제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

Microsoft 의 디지털 저작권 보호 기술 분석 및 향후 시스템 개발 요소

박주상, 윤기송, 박창순
한국전자통신연구원
컨텐츠서비스기반연구팀
e-mail : [kappa,ksyoon,cpark]@etri.re.kr

An Analysis of Microsoft DRM and Prospects for ETRI DRM System

Joosang Park, Kisong Yoon, Changsoon Park
Contents Service Platform Research Team
Electronics and Telecommunications Research Institute

요 약

Digital Rights Management System 은 컨텐트의 생성, 등록, 유통, 사용 등 전 과정에 걸쳐 작용하는, 디지털 컨텐트의 저작권을 보호 시스템이다. 이를 지원하기 위하여는 많은 요소가 필요하지만, 기본적으로 '컨텐트 암호화, 유통, 라이센스 발급, 사용'이라는 절차를 따른다. 본 논문은 여러 가지 DRM System 중에서 Microsoft DRM System 을 분석하고, ETRI DRM System 의 보완점을 살펴본다.

1. 서론

Digital Rights Management 은 기본적으로 컨텐트 소유자의 저작권을 보호함으로써, 디지털 컨텐트의 유통을 증진 시키기 위한 기술이다. 이를 위해 Digital media content 를 암호화해서, 그 컨텐트를 사용할 수 있는 라이센스를 적법한 절차를 거쳐 획득한 사람들만 사용할 수 있도록 접근을 제한하는 방법을 적용한다. 현재 MPEG, InterTrust, FASOO 등 여러 기관과 업체에서 DRM 을 연구하고 있다. 본 논문은 여러 가지 DRM System 중에서 Microsoft DRM System 을 분석하여, ETRI DRM System 의 보완요소를 찾기 위한 것이다.

2. Microsoft DRM 개요

Microsoft DRM 시스템은 위의 그림과 같이, 컨텐트 소유주, License Clearing House, 소비자, 세 주체의 상호작용에 관여한다. Windows Media Rights Manager 는 Microsoft DRM 에서 가장 핵심적인 기능을 담당하는데, 기본적으로 다음의 순서에 따라 프로세스가 진행된다.

1. 패키징(Packaging)
2. 유통
3. 라이센스 발급
4. 라이센스 획득
5. 컨텐트 사용

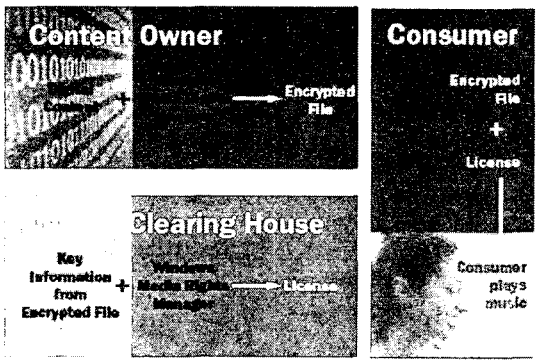

그림 1. Microsoft DRM 개요

전체 흐름을 살펴 보면 다음과 같다.

1. 디지털 컨텐트를 패키징한다.

A. Protected Media 생성
2. Protected Media 를 배포한다.
   A. Streaming Media Server
   B. Web Server Download
3. 라이센스 서버에 라이센스 발급정보 전송
4. Media 요청 및 수신
5. 라이센스 요청
6. 라이센스 수신
7. 휴대용 장치로 전송

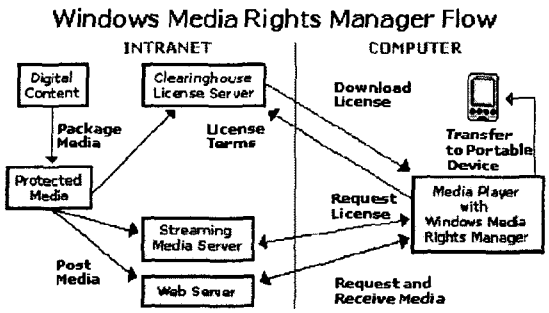

그림 2. Windows Media Rights Manager Flow

이상의 과정에서 Windows Media Rights Manager 는 4,5,6,7 의 과정에 직접 연관된다.

