2001 년 한국정보처리학회 추계 학술발표논문집 제 8 권 제 2 호

# E-Book 용 DRM Publisher 시스템의 설계

장우영, 신용탁, 신동규, 신동일
세종대학교 컴퓨터공학과
e-mail : ouyoung@gce.sejong.ac.kr

# Design of DRM Publisher System for E-Book

Wooyoung Jang, Yongtak Shin, Dongil Shin, Dongkyoo Shin
Dept. of Computer Engineering, Sejong University

요 약

인터넷은 처음에는 단순히 오프라인에서 유통되는 실물 상품의 흐름을 중개해주는 역할을 해왔으나 인터넷을 통한 실물상품의 중개는 아날로그 상태의 상품들이 인터넷이라는 거간꾼의 중개작용을 통한 전자상거래 형태로 정착되었다. 이러한 실물 상품 유통의 중개자였던 인터넷은 실물 상품들이 디지털화 됨으로써 컨텐츠들의 유통을 위한 통로이면서 동시에 그 자체로서 메시지가 되어버린 하나의 매체로 전환하게 되었다. 그러나, 인터넷을 통해 디지털 컨텐츠들이 쉽고 간편하게 원본과 똑같은 품질로 복제할 수 있을 뿐만 아니라 상상을 초월하는 빠른 속도로 이동이 가능하여 사용자들이 불법으로 얼마든지 이용할 수 있다는 것이다. 현재 국내, 국외에서 이러한 문제를 해결하기 위해 제안한 기술 디지털 컨텐츠들을 보호하고 관리할 수 있도록 하는 DRM(Digital Rights Management)이라는 시스템이 계속적으로 개발되고 있다[1]. 디지털 컨텐츠를 보호하고 저작권을 관리 하는 시스템인 DRM 에는 크게 세 가지의 기본 시스템(Publisher, Customer, DRM Server System)이 있다. 본 논문에서는 컨텐츠를 등록하고 저작권자가 그 컨텐츠를 관리하는 DRM Publisher System 을 키 알고리즘을 이용하여 설계한다.

## 1. 서론

최근 디지털 컨텐츠의 저작권에 대한 논쟁이 뜨겁게 달아오르고 있다. 최근 미국의 메이저 음반사와 온라인 음악 다운로드 사이트인 냅스터간의 저작권 관련 항소심에서 냅스터의 행동은 위법이니 중지하라는 판결이 나오면서 국내에서도 저작권에 대한 보호를 위해 여러 조치들을 취하고 있다. 그 예로 소리바다를 들 수 있는데, 아직까지 결론에 다다르지 못한 상태이지만 웹에서의 컨텐츠에 대해 저작권자를 보호해야 하는 상황은 반드시 올 것이다. 이러한 조치로서 디지털 컨텐츠를 관리하고 저작권자를 보호해주는 DRM 시스템이 개발하고 있으며, 상용화 하고 있다.

디지털 컨텐츠의 불법사용방지 및 저작권 보호를 위한 기술로 유일하게 주목 받고 있는 최신 기술로 DRM(Digital Rights Management) 기술이 있다. 이 DRM 기술은 신뢰성 있는 라이센스, 안전한 저작권과 허가, 신뢰성 있는 환경과 인프라를 가능하게 하는 하드웨어와 소프웨어를 포함하는 디지털 저작권 관리를 위한 넓은 의미의 기술이다. DRM 기술에는 관리하고 복제를 방지하기 위한 많은 기술들이 포함되어있다. 여기에는 중요하게 사용되는 워터마킹이 있으며, 이것은 저작권을 추적하고 복제를 방지하기 위해 사용되는 기술이다[2]. 그리고, 키 알고리즘을 이용해 사용자의 인증을 하는 기술이 있다. 그러나, 이 기술은 초기 단계이고, 이런 DRM 을 연구하기 위해 여러 워킹 그룹(MPEG, SDMI, EBX, OeB)에서 자체적으로 스펙을 개발 발표하고 있다[3].

