情 報 保 護 學 會 誌
第 11 券 第 5 號, 2001. 10

DRM 기술 및 제품 동향 분석

전 종 민*, 최 영 철*, 박 상 준*, 박 성 준*

요 약

DRM은 디지털 창작물에 대한 저작권을 보호하기 위한 기술로서, 컨텐츠가 출판되어 유통되고 사용되기까지의 전 과정에 대한 일련의 보호 및 관리 체계를 의미한다. 컨텐츠 시장이 활성화되기 시작함에 따라 DRM 기술에 많은 관심이 집중되고 있으며 IBM, Microsoft 등의 거대기업들도 시장에 진입하고 있다. 본 논문은 컨텐츠를 '보호'하는 보안기술의 측면에 입각하여 DRM 기술에 관하여 개략적으로 설명하고, 국내·외 시장에 제품을 출시한 업체들을 소개한다. 또한 DRM 시스템이 제공해야하는 기능 요구사항들을 요약하고, 지금까지 출시된 국내·외 주요 제품들의 특성을 간략히 분석해 본다.

Ⅰ. 서 론

초고속 인터넷 인프라가 보편화되면서 다양한 형태의 멀티미디어 컨텐츠 유통이 점차 활성화되고 있다. 영화, 음악, 도서 등 많은 수요층을 확보하고 있는 주요 오락컨텐츠뿐 아니라 조직의 정보자산, 도서관, 지리정보, 게임 등 생활 구석구석에서 부딪치는 수많은 컨텐츠들이 디지털 형태로 서비스되는 이른바 디지털 컨텐츠 시대가 도래하고 있다.

DRM은 이러한 디지털 자산에 대한 권리를 안전하게 보호하고 체계적으로 관리하기 위한 기술적인 매커니즘으로, 그림 1과 같이 다양한 응용분야에 적용되어 컨텐츠 거래/유통 인프라를 제공하게 될 것이다. 디지털 컨텐츠 시장에 대한 잠재력은 아직 소비시장이 채 형성되지 않은 현실에도 불구하고 많은 관심과 투자를 유도하고 있으며, DRM은 불법복제 문제를 해결하여 컨텐츠 시장이 성장의 성장을 유도할 것으로 기대하고 있다.

본 고에서는 DRM 시스템에 적용되는 보호기술과 그 제품들에 대하여 중점적으로 논하고자 한다.

* (주)비씨큐어 암호기술연구소
{jjmin, ycchoi, sangjoon, sjpark}@BCQRE.com

Ⅱ. DRM 기술 개요

DRM은 여러 가지 기술들이 조합되어 이루어지는 커다란 개념이며 다음과 같이 저작권 '관리기술'과 저작권 '보호기술'로 구별될 수 있다.

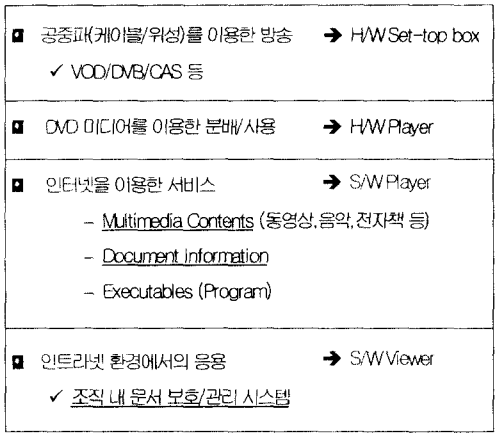
1. 저작권 관리 기술

저작권 관리 기술은 범세계적으로 통일된 일 련의 디지털 저작물 관리체계를 마련하기 위한 것으로, 저작권 관련 단체들을 중심으로 다음과 같은 기술 표준화 작업이 진행중이며, 관련 제품들도 출시되고 있다.

1.1 컨텐츠 식별자 (DOI[1])

IDF[2]에 의해 추진되고 있는 디지털 컨텐츠 식별체계 표준화 작업이다. 등록되는 모든 디지털 저작물에 유일한 식별자를 부여하기 위한 식별 및 등록체계를 정의하고, 부여된 식별자에 의한 접근의 용이성을 보장하기 위한 검색기능, DOI-IP 자동 변환기능[3] 등을 제공한다[1].

1) Digital Object Identifier
2) International DOI Foundation
3) 도메인 이름체계와 같이 등록된 저작물에 대한 DOI를 IP주소로 자동으로 변환해주는 체계.



〔그림 1〕 DRM기술 적용분야

1.2 컨텐츠 메타데이터(INDECS)[4]

유럽을 중심으로 한 저작권 단체들이 주도하는 디지털 컨텐츠의 메타데이터를 정의하는 표준화 작업으로, 저작물정보, 저작자정보, 저작권자 정보, 권리운용정보로 구별하여 컨텐츠의 메타데이터를 정의한다. INDECS는 DOI를 지원하며, 현재 표준화 작업중인 MPEG21은 DOI와 INDECS를 모두 수용할 것으로 보인다[2].

