1. 서론

상식에서 냉스터의 행동은 위법이니 중지하라는 괴롭기도 나오면서 국내에서도 저작권에 대한 보호를 위해 여러 조치들을 취하고 있다. 그 예로 소프트웨어 등에 담긴 허수어와 관련된 저작권을 보호하려는 사례들은 관광객으로도-warning, 이사라도 그런 고정관념이 못상에 상당히 많음을 드러내고 있는 실정이다. 이러한 사례로서 디지털 컨텐츠의 유통 및 저작권 보호를 위한 DRM(Digital Rights Management)을 개발하고 있으며, 상용화하고 있다.

디지털 컨텐츠의 불법사용방지 및 저작권 보호를 위한 기술로서 유일하게 주목 받고 있는 최신 기술로 DRM(Digital Rights Management) 기술이 있다. 이 DRM 기술은 신뢰성 있는 라이선스, 안전한 저작권과 허가, 신뢰성이 있는 접근을 가능하게 하는 하드웨어와 소프트웨어를 포함하는 디지털 저작권을 위한 네트워크 기술이다. DRM 기술은 관리하고 복제를 방지하기 위해 많은 기술들이 포함되어있다. 여기에는 많이 사용되는 저작권이 있으며, 이것은 저작권을 수작하고 복제를 방지하기 위해 사용되는 기술이었다. 또한, 이 기술을 이용해 사용자와 인터넷을 하는 기술이다. 그러나, 이 기술은 초기 단계이고, 이런DRM은 연구하기 위해 여러 형식 그룹(MPEG, SDMI, EBU, OeB)에서 자체적으로 스택을 개발하고 있다.[3].

DRM 시스템에서는 크게 세 가지의 기존 시스템(Publisher, Customer, DRM Server System)이 있다. Publisher System은 저작권자가 컨텐츠를 등록하고 자 신의 권리를 관리하는 것이며, Customer System은 컨텐츠를 구입하여 특정 구성요소를 이용하여 보고, 읽을 수 있는 것이다. 마지막으로 DRM Server System은 등록된 컨텐츠를 보호하고 관리하고, 소비자들에게 컨텐츠 런크를 제공하는 역할을 한다.

본 논문에서는 기본 DRM 시스템에서 컨텐츠를 등록하고, 관리하는 Publisher System을 설계한다. 이는 기 알고리즘과 통신 프로토콜인 SSL을 사용하여 저작권자와 권리가 그 권리를 보호하며 인터넷 등록할 수 있는 시스템이다. 먼저, DRM시작 기술은 무엇이, 어떠한 구조를 갖는가에 대해 설명하며, 여기에 사용되는 기 알고리즘에 설명 한다. 그리고, 저작권 인증로 X.509에 대한 설명을 하며, 마지막으로 본 논문에서 제시하게 되는 Publisher System을 설명한다.

2. 관련연구

2.1 DRM(Digital Rights Management) 시스템의 정의를 내리면, 암호화 기술을 이용하여 허가되지 않은 이용자가 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 관리하게 유통업자의 의도에 따라 전자상거래를 통해서 안전하고 관리하게 유통될 수 있도록 제공되는 모든 기술과 서비스 절차 등을 포함하는 개념이다. 다음 그림 1은 DRM을 이용하여 디지털 컨텐츠가 유통되는 전체 과정을 보여준다.

![그림 1 DRM 전체 구조](image)

위와 같은 페의 유통과정을 가지고 있기 때문에 때의 취약점이 보안이 중요하다. DRM 기술에는 빠른 가격력에 보안된 페노미나 보안 요소가 있는데, 첫 번째는 컨텐츠의 보안을 나누게 되는 암호화 (Encryption)이며, 두 번째는 악수나 접근할 수 없게 하는 접근 제한(Conditional access), 세 번째는 필터링으로 페제를 하지 못하게 하는 페제 제어(Copy Control), 페제 되었을 때 그 복제된 컨텐츠를 추적하고 확인하는 Identification과 tracing이다. [3]

2.2 SSL(Secure Socket Layer)

SSL은 넷스케이프에서 개발한 보안 프로토콜로 전송 프로토콜에서 통신자 사이의 통신의 비밀성과 데이터 무결성을 제공을 목적으로 한다. SSL 빠른 버전은 SSLv3.0이며 SSLv3.0을 기반으로 TLS(Transport Layer Security) 프로토콜 표준화가 발표되었다. 페 서버에서 SSL을 제공하고 있는 기기의의 특별한 프로그램을 다운로드 받지 않아도 일반적으로 많이 사용하는 넷스케이프와 인스톨러가 자동으로 보안 채널을 맺어주는 기 때문이다.

