

DRM시스템에서 Publisher 시스템의 설계

장우영⁰ 신용탁 신동일 신동규
세종대학교 컴퓨터 공학과

{ouyoung, yongtak, dshin, dkshin}@gce.sejong.ac.kr

Design of Publisher System to DRM System

Woo-Young Jang⁰ Yong-Tak Dong-il Shin Dong-Kyoo Shin
Dept. of Computer Engineering, Sejong University

요 약

인터넷 사용의 보편화로 사이버 공간이 날로 확장하고 있다. 테이프나 CD로 즐기던 음악을 PC 또는 전용 플레이어 이용해 MP3파일로 듣기도 하고 굳이 영화관에 가지 않고도 인터넷으로 영화와 비디오를 감상하는 시대가 이미 열렸다. 또한 최근에는 파일형태로 공급되는 전자 북(E-book)이 등장해 종이 책 시장을 넘보고 있다. 그러나, 디지털 콘텐츠들은 쉽고 간편하게 원본과 똑같은 품질로 복제할 수 있을 뿐만 아니라 상상을 초월하는 빠른 속도로 이동이 가능하여 사용자들이 불법으로 얼마든지 이용할 수 있다. 현재 국내외에서 이러한 문제를 해결하기 위해 제안한 기술로 디지털 콘텐츠를 보호하고 관리할 수 있도록 하는 DRM(Digital Rights Management)이라는 시스템들이 제안되어 계속적으로 개발되고 있다[1]. 디지털 콘텐츠를 보호하고 저작권을 관리하는 시스템인 DRM에는 크게 세 가지의 기본 시스템(Publisher Customer, DRM Server System)이 있다. 본 논문에서는 콘텐츠를 등록하고 저작권자가 그 콘텐츠를 관리하는 Publisher System을 키 알고리즘을 이용하여 설계한다.

1. 서 론

심에서 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 콘텐츠에 대해 저작권자를 보호해야 하는 상황은 반드시 올 것이다. 이러한 조치로서 디지털 콘텐츠를 관리하고 저작권자를 보호해주는 DRM시스템이 개발하고 있으며, 상용화 하고 있다.

디지털 콘텐츠의 불법사용방지 및 저작권 보호를 위한 기술로 유일하게 주목 받고 있는 최신 기술로 DRM(Digital Rights Management) 기술이 있다. 이 DRM 기술은 신뢰성 있는 라이선스, 안전한 저작권과 허가, 신뢰성 있는 환경과 인프라를 가능하게 하는 하드웨어와 소프트웨어를 포함하는 디지털 저작권 관리를 위한 넓은 의미의 기술이다. DRM 기술에는 관리하고 복제를 방지하기 위한 많은 기술들이 포함되어 있다. 여기에는 많이 사용되는 워터마킹이 있으며, 이것은 저작권을 추적하고 복제를 방지하기 위해 사용되는 기술이다[2]. 또한, 키 알고리즘을 이용해 사용자의 인증을 하는 기술이 있다. 그러나, 이 기술은 초기 단계이고, 이런DRM을 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. Publisher System은 저작권자가 콘텐츠를 등록하고 자신의 콘텐츠를 관리하는 것이며, Customer System은 콘텐츠를 구입하여 특정 리더기를 이용하여 보고, 읽고, 들을 수 있는 것이다. 마지막으로 DRM Server System은 등록된 콘텐츠를 보호하고, 관리하고, 소비자들에게 콘텐츠 리스트를 제공하는 역할을 한다.

본 논문에서는 기본 시스템에서 콘텐츠를 등록하고, 관리하는 Publisher System을 설계한다. 이는 키 알고리즘과 통신 프로토콜인 SSL을 사용하여 저작권자의 권리와 그 콘텐츠를 보호하며 등록할 수 있는 시스템이다. 먼저, DRM이란 기술은 무엇이며, 어떠한 구조를 갖는가에 대해 설명하며, 여기에 사용되는 키 알고리즘에 설명한다. 그리고, 저작권 언어로 XrML에 대한 설명을 하며, 마지막으로 본 논문에서 제시하게 되는 Publisher System을 설명한다.