1.3 컨텐츠 권리명세언어

컨텐츠의 메타데이터를 표현하는 권리명세언어는 ContentsGuard사가 개발한 XrML[5][3]을 비롯하여 ODRL[6], XACML[7] 등이 있으며, 모두 확장성을 제공하는 XML 형식이다. 현재 W3C, MPEG21등의 주요 표준기구에서는 이들 중 하나 또는 복수개의 권리명세언어를 표준 언어로 채택하기위한 심사작업이 진행 중이다.

2. 저작권 보호기술

저작권 보호기술은 관리기술에서 정의하는 일련의 원칙과 시나리오들을 강제화(Enforcement)하는 기술로 이해할 수 있다. 시장에 등장한 대부분의 DRM제품들은 저작권 보호기술을 상품화한 것이며, 주요 업체들은 자사의 솔루션에 표준화 작업이 진행되고 있는 표준 관리기술을 수용하려는 노력을 기울이고 있다. 안전한 저작권 보호기술을 위해서 다음과 같은 세부기술들이 요구된다.

2.1 암호 요소기술

컨텐츠 인증, 컨텐츠 사용자 인증, 거래 및 사용규칙 강제화, 거래 및 사용내용 확인(부인방지) 기능 등을 위하여 암호화, 전자서명, 그리고 이에 필요한 인증 및 키 분배 기술 등 다양한 암호 요소기술들이 사용된다. 컨텐츠는 출판되기 이전에 패키징 과정을 통해 안전한 형태로 보호된다. 패키징된 데이터는 컨텐츠와 메타데이터, 그리고 컨텐츠 복호화 정보를 포함하게 된다.

컨텐츠 암호화에 사용되는 키는 안전하게 보호하기 위해서 정당한 사용자(의 시스템)만이 접근 가능하도록 가공하여 컨텐츠 복호화 정보를 생성한다. 메타데이터에는 컨텐츠 유통 및 사용에 관한 비즈니스 규칙이 설정되어 있고 이 규칙 또한 위·변조될 수 없도록 암호학적으로 보호된다.

2.2 키 분배 및 관리

컨텐츠 보호를 위해 사용되는 암호기술들의 안전성을 보장하기 위해서는 안전한 키 관리 및 분배 매커니즘이 필요하다. DRM에서의 키 관리가 다른 암호시스템의 키 관리와 구별되는 가장 큰 특징은 사용자[8] 자신도 자신의 키를 알 수 없도록 관리되어야 한다는 점이다. 만약 자신의 키에 접근할 수 있다면 알고리즘의 비밀성이 보장되지 않는 한 컨텐츠 원본을 뽑아내서 복제할 수 있기 때문이다.

DRM 키 분배 방법은 대칭키 방식과 공개키 방식으로 구별될 수 있다. 대칭키 방식은 하나의 키 분배 서버로 모든 부하가 집중되고 모든 컨텐츠 거래에 키 분배 서버가 관여해야한다. 반면 공개키 방식을 사용할 경우 분산성, 확장성, 상호운용성 등에서 많은 장점을 갖게되나, 공개키기반구조(PKI)가 필요하다는 부담이 있다. 그러므로, 컨텐츠의 특성 및 적용 환경에 따라 적절한 키 관리 매커니즘을 선

4) Interoperability of Data in ECommerce Systems
5) Extensible Rights Markup Language
6) Open Digital Rights Language
7) Extensible Access Control Markup Language.

8) 사용자란 컨텐츠가 패키징된 이후 소비자에게 전달되는 과정에 참여하는 유통업자, 분배자, 소비자 등의 모든 역할개체들을 의미한다.

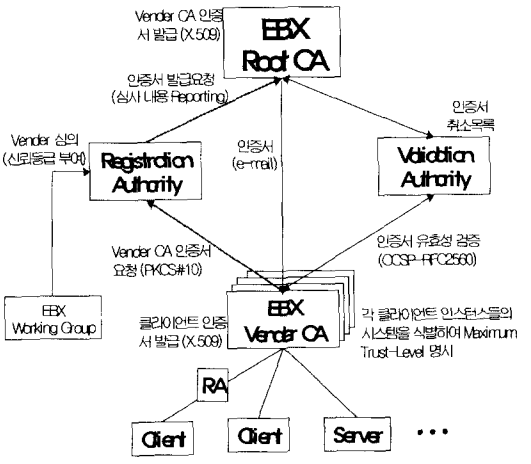
택하는 것이 바람직하다. 예를 들어 전자책, 음악 등과 같이 컨텐츠 유통 범위가 광범위하고 컨텐츠 유통 흐름에 많은 역할 개체들이 참여하는 경우, 하나의 키 분배 서버로 부하가 집중되는 키 관리 매커니즘은 적절하지 못하다.

EBX[9][4]는 전자책 교환시스템 표준에서 [그림 1]과 같은 방법으로 PKI를 적용하였다. 적용된 PKI 시스템은 앞서 언급한 바와 같이, 인증서 발급 시 자신의 개인키가 시스템으로 안전하게 저장되어 사용자들 자신도 개인키에 접근할 수 없도록 설계된다.

