Digital Rights Management – An Introduction
Outline

- What is digital rights management?
- Major players in DRM markets
- DRM Standards
  - MPEG-21IPMP
  - MPEG
- DRM Laws
...a subject that has been lurking in the underbrush of the digital information world for many years and is finally coming to the front. *Right management is, in some ways, the ugly beast that content providers – publishers, broadcasters, market researchers, consultancies, major corporations, and others – have wanted to keep in the closet.* The Internet has forced the closet door open; really, it has eliminated the door itself. What used to be relatively simple is now uncomfortably complex. What used to be a source of moderate business overhead is now a significant undertaking. What used to be the province of lawyers, agents, and administrators is now also the domain of technologies...

Is DRM a ugly beast to content providers?

---

Adopted from the book “Digital Rights Management, Business and Technology”
Implicit rights for traditional content (printed books) and digital content.
Needs for DRM Systems

- **Prevalence of new types of commerce**
  - E-commerce has become a huge business and a driving factor in the development of the Internet.
  - With the advent of evolved 2G and 3G mobile network, mobile e-commerce (m-commerce) will be more and more significant.

- **Importance of digital contents**
  - Online delivery of digital media, such as MP3 audio or video, is becoming an increasing important part in e-commerce and m-commerce.
  - Unlimited consecutive copying in the digital domain is the major obstacle for digital media distribution and associated business.

- **Digital rights management systems are required to protect both rights and business**

The term Digital Rights Management (DRM) was coined by some combination of vendors, their marketers, and industry analysts in the late 1990s.
Definitions of Digital Rights Management

A DRM system enables the secure exchange of intellectual property, such as copyright-protected music, video, or text, in digital form over the Internet or other electronic media, such as CDs, removable disks, or mobile networks.

DRM is the chain of hardware and software services and technologies governing the authorized use of digital content and managing any consequences of that use throughout the entire life cycle of the content.
A DRM system enables the secure exchange of intellectual property, such as copyright-protected music, video, or text, in digital form over the Internet or other electronic media, such as CDs, removable disks, or mobile networks.

DRM allows content owners to distribute securely to authorized recipients and gives them control over the whole distribution chain.
DRM Systems: The Technical View (1/2)

- DRM systems shall provide
  - Encryption of the content or parts in order to disallow uncontrolled access
    - Partial or full encryption
    - Real-time or off-line encryption
  - Decryption key management
  - Access control (conditional access) according to flexible usage rules
    - Usage rules can be adapted to the business model
    - Examples:
      - Restricting access to certain users, a limited time, or a limited number of accesses
      - Trading access right for customer information or advertisement exchange
      - Initial access to digital data may be free, while subsequent access must be paid for
DRM Systems: The Technical View (2/2)

- Interface to billing systems or mechanisms
  - DRM system must be able to trigger monetary transactions
- Copy control or copy prevention
  - The DRM system can enforce copy restrictions, such as no/one/several/unlimited copies of the multimedia data are allowed, and with/without rights to produce copies of these copies
  - Watermarking is suitable for some usage rules.
- Identification and tracing of multimedia data
  - Copies produced from the analog output cannot be prohibited
  - Individual watermarking (fingerprinting) of the distributed data shall be part of the DRM system
- Temper-proofing of digital contents
Building Blocks of DRM

The diagram illustrates both technical and non-technical building blocks of DRM.
Like any cryptographic system, a DRM system is as strong as its weakest component.
Why do Corporations Implement DRM?

<table>
<thead>
<tr>
<th>DRM for Commerce</th>
</tr>
</thead>
<tbody>
<tr>
<td>To protect the monetary value of digital content by</td>
</tr>
<tr>
<td>• protecting digital contents from unauthorized use</td>
</tr>
<tr>
<td>• enforcing payment terms and conditions</td>
</tr>
<tr>
<td>associated with its authorized use</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DRM for Confidentiality (DRM for privacy)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• to protect information from unauthorized use</td>
</tr>
<tr>
<td>• to govern the way information may be used on an authorized basis</td>
</tr>
<tr>
<td>• to record when and how information is used</td>
</tr>
</tbody>
</table>
New Business Model and Profit by DRM

- DRM is much about the **opportunity inherently in new business models** as it is about in preserving the business of old ones.

  - Subscribing expensive scientific journal v.s. buy single article
  - Monthly fee for downloading certain types of music v.s. CD albums

- Revenues other than content transactions are possible now
  - E.g.
    - Drug regulation documents
    - Blueprints and specifications for construction industry
The DRM Market

- Although the Internet was built with an “information wants to be free” environment in mind, DRM is becoming a more and more fundamental idea in the evolution. Recent research by IDC predicts that the market for DRM technology and services will be $200 million in 2001, and ultimately $3.5 billion in 2005.
# DRM Evolution

<table>
<thead>
<tr>
<th>Today</th>
<th>Evolutionary Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trial use</td>
<td>Required</td>
</tr>
<tr>
<td>Limited use</td>
<td>Pervasive</td>
</tr>
<tr>
<td>Piecemeal</td>
<td>End-to-end</td>
</tr>
<tr>
<td>Standalone/independent</td>
<td>Integrated</td>
</tr>
<tr>
<td>Visible</td>
<td>Transparent and visible as appropriate</td>
</tr>
<tr>
<td>Content-type specific</td>
<td>Content-type independent</td>
</tr>
<tr>
<td>PC only</td>
<td>Across a wide variety of devices</td>
</tr>
</tbody>
</table>
DRM-related Legislative Concerns