2 관련연구

2.1 DRM(Digital Rights Management)

먼저 DRM의 정의를 내리면, 암호화 기술을 이용하여 허가되지 않은 사용자로부터 디지털 콘텐츠를 안전하게 보호함으로써 콘텐츠 저작권 관련 당사자의 권리 및 이익을 지속적으로 보호 및 관리하는 시스템으로 정의할 수

있다. 즉, 디지털 콘텐츠가 저작자 및 유통업자의 의도에 따라 전자상거래를 통해서 안전하고 편리하게 유통업자의 의도에 따라 전자상거래를 통해서 안전하고 편리하게 유통될 수 있도록 제공되는 모든 기술과 서비스 절차를 포함하는 개념이다. 다음 그림 1은 DRM을 이용하여 디지털 콘텐츠가 유통되는 전체 과정을 보여준다.

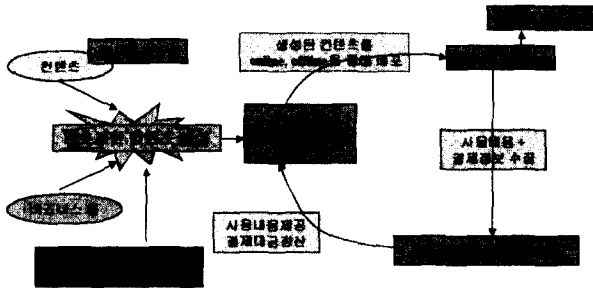


그림 1 DRM 전체 구조

위와 같은 웹 상에서의 유통과정을 가지고 있기 때문에 웹의 취약점인 보안이 중요하다. DRM 기술에는 웹의 취약점을 보완하기 위한 필수적인 보안 요소가 있는데, 첫 번째는 콘텐츠의 내용을 알 수 없게 암호화하는 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 콘텐츠를 추적하고 확인하는 Identification과 tracing이다[3].

2.2 SSL(Secure Socket Layer)

SSL은 넷스케이프에서 개발한 보안 프로토콜로 전송 프로토콜 위에서 송수신자사이의 통신의 비밀성과 데이터 무결성 제공을 목적으로 한다. SSL 최신 버전은 SSL3.0이며 SSL3.0을 기반으로 TLS(Transport Layer Security) 프로토콜 표준화가 발표되었다. 웹 서버에서 SSL을 채택하고 있는 이유는 사용자가 특별한 프로그램을 다운로드 받지 않아도 일반적으로 많이 사용하는 넷스케이프와 익스플로러가 자동으로 보안 채널을 맺어주기 때문이다.

SSL Handshake Protocol	SSL Change Cipher Spec Protocol	SSL Alert Protocol	HTTP
SSL Record Protocol			
TCP			
IP			

그림 2 SSL 프로토콜 구조

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

SSL 규약은 서버와 클라이언트의 진위 확인을 하도록

해 주며, 사용하는 어플리케이션에 대해 독립적이어서 HTTP나, FTP, Telnet 등의 어플리케이션이 SSL을 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, 메시지 확인 규칙 등의 방법을 통해 송수신 경로의 보안과 안정성을 유지시켜 준다[5].

2.3 XrML(Extensible rights Markup Language)

ContentGaurd사에서 Xerox의 DPRL 2.0을 바탕으로 만든 XML 기반의 디지털 권리 마크업 언어이다. 현재 W3C에 제안한 상태이며, 상거래 모델에 따른 권리, 요금, 조건부가 등 권리에 관련된 내용을 XML 표현 방식을 통해 정의한 언어이다.