2.3 TRM[10]

컨텐츠 보호를 어렵게 하는 요인은 컨텐츠가 사용되는 어떤 순간에 반드시 복호화 되어야한다는 점이다. 컨텐츠를 가공하거나 사용하는 과정에서 컨텐츠 복호화키 또는 복호화된 컨텐츠가 사용자에게 노출될 수 있다면, 암호기술을 깨지 않고도 보호되지 않은 컨텐츠를 얻어낼 수 있게된다.

TRM은 마치 블랙박스와 같이 세부동작과정이 드러나지 않도록 숨기고, 변형을 가하면 동작하지 않도록 제작된 소프트웨어 또는 하드웨어 모듈을 의미한다. DRM에서는 컨텐츠의 권리정보, 키정보, 복호화된 컨텐츠 등을 다루는 모듈에 TRM 기술을 적용하여, 디버깅 도구를 사용한 소프트웨어 역분석을 방지한다. 실제로 최근 크래킹된 Adobe사, Microsoft사의 전자책은 역분석에 의한 공격으로 추정된다. TRM 기술은 향후 DRM시스템의 안전성을 결정하는 중요한 요소기술로 자리잡을 것으로 예상된다.



[그림 2] 전자책 교환 시스템에 대한 PKI 적용 방안 (EBX 표준 Ver. 0.8)

III DRM 제품 동향

세계적으로 약 100개 이상의 업체들이 DRM관련 솔루션을 개발하였으며 국내에는 워터마킹을 제외하면 약 15개 정도의 업체가 DRM 관련 솔루션 또는 서비스를 상용화하고 있다. 본 장에서는 여러 가지 종류의 DRM 시스템들에 대하여 몇 가지 항목에 따라 분석하려고 한다. DRM 관련 주요 업체는 표 1과 같다.

1. 국외 DRM 제품 동향

국외 DRM 시장은 초반 시장 장악력에서 InterTrust가 독주하였으나, 2000년 이후부터 DRM 솔루션을 무료로 배포하기 시작한 Microsoft가 빠른 속도로 추격하고 있다. 여기에 사실상 전자책 표준으로 자리잡고 있는 PDF 포맷의 Abobe사와, XrML을 개발하여 공개한 ContentGuard 등이 e-book 분야에 사업을 확장하고 있다.

1.1 Microsoft

MS社의 DRM은 WMRM[11]과 DAS[12]가 있다. WMRM은 미디어 플레이어에 탑재되어 동영상과 음악을 지원하며, DAS는 MS e-book Reader에 탑재되어 전자책을 지원한다. WMRM은 자사의 Windows OS에 포함되어있는 윈도우미디어플레이어 버전6.4부터 이미 탑재하여 배포되었으므로, MS社의 DRM 클라이언트는 전 세계적으로 4억개가까이 설치되어있는 것으로 알려져 있다. 따라서, 사용자는 별도의 DRM클라이언트 플러그인 모듈을 설치할 필요 없이 윈도우미디어플레이어를 그대로 사용할 수 있다. WMRM은 스트리밍 서비스를 지

9) Electronic Book Exchange
10) Tamper Resistant Module
11) Window Media Rights Manager
12) Digital Asset Server

〔표 1〕 DRM 관련 업체

	社 명	제 품 명	특 징
국외	Adobe	Content Server	전자책
	Authentica	PageRecall 등	항상 온라인 사용
	Content-Guard	RightsEdge	XrML 개발/MS社와 제휴
	IBM	EMMS	-
	InterTrust	DigiBox 등	세계최초상용화
	MicroSoft	WMRM, DAS	MediaPlayer에 탑재
국내	드림인테크	e-Safer	기업문서보안
	디지캡	Digicap	-
	마크애니	SDMS 등	워터마킹기술보유
	메타라이츠	EacyWriter	XrML 편집기
	비씨큐어	CQDocument등	PKI 접목
	삼성전자	시큐맥스	자체mp3Plaier/단말기
	시큐어젠	SecurePublish	RightsMarket 기술도입
	실트로닉	RightS@fer	워터마킹기술보유
	트러스트 테크놀로지	ASP-DRM 등	InterTrust 기술도입
	파수닷컴	Fasoo DRM Service 등	InterTrust 기술도입 /DRM 서비스

원한다는 큰 강점을 갖고있으며, 특히, 음악파일의 경우 음악이 출력되기까지의 모든 경로에 전자서명을 이용하여 디바이스를 인증하는 안전한 출력패스(SAP[13])를 지원한다[5].

현재는 DRM 서버 엔진 SDK를 1년 기한으로 무료배포하고 있다. 해외에서는 이미 많은 업체들이 MS의 WMRM을 이용하여 유료방송시스템 및 영화 사이트를 구축하였으며, 국내에서는 DRM코리아와 비씨큐어 등이 WMRM을 이용한 유료 방송솔루션을 제공하고 있다.

1.2 InterTrust

세계 최초로 DRM을 상용화하여 관련 기술에 관한 많은 특허 및 노하우를 가지고 있으며, INDECS, MPEG21, W3C DRM 워킹그룹, OeBF 등 다수의 DRM 관련 표준화작업에 주도적으로 참여하고 있다. 특히 특허의 범위가 매우 광범위하여 많은 DRM관련 업체들은 InterTrust가 갖고있는 18건의 특허 범위를 벗어나서 기술을 개발을 하기 어려운 실정이다. 최근에는 MS社에 대하여 특허침해소송을 제기하여 판결 결과가 주목되고 있다.