DRM 시스템에는 크게 세 가지의 기본 시스템(Publisher, Customer, DRM Server System)이 있다. DRM Publisher System 은 저작권자가 컨텐츠를 등록하고 자신의 컨텐츠를 관리하는 것이며, Customer System 은 컨텐츠를 구입하여 특정 리더기를 이용하여 보고, 읽고, 들을 수 있는 것이다. 마지막으로 DRM Server System 은 등록된 컨텐츠를 보호하고, 관리하고, 소비자들에게 컨텐츠 리스트를 제공하는 역할을 한다.

본 논문에서는 기본 시스템에서 컨텐츠를 등록하고, 관리하는 DRM Publisher System 을 설계한다. 이는 워

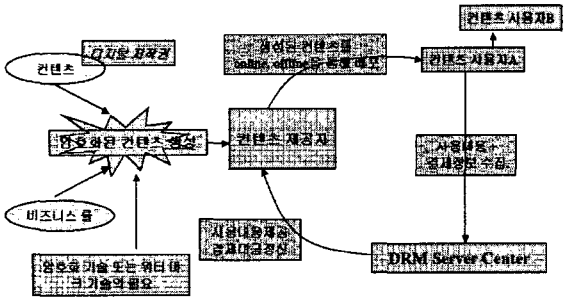
터마킹과 통신 프로토콜인 SSL 을 사용하여 저작권자의 권리와 그 컨텐츠를 보호하며 등록할 수 있는 시스템이다.

먼저, DRM 이란 기술은 무엇이며, 어떠한 구조를 갖는가에 대해 설명하며, 여기에 사용되는 SSL 보안 프로토콜을 설명한다. 그리고, 저작권 언어로 XrML 에 대한 설명을 하며, 마지막으로 본 논문에서 제시하게 되는 DRM Publisher System 을 설명한다.

## 2. 관련 연구

### 2.1 DRM(Digital Rights Management)

먼저 DRM 의 정의를 내리면, 암호화 기술을 이용하여 허가되지 않은 사용자로부터 디지털 컨텐츠를 안전하게 보호함으로써 컨텐츠 저작권 관련 당사자의 권리 및 이익을 지속적으로 보호 및 관리하는 시스템으로 정의할 수 있다. 즉, 디지털 컨텐츠가 저작자 및 유통업자의 의도에 따라 전자상거래를 통해서 안전하고 편리하게 유통업자의 의도에 따라 전자상거래를 통해서 안전하고 편리하게 유통될 수 있도록 제공되는 모든 기술과 서비스 절차 등을 포함하는 개념이다. 다음 그림 1 은 DRM 을 이용하여 디지털 컨텐츠가 유통되는 전체 과정을 보여준다.




[그림 1] DRM 전체 구조

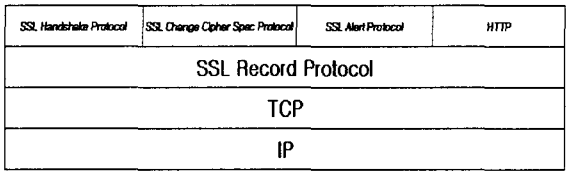
위와 같은 웹상에서의 유통과정을 가지고 있기 때문에 웹의 취약점인 보안이 중요하다. DRM 기술에는 웹의 취약점을 보완하기 위한 필수적인 보안 요소가 있는데, 첫 번째는 컨텐츠의 내용을 알 수 없게 암호하는 암호화(Encryption)이고, 두 번째는 아무나 접근할 수 없게 하는 접근 제한(Conditional access), 세 번째는 불법적으로 복제를 하지 못하게 하는 복제 제어(Copy Control), 복제 되었을 때 그 복제된 컨텐츠를 추적하고 확인하는 Identification 과 tracing 이다[3].

### 2.2 SSL(Secure Socket Layer)

SSL 최신 버전은 SSL3.0 이며 SSL3.0 을 기반으로 TLS(Transport Layer Security) 프로토콜 표준화가 발표되었다.