2.1 키 생성과 배포

Microsoft DRM 의 키생성과 관리는 컨텐트 소유주, License clearing house, 그리고 사용자의 컴퓨터에 설치된 플레이어 사이에서 이루어지는데, 먼저 컨텐트 소유주는 License Key Seed 와 Key ID 를 조합하여 Key 를 생성하고, 이를 이용하여 컨텐트 파일을 암호화한다. License clearing house 는 License Key Seed 와 패키징된 파일에서 읽어온 Key ID 를 조합하여 Key 를 생성하여 라이센스에 넣는다. 소비자의 컴퓨터에 설치된 플레이어는 발급받은 라이센스에 포함된 Key 를 이용, 패키징된 파일을 풀어서 사용한다. 아래의 그림은 이상의 과정을 설명한 것이다.

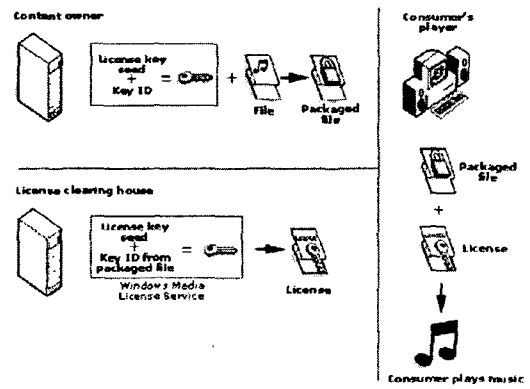

그림 3. 키 생성과 배포

2.2 라이센스

라이센스의 전송은 비즈니스 모델에 따라, 여러 가지 방법으로 여러 번 반복하여 이루어질 수 있다. 또한 사후 전송뿐만 아니라, 사전 전송도 가능하며, Silent 와 Non-silent 방식의 라이센스 전송도 가능하다. 라이센스 전송에 있어서, Silent 와 Non-silent 는 다음과 같은 차이를 말한다. 소비자가 컨텐트를 사용하기 위해서는 라이센스가 반드시 필요한데, 일반적으로 비즈니스 모델을 구현하는 과정에서 소비자가 라이센스 발급과정을 알아야 할 필요가 없도록 한다. 이런 경우를 Silent license delivery 라고 하고, 반대의 경우가 Non-silent delivery 이다.

컨텐트의 사용과 관련하여, 라이센스에 포함되는 내용은 사용횟수, 사용 또는 전송 대상 장치, 개시와 종료, 시디 작성 허용여부, 라이센스 백업 및 복구, 클라이언트 보안 수준 등이며, 그 외에도 다양한 사용 조건을 설정할 수 있다. 사용 혹은 전송 대상 장치는 SDMI 장치, Non-SDMI 장치 모두 적용 가능하다.

2.3 Windows Media Rights Manager 와 세부특징

Microsoft 의 DRM 기술에 필요한 컴포넌트는 2 가지인데, 하나는 Windows Media Rights Manager SDK 이고, 다른 하나는 Windows Media Format SDK 이다. 전자는 컨텐트 소유주가 수행할 컨텐트 패키징, 그리고 License clearing house 의 라이센스 발급에 관련된 기능을 개발하는데 사용되고, 후자는 개별 소프트웨어 개발사들이 플레이어를 개발하는데 사용한다.

Windows media rights manager 의 특징은 아래와 같이 3 가지로 요약된다.

1. Secure distribution of digital media
2. Flexible business models
3. Highly scalable platform

Secure distribution of digital media 와 관련하여, 다른 DRM 과 달리 MS 는 Individualization 과 Secure Audio Path 기능을 제공한다.