<table>
<thead>
<tr>
<th>SSL Handshake Protocol</th>
<th>SSL Change Cipher Spec Protocol</th>
<th>TLS Alert Protocol</th>
<th>HTTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Record Protocol</td>
<td>TOP</td>
<td>IP</td>
<td></td>
</tr>
</tbody>
</table>

그림 2 SSL 프로토콜 구조

그림 2는 SSL 프로토콜의 구조이다. 이는 크게 페드에이크 프로토콜과 메르크로 프로토콜로 되어 있고, 페드에이크 프로토콜은 다시 Change cipher spec protocol, Alert Protocol, 페드에이크 프로토콜로 나뉘어진다. [6] SSL 구축은 서버와 클라이언트의 전위 확인을 하도록 하며, 사용하는 암호기반에 대해 독립적이어서 HTTP나, FTP, Telnet 등의 암호기반은 SSL을 기본으로 운용되도록 할 수 있다. 또한 암호화 기(cryption key)와 관련된 혼란을 할 수 있을 뿐 아니라 상위의 응용 프로그램이 정보를 서버와 콘텐츠에서 사용하기 전에 서버의 전위를 확인해 줄 수 있다. 암호화와 전위 확인, 응용 기반의 페제의 범위를 통해 송수신 경로의 보안과 안정성을 유지시켜 준다. [5]

2.3 XrML(Extensible rights Markup Language)

ContentGuard 사에서 Xerox의 DPRP 2.0을 바탕으로 만든 XML 기반의 디지털 권리 방식 언어이다. 현재 W3C에 제안된 상태이며, 상거래 모델에 따른 권리, 요금, 조건귀가 등 권리에 관련된 내용을 XML 표현 방식을 통해 정의한 언어이다. XrML의 기본 구조로 할 수 있는 최상위 구조는 그림 3과 같다.

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

그림 3 XrML 최상위 구조

루트 요소 XrML 안에서는, 병렬 요소 BODY와 일의 요소 SIGNATURE가 있다. 후자는 보안 자체를 보존하려는 사람이 보존에서의 디지털 서명매는 BODY요소는 디지털 작업의 일의 요소와 XrML문서에 대한 일의 메타 정보로 구성되어 있고, 요소 TIME는 XrML문서가 유효한 시간 범위를 나타낸다. 요소 ISSUED는 이 문서가 발행된 시간을 나타내고, 요소 DESCRIPTOR는 이 문서의 설명을 나타낸다. 요소 ISSUER는 이 XrML문서를 작성하는 주요 요소이고, 요소 ISSUEDPRINCIPALS는 이 문서가 유효한 주요 주제이며, 요소 WORK는 저작물과 사용 권리를 정의한다. 요소 AUTHENTICATEDDATA는 이 XrML문서를 적용하는 응용프로그램에 제공되는 데이터를 포함한다.

3. Publisher 시스템의 설계

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

![그림 4 DRM 시스템 모델](image)

출판자가 DRM 시비에 등록을 하고 권한주는 자신의 데이터베이스에 저장한다. 서비스는 출판자가 등록한 권한과의 리스토를 작성하여 사용자에게 보여준다. 사용자는 서비스로부터 리스토를 보고 구매를 하게 되고 서비스는 사용자가 선택한 권한을 출판자에게 요청을 하게 된다. 출판자는 요청 받은 권한을 직접 사용자에게 다운로드하게 되는 모델을 갖는다.

4. 결론 및 향후 방향

현재 유료화 되어 가지고 있는 이러한 권한을 관리 보호하기 위해서는 독특한 기술이 있어야 한다. 그 기술이 바로 DRM이다. 국외에서는 활발하게 개발이 진행 중이며, 국내에서는 워킹 그룹을 만들어 DRM 기술을 개발 연구하고 있다.

본 논문에서 설명한 시스템은 DRM 전제 시스템 중에서 Publisher 시스템이다. 이 시스템은 출판자가 권한과를 서비에 등록할 때와 일반 작가들이 서비에 등록할 때에도 사용할 수 있다. 그러므로 권한을 출판자 자신의 데이터베이스에 저장하여 서비의 부담을 줄인다. 이 시스템을 완벽하게 구현하기 위해서는 필수 요소인 권한과의 추적과 확인을 보완해주는 위협이에 대한 자세한 연구와 개발이 필요하다.

참고문헌


[2] A tutorial on digital watermarking

[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

http://www.xrml.org/get_XrML.asp