SSL 규약은 서버와 클라이언트의 진위 확인을 하도록 해 주며, 사용하는 어플리케이션에 대해 독립적이어서 HTTP 나, FTP, Telnet 등의 어플리케이션이 SSL 을 기반으로 운용되도록 할 수 있다. 또한 암호화 키(encryption key)와 관련된 협상을 할 수 있을 뿐만 아니라 상위의 응용 프로그램이 정보를 서버와 교환하기 전에 서버의 진위를 확인해 줄 수 있다. 암호화와 진위 확인, 메세지 확인 규칙 등의 방법을 통해 송수신 경로의 보안과 안정성을 유지시켜 준다.[5]

다음 그림 2 는 SSL 프로토콜의 구조이다. 이는 크게 핸드세이크 프로토콜과 레코드 프로토콜로 되어있고, 핸드세이크 프로토콜은 다시 Change cipher spec protocol, Alert Protocol, 핸드세이크 프로토콜로 나뉘어진다[6].




[그림] 2 SSL 프로토콜 구조

### 2.3 XrML(Extensible rights Markup Language)

ContentGaurd 사에서 Xerox 의 DPRL 2.0 을 바탕으로 만든 XML 기반의 디지털 권리 마크업 언어이다. 현재 W3C 에 제안한 상태이며, 상거래 모델에 따른 권리, 요금, 조건부가 등 권리에 관련된 내용을 XML 표현 방식을 통해 정의한 언어이다.

XrML 의 기본 구조라 할 수 있는 최상위 구조는 그림 3 과 같다[4].

```
<XrML>
  <BODY>
        (ISSUED)?
        (TIME)?
        (DESCRIPTOR)?
        (ISSUER)?
        (ISSUEDPRINCIPALS)?
        (WORK)?
        (AUTHENTICATEDDATA)?
  </BODY>
  (SIGNATURE)?
</XrML>
```

[그림 3] XrML 최상위 구조

루트 요소 XrML 안에서는, 명령 요소 BODY 와 임의 요소 SIGNATURE 가 있다. 후자는 원본 자체를 보증하는데 사용된 전자의 디지털 서명이다. BODY 요소는 디지털 작업의 임의 묘사와 XrML 문서에 관한 임의 메타정보로 구성되어 있고, 요소 TIME 은 XrML 문서가 유효한 시간 범위를 나타낸다. 요소 ISSUED 는 이 문서가 발생된 시간을 나타내고, 요소 DESCRIPTOR 는 이 문서의 설명을 나타낸다. 요소 ISSUER 은 이 XrML 문서를 작성하는 주요 요소이고, 요소 ISSUED PRINCIPALS 는 이 문서가 일으키는 주요 목록이다. 요소 WORK 은 디지털 작업과 사용 권리들을 정의한다. 요소 ATHENTICATEDDATA 는 이 XrML 문서를 처리하는 응용프로그램에게 제공되는 데이터를 포획한다.

XrML 은 디지털 작업과 DPRL 버전에서 사용되는 방법과 비슷한 사용권리를 묘사한다. Work 를 정의하는 전반적인 구조는 다음과 같다. 각각의 엘리먼트에 대한 설명은 참고 문헌 [4]에 자세히 설명되어 있다.

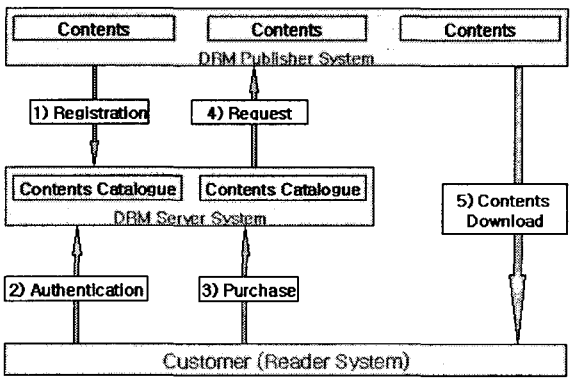
```
<WORK>
      (OBJECT)
      (DESCRIPTION)?
      (CREATOR)*
      (OWNER)?
      (DIGEST)*
      (PARTS)?
      (CONTENTS)?
      (COPIES)?
      (COMMENT)?
      (SKU)?
      (RIGHTSGROUP | REFERENCEDRIGHTSGROUP )+
</WORK>
```

[그림 4] Work 엘리먼트의 구성요소

## 3. DRM Publisher 시스템의 설계

DRM server 시스템은 리눅스를 운영체제로 하며, 서버와 클라이언트간의 연결은 암호화(encryption)와 진위 확 인(authentication), 메세지 확인 규칙(message authentication code) 등의 방법을 통해 송수신 경로의 보안과 안정성을 유지시켜 주는 SSL 을 사용한다.