컨텐츠는 저작권정보, 비즈니스루울, 복호화정보 등을 포함하는 Digibox라는 형태로 가공되어 보호되며, Rights Packager, Rights Server, Rights Client, Rights Toolkit 등의 컨텐츠보호 소프트웨어/하드웨어칩에서 클리어링하우스 까지 다양한 응용분야와 플랫폼에 대한 DRM 제품군을 구성하고 있다.

AOL, 필립스, 미쓰비시, 매직스, 레시프로컬 등의 업체들이 InterTrust사의 DRM 기술을 이용하여 서비스를 하고 있으며, 국내에는 파수닷컴과 트러스트테크놀로지가 기술을 도입하여 서비스 및 솔루션을 공급하고 있다. 또한 디바이스 파트너로는 컴팩, 소니, 삼성전자 등이 있으며, BMG, 블록버스터, 유니버설스튜디오의 뮤직그룹 등이 InterTrust사와 컨텐츠 파트너 관계를 맺고 있다.

현재는 연간매출 천만달러 정도의 비교적 중소업체이지만, DRM 분야에서는 잠재력을 충분히 인정받고 있는 선발주자로 평가되고 있다.

1.3 ContentGuard

2000년 Xerox社로부터 분사하여, 컨텐츠 권리명세표현언어인 XrML을 개발하고 공개하여 널리 알려진 DRM 업체이다. 공개된 XrML은 MS사를 비롯한 많은 중소 업체들이 사용하고 있으며, 국내에는 메타라이츠가 XrML 편집기를 개발하였다. MS社와는 제휴를 통해 긴밀한 유대 관계를 유지하고 있으며, MS社의 DAS 및 전자책은 XrML을 사용하였다.

Accenture, Adobe, WordPlay, Xerox 등과도 협력관계를 맺고있다.

1.4 Authentica

MailRecall, PageRecall, WebRecall 등, 다른 DRM 제품들과 차별화되는 제품들을 출시하였다. 'Recall'이라는 개념은 e-mail에 처음 적용된 것으로서, mail을 발송한 후에도 송신자가 원하지 않을 경우 수신자가 더 이상 메일을 볼 수 없도록 하는 기능에서 시작되었다.

시스템은 Policy 서버, 클라이언트의 Lease Manager와 응용 add-in 프로그램으로 구성된다. Policy Server에 등록된 사용자는 로그인한 후, 원하는 컨텐츠를 패키징하여 전송/배포하며, 사용이 허가된 수신자는 설정된 조건에 의거하여 컨텐츠를 사용한다. 소유자는 Rease Manager를 통하여 자신이 배포한 컨텐츠를

13) Secure Audio Path

관리할 수 있으며 언제든지 Recall함으로서 컨텐츠 사용을 제한할 수 있다. 시스템의 가장 큰 특징은 모든 사용권한 및 라이센스가 서버에 저장되므로 사용자는 컨텐츠를 항상 온라인으로 사용하게 된다는 점이다. Authentica의 제품은 최근, 국내에도 수입되어 판매되고 있다.

2. 국내 컨텐츠 보호 제품 동향

국내 컨텐츠 보호시장은 그 잠재적 기대효과로 인해 비교적 과열되어있는 양상이다. 과거에는 크게 워터마킹 업체와 DRM 업체로 구별되었으나, 워터마킹 업체들이 점차 DRM분야로 사업영역을 확장하고있는 추세이다.

국내 DRM시장은 크게 인터넷 환경의 컨텐츠 보호 시스템과, 인트라넷 환경의 문서보안시스템으로 나뉘어진다. 전자는 전자책, 방송/영화 등의 동영상, 그리고 음악분야 등 후자에 비해 매우 거대한 규모의 시장으로 성장할 것이 확실시되나, 아직은 디지털 컨텐츠 산업 자체의 수익기반이 갖추어지기까지 상당한 시간이 필요하며, Microsoft, InterTrust 등의 해외 업체들의 영향력에 의존적인 특성이 있다. 반면, 인트라넷 환경의 문서관리/보호 시스템은 시장규모가 비교적 작은 반면, 당장 수요가 증가하고있으며, 빌링시스템, 컨텐츠 신디케이션 등을 지원할 필요가 없어 시스템 모델이 전자에 비해 비교적 단순하기 때문에 국내의 업체들이 시장에 서둘러 진입하고 있다.

2.1 DRM 제품

다음에는 국내의 몇 가지 DRM 제품에 대하여 간략히 소개한다. 소개하는 내용은 대중매체를 통해 수집한 객관적인 사실을 토대로 하였다.

▶ 디지캡
- 국내 DRM 시장 진입 시기 빠름.
- 오디오, 동영상, 전자책 분야까지 다양한 제품 출시.
- mp3 player 등의 단말기 지원
- 최근, 워터마킹 기능을 추가하였음.

