디지털 컨텐츠는 비 손실 복제, 디지털 정보의 접근 용이성, 쉽고 빠른 배포 가능, 매우 적은 복제 비용 등의 특성으로 불법적인 복제와 배포가 널리 행해지고 있다. 이에 대한 대책으로 DRM(Digital Rights Management)에 대한 많은 연구가 이루어지고 있다. 최근 모바일 Device를 이용한 디지털 컨텐츠의 사용이 늘고 있다. 모바일환경에서 디지털 컨텐츠를 이용하기 위해서는 모바일환경의 여러 가지 조건을 고려해야한다. 본 논문에서는 X9.59 지불프로토콜을 이용하여 보다 안전하고 편리하며 모바일 환경에서도 적용 가능한 DRM기반 컨텐츠 유통 시스템을 설계하고 구현한다.

1. 서론

인터넷의 고속화, 대용량화로 디지털 컨텐츠의 이용이 증가하고 있다. 디지털 컨텐츠는 아날로그 데이터의 복사와 달리 여러 번의 복사를 수행하여도 동일한 품질을 유지하며, 인터넷을 통한 접근이 매우 용이하다. 또한 디지털 컨텐츠는 인터넷을 통해 쉽고 빠르게 배포가 가능하다. 그리고 복사 시에 드는 비용이 매우 적다. 이러한 특징들로 인하여 불법 복사로 인한 디지털 컨텐츠에 대한 저작권 문제가 발생한다. 이와 같이 인터넷상에서 디지털 데이터의 저작권을 보호하기 위한 방법으로 DRM[6,7,8]이 널리 사용되고 있다.

DRM을 사용함으로써 디지털 컨텐츠의 합법적인 유통 및 사용이 가능하고 이에 따라 디지털 컨텐츠 사용에 따른 수익구조를 기대할 수 있다.

최근 무선 인터넷의 발달로 모바일 장비를 이용한 컨텐츠 사용 역시 증가하고 있다. 모바일 장비의 특성상 처리할 데이터의 양이 작을수록, 처리 단계가 적을수록 좋다. 모바일 환경에서 디지털 컨텐츠를 이용하기 위해서는 모바일 환경의 특성을 고려해야 한다.

본 논문에서는 X9.59 지불 프로토콜[1]을 이용하여 모바일 환경에서도 좀더 편리하고 안전하게 디지털 컨텐츠를 이용할 수 있는 DRM기반 컨텐츠 유통 시스템을 설계하고 구현한다.

논문의 구성은 다음과 같다. 2절에서는 관련연구에 대해서 기술한다. 3절에서는 본 논문에서 제시한 DRM기반 컨텐츠 유통 시스템에 대해서 설명한다. 4절에서는 구현 및 평가에 대해서 기술하고 5절에서는 결론과 향후 과제를 제시한다.

2. 관련 연구

2.1 DRM(Digital Rights Management)

DRM[6,7,8]은 디지털 저작권 관리 시스템을 뜻하며 컨텐츠의 지적 재산권이 디지털 방식에 의해서 안전하게 보유/유지 되도록 하는 시스템으로 정의할 수 있다. 즉, 디지털 컨텐츠가 저작자 및 유통업자의 의도에 따라 전자상거래를 통해서 안전하고 편리하게 유통될 수 있도록 제공되는 모든 기술과 서비스 절차 등을 포함하는 개념이다. 그림1은 일반적인 DRM 구조이다. DRM을 이용한 디지털 컨텐츠의 유통 시스템이 갖추어야 할 기본 조건은 다음과 같다.

① 컨텐츠와 비즈니스 규칙의 패키징
컨텐츠 소유자는 판매할 컨텐츠와 적용될 비즈니스 규칙을 함께 암호화하여 안전하게 전달될 수 있는 방법을 제공해야 한다.

② 컨텐츠 배포
패키징된 디지털 컨텐츠를 인터넷, CD-ROM 또는 e-mail 등을 통해 안전하게 최종 사용자에게 전달

할 수 있는 방법을 제공해야 한다.

③ 컨텐츠 구입 및 사용

사용자가 컨텐츠에 대한 정당한 지불을 통해 컨텐츠를 이용할 수 있는 License를 획득할 수 있는 방법을 제공해야 한다.