전체 구조를 설명하기 전에 본 논문에서 선택한 DRM 시스템의 모델은 그림 5 와 같다.

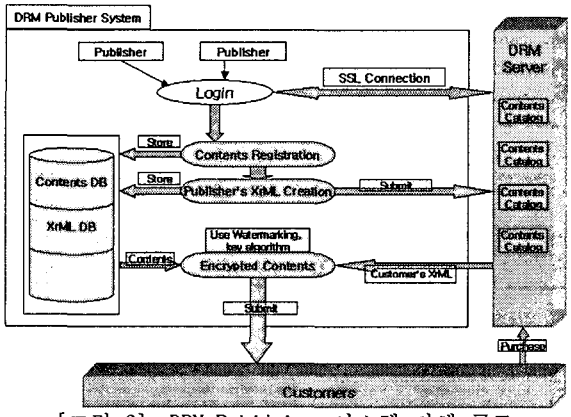



[그림 5] DRM 시스템 모델

출판자가 DRM 서버에 등록을 하고 컨텐츠는 자신의 데이터 베이스에 저장한다. 서버는 출판자가 등록한 컨텐츠의 리스트를 작성하여 사용자에게 보여준다. 사용자는 서버로부터 리스트를 보고 구매를 하게 되고 서버는 사용자가 선택한 컨텐츠를 출판자에게 요청을 하게 된다. 출판자는 요청 받은 컨텐츠를 직접 사용자에게 다운로드하게 되는 모델을 갖는다.

다음 그림 6 는 DRM Publisher 시스템의 전체 구조를 보여준다.

여기서 Publisher 는 DRM server 에 등록(회원 가입)된 조건을 전제로 한다. 먼저 Publisher 는 로그인을 통해 DRM Server 에 연결되고, 연결되면서 서로간의 인증을 위해 SSL 을 사용하여 보안 연결이 된다. 그리고, Contents Registration 에서 등록하게 될 컨텐츠의 정보인 저자, 출판일, 출판사, 가격 등을 입력하고, 이를 기반으로 DOM 파서를 이용하여 Publisher's XrML 문서를 생성하여 DRM server 에 전송하고 자신의 XrML DB 에 저장하고, 컨텐츠는 자신의 Contents DB 에 저장한다.

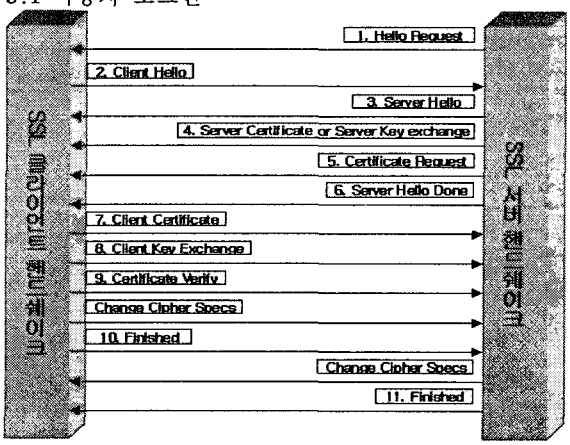



[그림 6] DRM Publisher 시스템 전체 구조

DRM 서버에서는 출판업자가 작성하여 보낸 XrML 문서를 DB 에 저장하고 컨텐츠에 대한 정보들을 Contents Catalog 를 작성하여 사용자들에게 보여주게 된다. 사용자가 구매 할 때, 컨텐츠에 대한 조건을 작성하여 서버에 보내게 되는데, 서버는 이를 받아 Customer's XrML 문서를 생성하여 DRM Publisher System 에게 전송한다. 출판업자는 이 XrML 문서와 그에 해당하는 컨텐츠를 워터 마킹과 키 알고리즘을 이용하여 암호화된 컨텐츠를 생성하여 사용자에게 전송하게 된다.