▶ 마크애니
- SDMI, STEP2000 에서 워터마킹 알고리즘 입상.
- 문서DRM 및 증명서 위조방지 시스템 출시
- 익스플러러에서 동작하는 웹 응용제품 출시

▶ 비씨큐어
- PKI를 비롯한 암호기술로 2001년 DRM시장 진입
- 전자서명 기능을 갖는 인증서 기반의 문서 DRM 시스템(*CQDoc*™) 출시
- MS의 WMRM 응용제품(*CQMedia*™) 출시 (동영상/음악)

▶ 삼성전자
- 국내 DRM 시장진입 시기 빠르며, 2001년 씨큐맥스 2.0 출시.
- 키 관리 서버를 자체 운영하고, 패키징 및 판매내역 조회기능 등을 위한 DRM CP Server 제공.
- 자체 개발한 mp3플레이어 '뮤직드라이브'에 오디오 DRM 기능이 내장되어있으며, 삼성전자의 mp3 재생 단말기에 DRM 기능 탑재

▶ 실트로닉
- 워터마킹 제품과 DRM 제품 모두 출시
- 윈도우 미디어플레이어와 WinAmp 등의 응용 프로그램 지원
- 웹상에서 마크가 삽입된 컨텐츠를 검색하는 워터마크 제품 출시

▶ 파수닷컴
- DRM 시장 진입시기 빠름. InterTrust의 기술을 도입하여 2000년 중반에 DRM 서비스 개시.
- 동영상, 음악, 만화, 문서 등 많은 종류의 패키징 툴과 응용 프로그램을 지원.
- 최근 문서DRM시스템을 출시하였으며, 자체 DRM 기술개발도 진행중인 것으로 알려짐.

2.2 워터마킹 제품

저작권 보호기술의 하나로 최근 3년 사이에 각광받기 시작한 워터마킹 기술은 알고리즘의 '안전성 검증' 문제 및 불법복제 후 '사후 추적' 기능이라는 특성으로 인해 수익모델을 찾는데 어려움을 겪고 있다.

국내에서는 마크애니, 실트로닉, 디지털이노텍 등이 워터마킹 기술 보유업체이며, 컨텐츠 코리아 등도 원천기술 도입을 통해 다양한 워터마킹 응용제품을 출시하고 있다. 최근에는, 증명서 위조방지에 적용되는 새로운 연성 워터마킹 기술이 마크애니, 컨텐츠코리아 등에 의해 상용화되고 있다. 또한, 실트로닉은 워터마크된 컨텐츠의 불법복사본을 웹에서 감시할 수 있는 제품을 출시하였으며, 컨텐츠 코리아는 디지털 컨텐츠

거래 시 구매자 정보를 실시간으로 컨텐츠에 삽입하는 핑거프린팅 제품을 발표하였다.

〔표 2〕 워터마킹 기술 적용분야

저작권증명	내용	저작권이 등록되지 않은 컨텐츠에 대한 저작권 증명
	예제	인터넷에 공개된 특종 기사의 사진.
	비고	상거래에 사용되는 컨텐츠는 사전에 저작권이 등록된다.
모니터링	내용	특정 컨텐츠에 대한 불법 복사본을 감시하기 위한 모니터링 정보
	예제	DigiMarc사의 Mark Spider (웹에서 특정 워터마킹이 삽입된 컨텐츠 검색)
	비고	검색의 효율성 문제
복사제어정보	내용	워터마크를 컨텐츠의 복사 및 사용을 제어하는 제어정보로 사용
	예제	CPTWG Data Hiding Subgroup의 워터마킹 기술 (DVD Player에 적용을 시도함 (Galuxy Group, Millenium Group)
	비고	워터마킹을 검사하지 않는 해적판에 의한 복제 문제. 안전성이 알고리즘의 비밀성에 의존.
핑거프린팅	내용	컨텐츠 판매 시 구매자 정보를 컨텐츠에 핑거프린팅하여, 불법복사본 발견 시 부정행위자 추적
	예제	실시간 구매자 정보 핑거프린팅
	비고	서로 다른 마크가 삽입된 동일 컨텐츠들에 의한 공모공격(Collusion Attack)에 대한 대책필요.
출력물복사방지	내용	fragile 워터마킹을 사진/그림 등에 삽입하여, 출력물이 복사되는 경우 워터마크가 깨지도록 함. 출력에는 강인하나 복사에는 취약한 워터마킹 알고리즘 사용.
	예제	여권, 증명서(행정문서) 등의 위/변조 방지
	비고	워터마킹 알고리즘의 안전성 검증문제(알고리즘의 비밀성에 안전성 의존, 출력물 스캔공격 등)

워터마킹 알고리즘은 표 2와 같이 다양한 기능을 제공할 수 있으나, 각각에 적용되기 위하여 해결해야 할 기술적인 문제점들도 산재해 있는 것으로 보인다.

Ⅳ DRM 시스템의 기능 분석

1. DRM 시스템의 기능(요구사항)

1.1 컨텐츠 보호/인증

컨텐츠는 암호화된 형태로 안전하게 보호되어야 하며, 구매자는 컨텐츠의 저작권자, 공급자 등의 관련정보를 확인함으로써 컨텐츠 진위여부를 인증할 수 있어야 한다.