④ Superdistribution

컨텐츠에 대한 정당한 권리를 가진 사용자가 다른 사용자에게 직접 또는 CD-ROM 등을 통해 전달할 수 있는 방법을 제공해야 한다. 전달 받은 사용자는 정당한 사용권한을 부여 받아야만 컨텐츠를 이용할 수 있다.

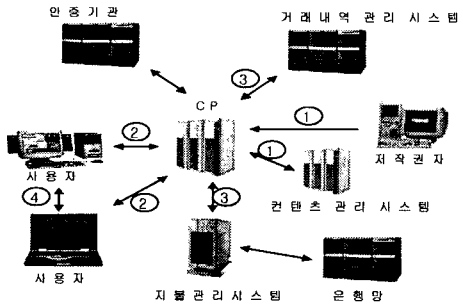

그림1. 일반적인 DRM 모델

2.2 X9.59

X9.59[1]는 account 기반의 지불방법에 대한 Finance Industry 표준이며 AADS(Account Authority Digital Signature)에 바탕을 두고 있다. X9.59는 CA-based PKI[5]를 사용하지 않고 안전하고 편리한 지불 방법을 제공한다. 공개키는 FI(Finance Industry)에 저장된다.

그림2는 X9.59의 지불 프로토콜을 나타낸다.

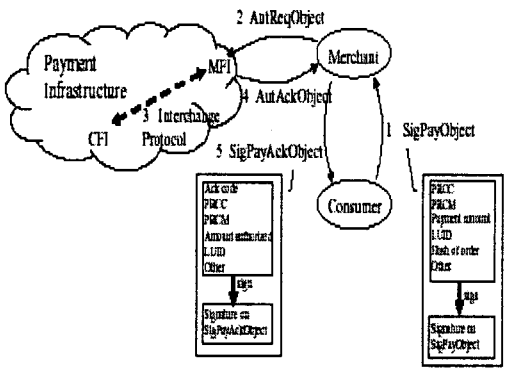

그림2. 지불 프로토콜

X9.59는 Consumer와 Merchant의 account/card number 대신에 Payment Routing Code(PRC)를 사용한다. PRC는 FI가 할당한 account number이며 FI 내부에서만 실제의 account/card number를 찾을 수 있다. consumer-CFI와 merchant-MFI는 서로를 신뢰한다.

Consumer가 Merchant에 접속하여 서비스 혹은 물품에 대한 정보를 요청하고 선택한 다음 결제 요청 메시지를 생성하고 자신의 개인키로 서명한 다음 Merchant에게 전달한다. Merchant는 이 메시지를 자신이 등록한 MFI에게 전달하고 MFI는 Consumer가 등록한 CFI에게 전달한다. CFI는 해당 Consumer의 공개키로 메시지의 서명을 검증하고 transaction을 처리한다. CFI는 결제 요청 응답 메시지를 생성하고 자신의 개인키로 서명한 다음 MFI에게 전달한다. 이 메시지는 Merchant를 거쳐 Consumer에게 전달된다. Consumer는 CFI의 공개키로 서명을 검증한 다음 처리 결과를 확인한다.

2.3 CONSEPP

CONSEPP(CONvenient and Secure Electronic Payment Protocol Based X9.59)[4]는 X9.59를 기본 개념으로 하면서 X9.59가 가진 Merchant의 인증서 문제를 해결하기 위해 다음의 방법으로 Merchant의 인증 문제를 해결하고 있다.

Consumer가 Merchant 인증요청 메시지를 생성하여 Merchant에게 전달한다. Merchant는 메시지를 MFI에게 전달한다. MFI는 해당 Merchant의 공개키를 Consumer의 등록은행인 CFI에게 전달한다. CFI는 Merchant의 공개키를 포함하는 인증요청 응답메시지를 생성하고 자신의 개인키로 메시지에 대해 서명을 한다. 이 메시지는 MFI와 Merchant를 거쳐 Consumer에게 전달된다. Consumer는 수신된 메시지에 대한 서명을 CFI의 공개키를 이용하여 검증한다. 그림3은 Merchant 인증 과정을 나타낸 것이다.