Individualization 은 사용자의 하드웨어 ID 를 이용하여 Unique DLL 을 생성, 이를 사용자의 컴퓨터와 바인딩 함으로써, 보안을 강화한 것이다.

SAP - Secure Audio Path - 는 Windows Millennium Edition 과 Windows XP 에서 Windows media rights manager SDK 를 통해서 사용할 수 있는 특징인데, 음악의 불법복제를 막기 위한 것이다. 음악에 Cryptographic noise 를 삽입하고 패키징해서 Protected media 를 생성하기 때문에, 이를 사용하려면, 먼저 오디오와 관련하여 시스템을 인증하고, 커널에서 작동하는 DRM 컴포넌트에 의해 noise 가 제거되면 원래의 음악을 들을 수 있다. 그렇지 않은 경우, 잡음만 들린다. SAP 의 수준과 관련 요소는 아래와 같다.

Secure Audio Path level	SAP required	Device verified	Digital output disabled
SAP is not required.	No	No	No
Weakest level	Yes	No	No
SAP-certified drivers	Yes	Yes	No
The highest level of security	Yes	Yes	Yes

표 1. SAP 의 수준과 관련 요소

각 레벨에 대해 살펴보면, SAP 가 요구되지 않는 상황에서는 Windows 98, NT 4.0(Service Pack 6), 2000, ME, 그리고 XP 에서 컨텐트를 사용할 수 있다. Weakest level 에서는 드라이버의 인증여부와 디지털 출력의 비활성화 여부는 검사하지 않지만, SAP 로 파일을 보호할 수 있도록 한다. 세 번째 단계는 SAP 인증된 드라이버를 사용해야 하지만 사운드카드의 디지털 출력은 여전히 유효한상태이다. 마지막으로 파일에 SAP 를 적용하고, 인증된 드라이버를 사용하며, 사운드 카드의 디지털 출력을 사용하지 못하도록 설정하면 최고의 보안 상태가 적용된다. 두 번째부터 세 번째 단계까지는 모두 Windows ME 와 XP 에서만 지원된다.

Microsoft DRM 에서는 라이센스와 미디어가 각각 분리되어 배포되며, 라이센스의 조건 변경이 쉽고, 대여 혹은 회원제 형태의 모델을 적용하거나, preview 의 제한, 투명한 라이센스 발급, 휴대용 SDMI 장치에 대한 전송 통제 등의 세부 기능이 있어서, 이를 통해 유연한 비즈니스 모델을 만들 수 있다.

또한 Microsoft DRM 은 통합이 용이하고, 미디어를 스트리밍이나 다운로드 방식으로 서비스 할 수 있고, 50 만 건의 라이센스 발급, 50 만 건의 음악 파일 패키징을 하루에 처리 할 수 있다. COM 기반의 플랫폼을 사용하므로, 현 비즈니스 모델과 라이센스 획득 모델을 통합할 수 있고, 이미 250 만 개 이상의 플레이어가 설치되어 있기 때문에, Microsoft DRM 은 Highly scalable platform 을 제공한다.

2.4 SDK 의 버전과 특징

새로운 버전의 SDK 가 나오면서, 추가된 특징들은 다음과 같다.

1. Business Rules
2. Dynamic modification of content headers
3. Player application exclusion
4. Protected content manager exclusion
5. SDK security level

이를 좀더 살펴보면, 비즈니스 룰과 관련하여, Expiration after first use, Expiration on store, Allow saving of protected streams 과 같은 특징이 추가 되었는데, 이는 컨텐트를 처음 사용한 후 폐기시한을 정하거나, 라이센스가 사용자의 컴퓨터나 장치에 저장된 후 폐기시한을 정할 수 있다. 또한 스트리밍으로 서비스되는 Protected media 의 저장을 허용 여부를 정할 수도 있다. 그러나 이 경우 역시 패키징된 형태로 정되기 때문에 사용하려면 라이센스를 요구하게 된다.