1.2 사용자 인증

출판사와 분배자, 분배자와 소비자 등 모든 컨텐츠를 거래 당사자들간에 서로를 인증할 수 있는 신뢰서비스가 필요하다. 공급자는 수요자를 인증한 후 상대방의 비밀정보와 관련된 정보(예:공개키)로 보호된 라이센스를 내려주게 되므로, 안전한 인증 매커니즘을 사용하는 것은 DRM시스템에서 중요한 요소이다.

1.3 Usage/Business Rule 적용

컨텐츠 출판사는 컨텐츠 분배자에게 상호간의 계약에 따른 비즈니스규칙을 적용하여 제공하며, 분배자는 소비자 기호에 맞는 사용규칙을 반영하여 컨텐츠를 제공한다. 이러한 규칙들은 XrML등의 권리명세언어를 이용해 작성될 수 있으며, 안전하게 보호된 '라이센스' 형태로 제공된다. 규칙은 다양한 비즈니스모델 및 사용환경을 제공하기 위하여 융통성 있게 제공되어야 한다.

1.4 라이센스보호

컨텐츠 사용규칙 그리고(또는) 컨텐츠 복호화 정보를 포함하는 라이센스는 위/변조로부터 안전하게 보호되어야 하며, 다른 사용자에게 복사되어도 사용할 수 없어야 한다. 특히 컨텐츠 복호화 정보는 절대로 노출되지 않도록 기밀성을 유지해야 한다.

1.5 라이센스 백업기능

컨텐츠를 사용하던 특정 PC를 바꾸거나 OS를 다시 설치하는 등의 이유로 포맷할 경우, 컨텐츠에 저장된 라이센스를 백업하고 다시 로드할 수 있어야 한다. DRM 제품에 따라(MS WMRM) 새로 설치하는 경우 사용자의 DRM클라이언트의 유일한 식별자가 변경되는 경우도 있다. 어떠한 경우라도 백업된 라이센스를 다시 설치하여 사용권한을 그대로 유지할 수 있는 매커니즘이 제공되어야 한다.

1.6 하드웨어바인딩

여러 명, 또는 여러 사업자들이 하나의 컨텐츠를 공유하는 것을 막기 위하여 주어진 컨텐츠를 특정하드웨

어에서만 동작하도록 하드웨어정보에 바인딩하는 것이 필요하다. 특히, 아이디와 패스워드로 사용자를 인증하는 시스템의 경우, 패스워드를 공유함으로써 컨텐츠를 대량으로 분배하는 것을 방지해야 한다. 동시에 사용의 편의성을 위해 한 곳 이외의 장소에서 컨텐츠를 사용할 수 있도록 시스템은 적절한 하드웨어 바인딩 정책을 지원해야 한다. 이러한 매커니즘은 주로 라이센스를 특정 하드웨어에서만 유효하도록 하는 방법을 사용한다.

1.7 클리어링하우스

컨텐츠 판매 및 사용내역을 확인하여, 소유권에 관한 금전적인 관계를 정산하고, 컨텐츠 비즈니스에 필요한 통계자료를 확보하는 기능을 제공한다. 컨텐츠 제공과정에 연관된 역할 개체들 간의 Value Chain을 지원하여 저작권에 관한 투명한 정산을 집행할 수 있어야 하며, 지불시스템과도 연동되어야 한다. 문서관리 DRM의 경우, 사용자들의 컨텐츠 사용내역을 관리자가 모니터링할 수 있는 인터페이스가 제공될 수 있다.

1.8 휴대용 단말기 지원

많은 멀티미디어 컨텐츠들이 mp3 재생, 동영상 재생기능을 갖춘 휴대용 단말기에서 사용된다. DRM기능은 단말기에 전송되어도 그대로 적용될 수 있어야 하며, 단말기 모듈은 낮은 연산능력으로도 효율적으로 작동할 수 있어야 한다.

1.9 Super-Distribution

사용자들 간에도 컨텐츠 분배가 일어날 수 있어야 한다. 예를 들어, 사용자A가 구매한 컨텐츠를 사용자B에게 전달했을 경우 사용자B도 컨텐츠 사용비용을 지불한 후 컨텐츠를 사용할 수 있고 다시 사용자C에게 전달할 수 있다. 또한, 사용자들간의 컨텐츠 빌려주기, 주기 등의 기능을 제공하는 것도 고려되어야할 사항이다. Super- Distribution이 발생할 경우 컨텐츠 내용은 그대로 사용하고 복호화 정보를 포함하는 라이센스의 내용만 변경된다.

2. DRM 시스템의 특성 분류

DRM 시스템들은 다음과 같은 기준에 따라 몇 가지 방식들로 구별된다. 각 방식의 시스템들은 장·단점들을 갖고있으며 적용 환경에 따라 적절히 선택될 수 있다.