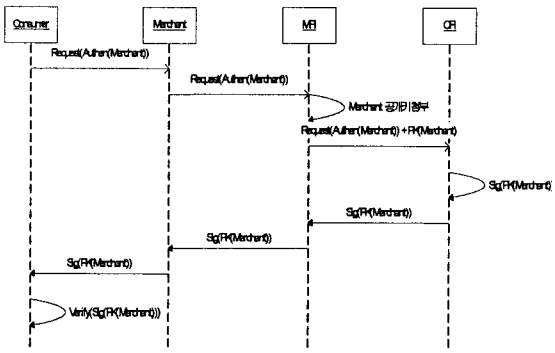

그림3. Merchant 인증 과정

3. DRM기반 디지털 컨텐츠 유통 시스템

3.1 시스템 구성

제안된 시스템은 Icarus로 불리며 MID(Mobile Information Device)와 CP(Contents Provider), 그리고 ClearingHouse와 FIs(Finance Industry)로 구성된다.

MID는 CP(Contents Provider)가 제공하는 컨텐츠를 사용하는 모바일 장비 사용자를 말한다.

CP가 컨텐츠 저작권자의 동의를 얻어서 컨텐츠를 패키징하여 컨텐츠를 제공한다. 패키징 관련 정보는 Clearinghouse에 저장되는데 이 정보는 License 발급시에 사용된다.

먼저 MID와 CP는 시스템을 이용하기 위해 각각 은행에 계좌를 개설한 후 은행이 생성한 키 쌍과 PRC, 그리고 은행의 공개키를 저장한다. 이는 MID의 제한된 기능을 고려한 것이다..

그림4는 Icarus 전체 시스템을 나타낸다.

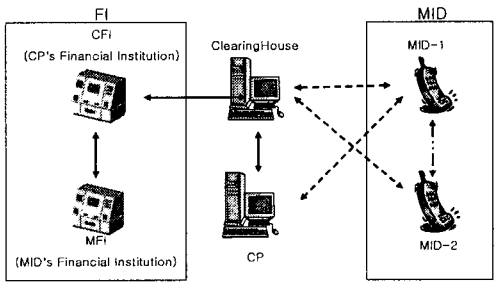

그림4. Icarus 전체 시스템 구성도

MID1과 MID2는 IrDA를 이용하여 컨텐츠를 주고받는다. MID2가 다시 CP에 접속하여 컨텐츠를 다운로드 받는 것은 시간 및 비용의 부담을 가중시키므로 사용하기에는 적합하지 않다.

MID1과 CP는 CONSEPP을 이용하여 상대방을 인증한다.

3.2 결제 과정

패키징된 컨텐츠를 다운로드 받은 후 컨텐츠에 대한 License를 결정하고 결제 과정을 처리한다. 거래내역은 ClearingHouse에 저장된다. Icarus에서는 ECDSA 알고리즘을 이용하여 서명을 생성한다.

결제 과정은 다음과 같다.

① MID1은 결제 요청 메시지를 생성하고 서명을 한 다음 CP에게 전달한다.
② CP는 결제 요청 메시지를 Clearinghouse에게 전달한다.
③ Clearinghouse는 결제 요청 메시지를 CFI에게 전달한다.
④ CFI는 결제 요청 메시지를 MFI에게 전달한다.
⑤ MFI는 MID의 서명을 검증하고 거래를 처리 한 다음 결과 메시지를 생성하고 자신의 개인키로 서명을 해서 CFI에게 전달한다.
⑥ CFI는 전달된 메시지를 Clearinghouse에게 전달하고 Clearinghouse는 결제 처리 응답 메시지를 확인하고 거래 내역을 저장한 다음 해당 컨텐츠에 대한 License를 생성하고 결제 처리 응답 메시지와 License를 CP를 통해 MID에게 전달한다.
⑦ MID는 MFI의 서명을 검증하고 결제 처리 결과를 확인한다.

그림5는 결제 과정을 순서 다이아 그램으로 표현한 것이다.