위 구조는 크게 세 부분으로 나누어진다. 사용자 로그인과 컨텐츠 등록 그리고, 컨텐츠와 XrML 의 암호화이다.

### 3.1 사용자 로그인




[그림 7] SSL 핸드 쉐이크 프로토콜

사용자 로그인은 서버와 출판업자들 사이에 보안을 유지하기 위해 SSL 을 사용하여 연결을 해주는 부분이

다. SSL은 암호화와 진위 확인, 메세지 확인 규칙 등의 방법을 통해 송수신 경로의 보안과 안정성을 유지시켜 준다. 그림 7은 SSL 핸드 쉐이크 프로토콜의 과정이다.

### 3.2 컨텐츠 등록

컨텐츠에 대한 저자와 출판날짜, 출판업자 등 정보들을 XrML 문서로 만들어 준다. 그리고, XrML 문서는 DRM 서버에 전송되어 그 곳의 데이터 베이스에 저장되고, 출판업자의 데이터 베이스에도 저장된다. 컨텐츠는 출판업자의 데이터 베이스에 저장된다.

### 3.3 컨텐츠와 XrML의 암호화

사용자가 컨텐츠를 구매했을 때 서버는 사용자의 XrML 문서를 생성하게 되고, 이 문서를 출판업자에게 전송한다. 출판업자는 사용자의 XrML 문서를 받아 사용자가 구매하고자 한 컨텐츠를 찾아 암호화 한다. 암호화는 워터 마킹과 키 알고리즘을 이용하여 사용자의 XrML 문서와 컨텐츠를 암호화한다. 이때 특정 리더기만이 읽을 수 있도록 파일 포맷을 하여 사용자에게 전송한다.

## 4. 결론 및 향후 방향

현재 유료화 되는 컨텐츠를 관리 보호하기 위해서는 특별한 기술이 있어야 한다. 그 기술이 바로 DRM이다. 국외에서는 활발하게 개발이 진행 중이며, 국내에서는 워킹 그룹을 만들어 DRM 기술을 개발 연구하고 있다.

본 논문에서 설계한 시스템은 DRM 전체 시스템에서 DRM Publisher 시스템이다. 이 시스템은 출판자가 컨텐츠를 서버에 등록할 때와 일반 작가들이 서버에 등록할 때에도 사용할 수 있다. 그리고, 컨텐츠들을 출판사 자신의 데이터 베이스에 저장하여 서버의 부담을 줄인다. 그러나, 출판업자의 데이터 베이스가 부담이 크다는 단점이 있다. 이는 서버의 데이터 베이스에 사용자들이 많이 구매한 컨텐츠를 뽑아 저장하는 방법을 사용하여 부담을 덜 수 있다. 또, 이 시스템을 완벽하게 구현하기 위해서는 필수 요소인 컨텐츠의 추적과 확인을 보완해주는 워터 마킹에 대한 자세한 연구와 개발이 필요하다.

## 참고문헌

[1] DRM Working Group, http://www.drmkorea.org/
[2] " A tutorial on digital watermarking" Perez-Gonzalez, F. Hernandez, J.R. Security Technology, 1999. Proceedings. IEEE 33rd Annual 1999 International Carnahan Conference on , 1999 , Page(s): 286 □ 292
[3] " Digital rights management and watermarking of multimedia content for m-commerce applications" Hartung, Ramme, F. IEEE Communications Magazine Volume: 38 11 , Nov. 2000 , Page(s): 78 □ 84
[4] XrML Specifications version 1.0, http://www.xrml.org/get_XrML.asp
[5] SET and SSL: electronic payments on the Internet Sherif, M.H.; Serhrouchni, A.; Gaid, A.Y.; Farazmandnia, F. Computers and Communications, 1998. ISCC '98. Proceedings. Third IEEE Symposium on , 1998 Page(s): 353 □ 358
[6] A. Freier, P Karlton and P. Kocher: "The SSL Protocol, version 3.0, Internet Draft,". March 1996, http://home.netscape.com/eng/ssl3/ssl-toc.html