2.1 온라인 사용방식과 오프라인 사용방식

동영상 스트리밍 서비스를 제외한 대부분의 DRM 시스템은 컨텐츠에 대한 라이센스를 얻은 이후에는 오프라인으로 사용할 수 있도록 지원한다. 그러나, 매번 컨텐츠를 사용할 때마다 온라인으로 연결하여 사용하는 온라인 사용방식도 있다. 온라인을 보장하지 않아도 되는 오프라인 사용방식이 더 일반적인 시스템이라 할 수 있지만, 온라인 사용방식은 항상 인터넷에 연결되어있다는 조건만 만족한다면 몇 가지 장점을 가질 수 있다.

우선, 컨텐츠 사용규칙 및 복호화 정보 등 컨텐츠에 관한 많은 정보들이 서버에 저장·관리될 수 있다. 이 경우, 컨텐츠 사용규칙을 언제든 동적으로 변경하여 사용권을 제어할 수 있어 융통성이 향상된다. 또한, 전체적인 시스템의 구조가 단순해지며, 라이센스 처리에 관한 클라이언트 모듈의 구현도 간단해질 수 있다. 그러나, 온라인 환경을 항상 보장하는 것은 긴급한 상황 등에서 컨텐츠의 가용성을 완전히 보장하기 어렵다. 따라서, 온라인 사용방식은 오프라인 사용방식과 적절한 조화를 이루어 사용될 수 있을 것이며, 특히, 비교적 온라인 환경이 잘 보장되는 문서관리 DRM의 경우에 유용하게 적용될 수 있다.

2.2 라이센스와 키분배

패키징된 컨텐츠를 사용하기 위해서는 컨텐츠 복호화 정보가 필요하다. 세부적인 매커니즘은 시스템마다 다르지만, 대체로 라이센스는 컨텐츠 복호화정보 또는 이와 관련된 정보를 포함한다. DRM 시스템은 컨텐츠 패키징 시, 라이센스를 컨텐츠에 포함하여 전달하는 방식과 라이센스를 독립적으로 분리

〔표 3〕 DRM 제품 특성 비교

비교항목 / 업체명	사용자 설치모듈	라이센스 형태/위치	라이센스 백업	H/B	단말기 지원	S/D	동적인 권한변경	TRM	키분배 (추정)	지원 응용 프로그램	특징
Microsoft	없음	컨텐츠와 분리	○	○	○	○	×	○	공개키	동영상/음악/전자책 (MediaPlayer, e-book Reader)	무료, 스트리밍
InterTrust	Enabler, 응용	컨텐츠에 포함	○	○	○	○	○	○	공개키/대칭키	동영상/음악/문서 등 많은 응용 지원	
Authentica	Lease Manager, 응용	컨텐츠와 분리(서버)	○	×	×	-	○	?	공개키	Explorer, 메일, Acrobat 등	온라인 사용
디지캡	토큰매니저, 응용	컨텐츠에 포함	?	○	○	?	×	×	대칭키	MediaPlayer, Winamp 등	워터마킹
마크애니	Viewer	컨텐츠에 포함	○	○	사례 없음	-	×	×	대칭키	문서 (MS-Office, Univiewer 등)	워터마킹
시큐맥스	응용	컨텐츠에 포함	○	○	○	○	×	×	대칭키	음악(자체 Player)	단말기
실트로닉	응용	컨텐츠에 포함	?	○	사례 없음	○	×	×	공개키	MediaPlayer, Winamp 등	워터마킹
비씨큐어	CQAgent, 응용	컨텐츠와 분리	○	○	사례 없음	-	○	○	공개키/대칭키	MediaPlayer, MS-Office 등	PKI
파수닷컴	Enabler, 응용	컨텐츠에 포함	○	○	사례 없음	○	○	?	사전 분배	동영상/음악/문서/만화/전자책 등	클리어링 하우스

하여, 컨텐츠 사용요청 시 지불 과정을 거쳐 따로 전달하는 방식으로 구별될 수 있다. 전자의 경우, 컨텐츠가 컨텐츠 사용자에게 다운로드될 때 동적으로 라이센스를 포함하여 전달하게 되어, 이후 DRM 서버와 더 이상의 트랜잭션 없이 컨텐츠를 사용하게 된다. 반면 후자의 경우 패키징된 컨텐츠는 누구에게나 똑같은 형태로 제공되고, 컨텐츠 사용요청 시 라이센스 발급을 위한 별도의 트랜잭션이 요구된다.[14]

암호 매커니즘으로 보면, 라이센스가 전달되는 과정에서 사용자 인증 및 키 분배가 발생하게 되며, 여기에 사용되는 인증 및 키 분배 방식에 따라 대칭키 방식과 공개키 방식으로 구분된다. 만약 사전 키 분배 방식을 사용한다면 컨텐츠 복호화 정보가 항상 클라이언트에 준비되어있는 경우이며, 키 분배 부담을 덜어낼 수 있어 효율성, 융통성에 큰 장점을 갖게되나 안전성 측면에서 사전에 분배된 키에 대한 보호문제가 중요한 관건이 된다.

DRM에 PKI를 적용한 제품으로 MS사의 WMRM이 있다. 각각의 서버 또는 클라이언트 인스턴스들은 Indivisualization 과정을 통해 키 쌍을 할당받게되며, 크래킹되었거나 안전하지 않다고 판단되는 인스턴스들에 대해서는 인증서 취소목록을 유지하여 서비스 대상에서 제외시키게 된다. 인증서 취소목록은 MS의 웹사이트를 통해 배포된다.