3.3 Superdistribution

Superdistribution은 DRM의 갖추어야 할 기본적인

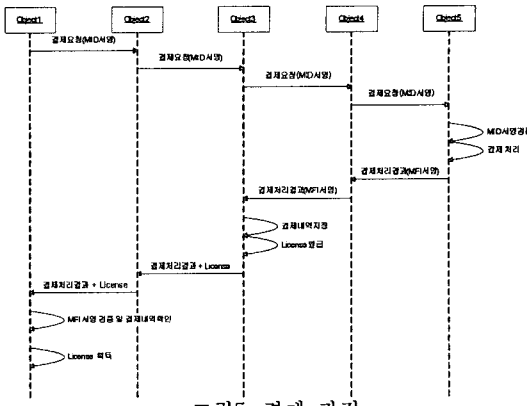

그림5. 결제 과정

기능으로서 컨텐츠에 대한 권리를 소유한 사용자가 다른 사용자 혹은 매체를 통해 배포하는 것을 뜻한다. 이 절에서는 컨텐츠에 대한 권리를 소유한 사용자(MID1)가 다른 사용자(MID2)에게 컨텐츠를 배포하는 것에 대해서 논한다. 배포된 디지털 컨텐츠는 마찬가지로 컨텐츠에 대한 License를 가져야만 사용이 가능하다.

그림6은 본 논문에서 사용되는 License의 XML Schema이다.

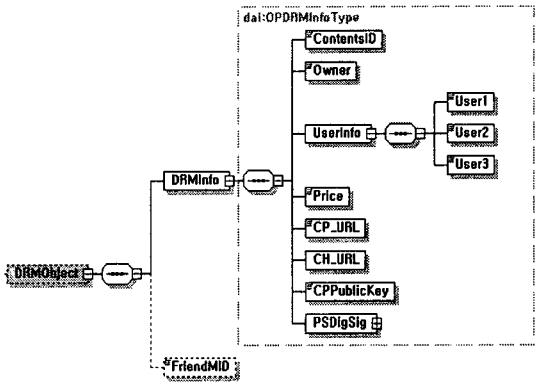

그림6. License의 XML Schema

컨텐츠를 사용하고자 할 때 사용자의 정보가 Owner 또는 UserInfo 내에 있을 경우에만 사용이 가능하다. 컨텐츠를 최초로 다운 받은 사용자 MID1에 대한 정보가 Owner에 저장된다. 다른 MID에게 컨텐츠를 전달할 때에는 다음과 같은 과정이 이루어진다.

① 디지털 컨텐츠에 대한 권리를 가진 사용자만이 다른 사용자 MID2에게 컨텐츠를 전달할 수 있다.
② 전달 받고자 하는 사용자 MID2가 MID1에 접속하여 컨텐츠를 전달받는다.
③ MID2는 자신에 관한 정보를 MID1에게 전달한다.
④ MID1은 MID2에 관한 정보를 포함하는 결제 요청 메시지를 생성하고 서명한 후 Clearinghouse로 전송한다.
⑤ 전달된 메시지는 CFI를 통해 MFI에게 전달된다.

⑥ MFI는 MID1의 서명을 검증하고 거래를 처리한다. 결제 요청 응답 메시지를 생성하고 자신의 개인키로 서명한 다음 CFI를 통해 Clearinghouse에게 전달한다.

⑦ ClearingHouse는 결제 요청 처리 결과를 확인하고 결제 내역을 저장한 다음 MID2가 해당 컨텐츠를 사용할 수 있도록 License를 발급하고 결제 요청 응답 메시지와 License를 MID1에게 전달한다.

⑧ MID1은 결제 요청 응답 메시지를 확인하고 License를 자신에게 적용하고 MID2에게 전달한다.

⑨ MID2는 전달된 License를 이용하여 컨텐츠를 사용할 수 있다.

그림7은 Superdistribution 과정을 순서 다이아 그램으로 나타낸 것이다.