Protected content manager exclusion 기능은 Protected content manager 를 사용자의 컴퓨터나 장치에 설치된 플레이어에 포함시켜서, 컨텐트의 암/복호화와 라이센스의 권리를 강제하는 기능을 가지고 있다. 이는 라이센스 서버에 의해 강제로 수행되며, 이를 지원하기 위해, Microsoft 는 Protected content manager exclusion list 를 발행한다.

Dynamic modification of content header 는 패키징된 파일을 디스크에 저장하지 않은 채로, 컨텐트 헤더를 동적으로 변경할 수 있는 기능이다. 이렇게 하면, 소비자가 패키징된 파일을 다운로드 받기 전에, 정보를 새로이 추가하거나 변경할 수 있게 된다. 패키징 과정에서, 컨텐트 헤더 변경은 비즈니스 프로세스에 따라, 여러 주체에 의해 이루어지거나, 또는 여러 차례 변경될 수 있다. 예컨대, 하나의 컨텐트 소유주가 여러 벤더를 상대한다면, 그는 미리 파일을 패키징해두고, 각 벤더 식별 정보를 넣어 컨텐트 헤더만 바꾸어서 각각의 벤더에게 유통시킬 수 있다.

Windows media rights manager version 1 은 1999 년 8 월에 발표되었고, 다시 2000 년 여름에 WMRM version 7 이 발표되었다. Version 7 은 Digital media file 의 보호와 재생을 수행할 Application 을 구현할 수 있는 서버와 클라이언트 개발 툴킷을 포함하고 있는데, 서버용 SDK 는 WMRM version 7 이고, 클라이언트 SDK 는 Windows media format SDK 다. 가장 최근 것은 WMRM version 7.1 로서, 2001 년 9 월에 발표되었다.

WMRM version 1 의 특징은 가장 광범위한 접속을 허용하지만, 공격을 탐지하더라도, 갱신이나 취소와 같은 보호장치를 사용할 수가 없는 단점이 있었다. Version 1 을 적용하되, 컨텐트에 대해 version 7 의 라이센스를 적용함으로써 소비자의 접근 보장과 보안 강화를 함께 도모할 수는 있으나, version 1 의 위험은 여전히 남는다.

WMRM version 7 은 가장 안전하지만, 안전을 보장하기 위해서는 version 1 의 라이센스 발급을 중지해야 한다.

WMRM version 1 과 version 7 의 특징을 정리하면 다음 표와 같다.

	Rights Manager Version 1	Rights Manager Version 7
Schedule	1999 년 4 월	2000 년 여름 (ver7.1 은 2001 년 가을)
Platforms	MS Windows Apple Macintosh	MS Windows
O.S	Windows 95, 98, 2000, ME, XP, NT 4.0, Mac OS 8.1	Windows 98, 2000, ME, XP
Portable Device Support	SDMI device Non-SDMI device Portable media	SDMI device Non-SDMI device Portable media
Codecs	WMA 1,2,7	WMA 1,2,7,8

	WMV 7 MS MPEG-4 v1~v3 ISO MPEG-4 ver1, ACELP, Voxware, ATRAC-3	WMV 7,8 MS MPEG-4 v1~v3 ISO MPEG-4 ver1, WMS 7, Only DMO codecs supported for added security, ACELP, Voxware, ATRAC-3
Windows media player	Windows media player version 6.4 and later	Windows media player version 7 and later
3rd party players	WinAMP, MusicMatch, Sonique, Rioport, Sonic Foundry	MusicMatch
Business Rules	Expiration Date Unlimited play Transfer to SDMI/non-SDMI Burn to CD	Expiration Date Unlimited play Transfer to SDMI/non-SDMI Burn to CD Start time End time Duration Counted operations(plays, transfers)
User Experience	Silent licensing and pre-delivery of licenses are not supported. Users are very aware of the extra steps that they have to go through.	Improved: Silent licensing Pre-delivery of licenses Backup and restore of licenses Modal dialogs within player License management
Security	Encryption of content and license	Encryption of content and license, plus: Individualization Secure Audio Path (Windows ME, XP) Revocation of player application Revocation of content(ver.7.1) Exclusion of player application(ver.7.1) Exclusion of Protected Content Module(ver.7.1)