14) MS사의 WMRM이 후자의 방식을 사용한다.

V. 상용 제품들의 특성 비교

현재 상용화되어있는 DRM 제품들에 대하여 앞서 언급한 여러 가지 특성에 따라 〔표 3〕에 정리하였다. 정리된 내용은 레퍼런스 사이트를 통한 직접 테스트, 제품 전시회를 통한 간접 테스트, 업체의 인터넷 사이트를 통한 정보수집, 그리고 해당 업체에 문의한 결과를 토대로 하였다. 제품별 버전 등 테스트 시기 차이로 인해 향상된 기능이 반영되지 못했을 수도 있다. 비교항목의 H/B는 하드웨어바인딩 기능, S/D는 Super-Distribution기능, 그리고 TRM은 TRM 기술 적용 여부를 각각 의미한다.

VI. 결 론

DRM 기술은 수면위로 떠오른 지 아직 몇 년이 채 지나지 않았지만, 향후 시장성에 대한 잠재적 가능성 때문에 관심이 고조되고있는 새로운 분야이다. 바라보는 시각에 따라 DRM기술에 대한 서로 다른 의견들을 가지고 있어 약간은 혼란스럽기도 하며, 컨텐츠 유통의 기반 인프라라는 측면에서 세계적인 표준기구의 활동과 저작권 법/제도와 관련된 정부의

정책 등과도 상당부분 연관되어있다.

본 고에서는 DRM기술 중, 컨텐츠 보호 매커니즘과 관련하여 기술에 관한 전반적인 개괄 및 업계의 제품 동향에 대하여 알아보았다. 세계 DRM 시장은 InterTrust와 Microsoft를 주축으로 5~6여 업체가 주도하고 있는 양상이며, 국내 DRM시장은 2000년 중반부터 시장이 형성되기 시작하여 현재는 10~15여 업체들이 치열한 시장경쟁을 벌이기 시작하였다. 그러나, 상대적으로 시장의 규모는 아직 미미한 것으로 보인다.

DRM제품의 성능은 기능성 및 안전성의 측면에서 평가될 수 있을 것이며, 컨텐츠의 특성 및 적용환경에 따라 두 가지 요소를 적절히 반영하는 것이 바람직할 것이다. 또한, 지금의 제품들이 기본적인 기능을 제공하는 수준이라면, 향후에는, P2P 등 다양한 응용서비스와 연결된 새로운 제품 및 서비스들이 등장할 것으로 기대된다.

참 고 문 헌

[1] "The DOI Handbook 1.0.0", International DOI Foundation, Fab, 2001.

[2] www.indecs.org/index.htm.

[3] "XrML Spec. 1.3", June., 2000. www.rxml.org,

[4] "Electronic Book Exchange System0.8", EBX, July, 2000.

[5] http://www.microsoft.com/windows/windowsmedia/en/wm7/drm.asp

〈著 者 紹 介〉

전 종 민 (Jongmin Jeon)
정회원

1999년 2월 : 성균관대학교 정보공학과 공학사
2001년 2월 : 성균관대학교 정보공학과 공학석사
2000년 7월 ~ : (주)비씨큐어 주임연구원
관심분야 : 정보보호, 암호프로토콜, DRM

최 영 철 (Youngchun Choi)
정회원

1996년 2월 : 성균관대학교 정보공학과 공학사
1998년 2월 : 성균관대학교 정보공학과 공학석사
1998년 3월 ~ 2000년 6월: 한국 정보보호센터
1998년 3월~현재 : 성균관대학교 정보공학과 박사과정
2000년 6월~ : (주)비씨큐어 시스템개발부장
관심분야 : 정보보호, PKI, 전자서명

박 상 준 (Sangjoon Park)
정회원

1984년 2월 : 한양대학교 수학과 이학사
1986년 2월 : 한양대학교 수학과 이학석사
1999년 2월 : 성균관대학교 정보공학과 공학박사(암호학)
1986년 3월~2000년 9월 : 한국전자통신연구원 부호기술부 책임연구원
2000년 9월 ~ : (주)비씨큐어 암호기술연구소장
관심분야 : 암호이론, 정보보호

박 성 준 (Sungjoon Park)
정회원

1983년 2월 : 한양대학교 수학과 이학사
1985년 2월 : 한양대학교 수학과 이학석사
1995년 2월 : 성균관대학교 정보공학과 공학박사(암호학)
1985년~1994년 : 한국전자통신연구원 부호기술부 선임연구원
1996년~2000년 : 한국정보보호센터 기반기술팀장
1997년~1998년 : 정통부 전자서명법제정 실무위원
1999년~ : 외교통상부 전자상거래 자문그룹위원
1999년~ : 성균관대학교 정보통신대학원 겸임교수
1999년~ : 고려대학교 정보보호기술학과 연구교수
2000년~ : 이화여자대학교 정보과학대학원 겸임교수
2000년~ : 암호이용촉진법 제정 실무위원
2000년~ : (주)비씨큐어 대표이사
관심분야 : 암호이론, 정보보호