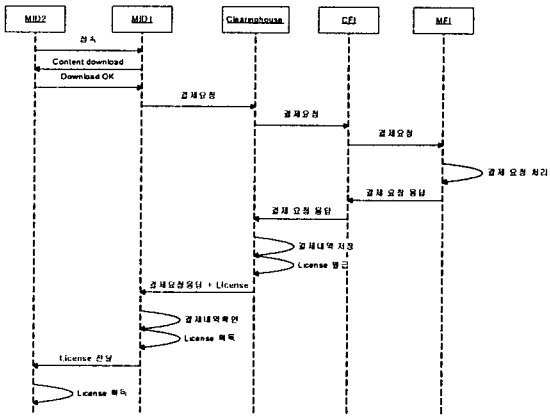

그림7. Superdistribution

4. 구현 및 평가

4.1 구현

① 구현 환경

- Clearinghouse, CP, CFI, MFI : Servlet
- MID1, MID2 : J2ME
- Language : JDK 1.4.1

② 비즈니스 규칙과 패키징

비즈니스 규칙은 해당 컨텐츠와 사용 환경에 따라 서로 다른 규칙이 적용된다. 비즈니스 규칙을 사용자에게 제시한 후 컨텐츠와 비즈니스 규칙이 결정되면 패키징 및 암호화 과정을 거치고 복호화에 관련된 정보는 Clearinghouse에 저장된다. 이 정보는 컨텐츠에 대한 결제가 이루어진 후에 사용자에게 전달되어 복호화에 사용된다. 컨텐츠의 배포시 결제는 컨텐츠 배포자가 부담하며 최대 6명까지 배포가 가능하도록 하였다.

4.2 평가

본 논문에서 제시한 시스템은 2.1에서 제시한 DRM을 이용한 컨텐츠 유통 시스템이 갖추어야 할 기본 조건을 만족하고 있다. 더불어 사용자간 IrDA를 이용하여 컨텐츠 배포 방법을 구현하여 편리한 컨텐츠 배포 방법을 제시하였고, PKI를 적용한 시스템에 비해 보다 간단하면서도 안전한 시스템을 제안하였다. 따라서 모바일 환경에서도 PKI에 의한 CRL부담에서 벗어나서 거래를 할 수 있게 되었다.

5. 결론

본 논문에서는 X9.59 지불 프로토콜을 이용하여 안전하고 편리하며 모바일 환경에 적용 가능한 DRM을 이용한 컨텐츠 유통 시스템을 설계하였다. X9.59를 기본으로 하는 CONSEPP를 이용하여 결제 과정을 설계함으로써 CA 및 Certificate 사용에 따른 설치 및 유지비용 절약하고 보다 간단한 시스템을 제안하였다. 또한 메시지의 크기를 줄이고 ECDSA 알고리즘을 이용하여 모바일 환경에서도 사용할 수 있도록 하였다.

그리고 사용자간 IrDA를 이용하여 컨텐츠를 편리하고 쉽게 배포할 수 있는 방법을 제시하여 컨텐츠 제공자의 이익을 높일 수 있는 모델을 제시하였다.

향후 연구 과제로 다양한 비즈니스 규칙을 적용할 수 있는 방법에 대한 연구가 필요하다.

[참고문헌]

[1] American National Standard DSTU X9.59 Electronic Commerce for Financial Service Industry: Account Based Secure Payment Object, 2000.

[2] A.Wheeler, L. Wheeler, Payment Security & Internet Reference, http://www.garlic.com/~lynn

[3] 강호갑, "소프트웨어 저작권 보호 기술," http://www.drm.or.kr

[4] Albert Levi. Certin K. Koc,"CONSEPP: Convenient and Secure electronic payment Protocol based on X9.59," Proceedings 17th Annual Computer Security Application Conference, 2001, New Orleans, Louisiana.

[5] R. Housley, W.Ford W. Polk and D. Solo, RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", Internet Engineering Task Force, January 1999.

[6] Frank Hartung and Friedhelm Ramme, "Digital Rights Management and Watermarking of Multimedia Content for M-Commerce Application," IEEE Communications Magazine November 2000.

[7] Qiong Liu, Reihaneh Safavi-Naini, "Digital Rights Management for Content Distribution", http://citeseer.nj.nec.com/560657.html

[8] Joan Feigenbaum and Michael J. Freedman, "Privacy Enginnering for Digital Rights Management Systems", http://citeseer.nj.nec.com/feigenbaum01privacy.html