표 2. WMRM version 1 과 version 7 의 특징

3. 결론

이상에서 살펴본 Microsoft DRM 기술은 기존의 DRM 과 달리 몇 가지 주요한 차이점을 가지고 있다. 정리하면, Microsoft DRM 은 개별 프로그램이나 PC 혹은 단말기와 같은 장치위주로 구성되어 있고, DRM 을 구성하는 여러 가지 프로세스 중에서 '패키징 - 라이센스 발급 - 사용'에 초점을 두고 있다. 하드웨어 ID 를 이용한 Unique DLL 을 생성하여 사용자의 컴퓨터와 바인딩하는 Individualization 이나, 운영체제, 사운드 카드, 드라이버를 통해서 음악파일을 관리하는 SAP, 운영 체제의 커널 수준에서 작동하는 Protected Content Manager Exclusion 등의 요소는 Microsoft DRM 기술이 운영체제와 컴퓨터, 단말기 등의 장치 위주의 관리에 집중하고 있음을 보여준다. 한편, DRM 을 실제 상황에 적용하기 위해서는 전역 식별자, 모니터링 및 추적, 계약, 그리고 IPR Database 등의 요소가 함께 적용되어야 하는데, Microsoft DRM 기술에서는 이러한 요소가 나타나지 않고, 다만 컨텐트 소유주가 패키징을 하여 유통시킨 후, 이에 대한 라이센스의 발급과 소비자의 사용에 대한 기술로만 구성되어 있다.

4. ETRI DRM System 보완요소

현재 ETRI 는 DRM 을 기반으로 하여, 디지털 컨텐츠 유통 솔루션을 개발 중이다. 여기에는 컨텐츠 유통 시스템, 클리어링 센터 시스템, DRM 기반 소프트웨어가 포함되어 있으며, 현재 이들 시스템의 통합 및 시험이 완료되었으며, 관련 표준화도 함께 진행중이다.

향후 보다 나은 시스템을 개발하기 위하여는 다음과 같은 측면에서 Microsoft DRM 과는 차별화해야 할 필요가 있다.

1. 다단계 유통 시스템
2. 키 생성 및 관리
3. 식별 체계와 결합
4. XrML Version 2.0 의 사용조건과 권리 수용
5. 호환성 확장
6. 메타데이터 표준화
7. Total Solution 제공

Total Solution 을 제공하기 위해 필요한 sub-system 과 기능은 아래 표와 같다.

Sub-system	주요 기능
Identifier system	식별자 발급과 관리 식별자 변환 및 중계 식별자 발급 내역 참조 IPR Database 연결 관리
IPR Database	컨텐트 정보 등록 및 관리 컨텐트 정보 제공 다른 데이터베이스와 연결 및 호환
Monitoring Service	컨텐트 유통 상황 모니터링 클라이언트를 통한 컨텐트 사용 모니터링 불법 유통되는 컨텐트 추적

표 3. Sub-system 및 주요 기능

참고문헌

[1] 송영원, 최현우, "MPEG-21 표준화 기술", 정보과학회지 제 19 권 제 6 호 p4~13 2001.6

[2] ISO/IEC JTC1/SC29/WG11 N3500, "Information technology – Multimedia Framework(MPEG-21)

[3] "Windows Media Rights Manager Whitepaper" 외 20 건, http://www.microsoft.com/windows/windowsmedia/drm.asp

[4] Tagish, "Synthesis of the IMPRIMATURE Business Model", 1998.10

[5] 박복녕, 김정범, 김태윤, "저작권 위탁 관리를 위한 P-ESD 시스템 설계", 한국정보처리학회 춘계학술발표논문집 제 9 권 제 1 호 p875~878 2002.