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

```

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

그림 3 XrML 최상위 구조

루트 요소 XrML안에서는, 명령 요소 BODY와 임의 요소 SIGNATURE가 있다. 후자는 원본 자체를 보증하는데 사용된 전자의 디지털 서명이다. BODY요소는 디지털 작업의 임의 묘사와 XrML문서에 관한 임의 메타 정보로 구성되어 있고, 요소 TIME은 XrML문서가 유효한 시간 범위를 나타낸다. 요소 ISSUED는 이 문서가 발생된 시간을 나타내고, 요소 DESCRIPTOR는 이 문서의 설명을 나타낸다. 요소 ISSUER은 이 XrML문서를 작성하는 주요 요소이고, 요소 ISSUED PRINCIPALS는 이 문서가 일으키는 주요 목록이다. 요소 WORK은 디지털 작업과 사용 권리들을 정의한다. 요소 AUTHENTICATEDDATA는 이 XrML문서를 처리하는 응용프로그램에게 제공되는 데이터를 포함한다.

XrML은 디지털 작업과 DPRL버전에서 사용되는 방법과 비슷한 사용권리를 묘사한다. Work를 정의하는 전반적인 구조에 대한 설명은 참고 문헌 [4]에 자세히 설명

되어 있다.

3. Publisher 시스템의 설계

전체 구조를 설명하기 전에 본 논문에서 선택한 DRM 시스템의 모델은 그림 4와 같다.

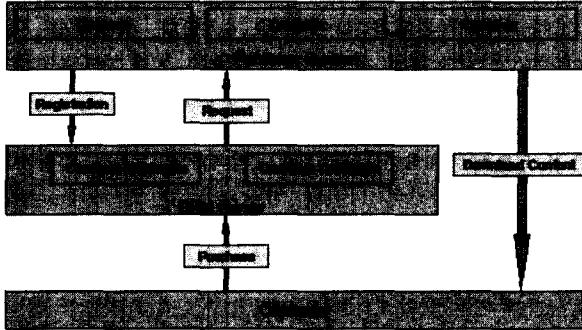


그림 4 DRM 시스템 모델

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

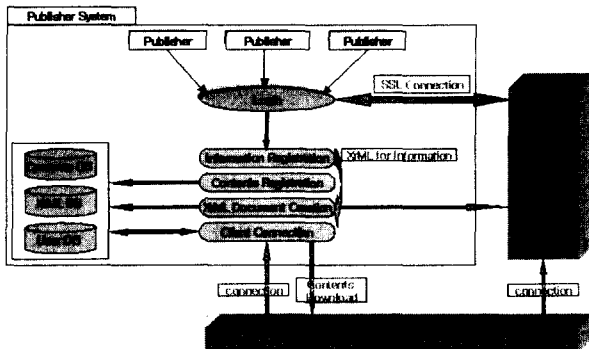


그림 5 Publisher 시스템 전체 구조

그림 5은 publisher 시스템의 전체 구조를 보여준다. 여기서 Publisher는 DRM server에 등록(회원 가입)된 조건을 전제로 한다. 먼저 Publisher는 로그인을 통해 DRM Server에 연결되고, 연결되면서 서로간의 인증을 위해 SSL을 사용하여 보안 연결이 된다. 그리고, Information Registration에서 등록하게 될 콘텐츠의 정보인 저자, 출판일, 출판사, 가격 등을 입력하고, 이를 기반으로 DOM 파서를 이용하여 XrML 문서를 생성하여, 콘텐츠와 생성된 XrML문서를 데이터 베이스에 각각 저장한다. 콘텐츠는 워터마킹을 추적과 확인을 위해 사용하게 한다[2].

4. 결론 및 향후 방향

현재 유료화 되어 가고 있는 이러한 콘텐츠를 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 시스템 중에서 Publisher 시스템이다. 이 시스템은 출판자가 콘텐츠를 서버에 등록할 때와 일반 작가들이 서버에 등록할 때에도 사용할 수 있다. 그리고, 콘텐츠들을 출판사 자신의 데이터 베이스에 저장하여 서버의 부담을 줄인다. 이 시스템을 완벽하게 구현하기 위해서는 필수 요소인 콘텐츠의 추적과 확인을 보완해주는 워터마킹에 대한 자세한 연구와 개발이 필요하다.

참고문헌

[1] DRM Working Group, <http://www.drmmkorea.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>