- Digital Millennium Copyright Acts (DMCA)
  - Signed into law by U. S. President Clinton on October 28, 1998, is one of the response to the requirements in two World Intellectual Property Organizations (WIPO) treaties.
  - The anti-circumvention provision is the most controversial part of DMCA since it prohibits making or selling devices or services that circumvent technological measure used to protect copyrighted works.
  - Exception to anti-circumvention provision:

  - Government activities
  - Decision making of educational institutes
  - Reverse-engineering for program interoperability
  - Encryption researches
  - User privacy protection
  - System security testing
  - Protection for accessing Internet by minors
What is digital rights management?
- Motivations
- Corporations’ view
- Technological view

Major players in DRM markets
- DRM Systems
  - interTrust
  - Microsoft
  - RealNetwork
- Aggregators
- Rights Language

An introduction to MPEG-21 Part 4: IPMP
interTrust: Rights/ System

• Standard format (like MPEG-4, PDF...)
• Proprietary format (for AAC, MP3)

• Metadata
• Usage rules

DRM systems not involved in commerce

• Both HW/SW are supported
interTrust: Rights/ System

- **System components**
  - Packagers
  - Servers
  - Clients
  - Toolkits

- **Characteristics**
  - SDK for third party applications, such as music players
  - Supporting both Internet-enabled or tethered devices

- **Challenges**
  - To recruit more content owners to distribute content over it
interTrust Now

- InterTrust restructured its operations and changed its strategy and business model
  - Software development was ceased
  - Focus on licensing intellectual properties

- On May 23, 2002, interTrust announce a global intellectual property licensing agreement with Sony that allow Sony to use all of interTrust’s patents for 28.5 million dollars (Sony is the 2nd large consumer electronics vendor)

- Analysis
  - interTrust’s cash flow can be positive for the first time
  - Sony is serious about DRM
IBM: Electronic Multimedia Management System

- The IBM EMMS Content Preparation Software Development Kit (SDK)
  - integrates DRM capabilities into vertical or custom applications
- The IBM EMMS Content Mastering Program
  - a turnkey content-preparation DRM application for music content and its associated promotional material
- The IBM EMMS Content Hosting Program
  - a storage facility for EMMS formatted content
- The IBM EMMS Web Commerce Enabler
  - deploy EMMS DRM content into custom retail offerings or enterprise portals, facilitating end-user download or streaming of desired content
- The IBM EMMS Clearinghouse Program
  - provides DRM functions and acts as a central control point for managing, authorizing and reporting transactions
Microsoft: Windows Media DRM 9 Series

- Microsoft’s Definitions of DRM
  - A set of technologies content owners can use to protect their copyrights and stay in closer contact with customers.
  - A technology that enables the secure distribution, promotion, and sale of digital media content on the Internet.
The first version of Windows Media DRM was released in August 1999.

In 2002, Microsoft released Windows Media DMR version 7, offering greater flexibility and better security to its users.

- The Freeme software can breach the DRM protection.

The latest release, Windows Media DRM 9 Series, launched in January 2003, supports real-time encryption (also known as "Live DRM") and enables content to be delivered simultaneously to consumers as it happens.
WMRM Architectures

Windows Media Rights Manager Flow

1. Digital Content
   - Package Media
     - Protected Media

2. Post Media
   - Streaming Media Server
     - Web Server

3. License Terms
   - Clearinghouse License Server

4. Request and Receive Media
   - Request License

5. Request License
   - Media Player with Windows Media Rights Manager

6. Download License
   - Computer

7. Transfer to Portable Device
   - INTRANET

Flow Diagram Description:
- Step 1: Digital Content is packaged into protected media.
- Step 2: The protected media is posted to the streaming media server.
- Step 3: License terms are checked by the clearinghouse license server.
- Step 4: License request is made to the media player with Windows Media Rights Manager.
- Step 5: License is requested.
- Step 6: Download license is initiated.
- Step 7: Media is transferred to a portable device.
License and Keys

Content owner

License key seed + Key ID = File + Packaged file

Consumer's player

License clearing house

License key seed + Key ID from packaged file = License

Windows Media License Service

License

Consumer plays music
Microsoft® Windows Media® Digital Rights Management (DRM) 9 Series builds upon a proven and secure end-to-end DRM system that offers content providers and retailers a flexible platform for the secure distribution of digital media files while providing users ease of use and a greater opportunity to consume premium content.
Major Components

- Microsoft Windows Data Session Toolkit
- Microsoft Windows Media Rights Manager 9 Series – Live DRM
  - Required SDK
    - Windows Media Rights Manager 9 Series
      - Approval of license is required
    - Windows Media Encoder 9 Series
    - Windows Media Format 9 Series
Windows Media Digital Rights Management SDKs

- Microsoft® Windows Media® Digital Rights Management (DRM) consists of the following products:
  - Windows Media Rights Manager Software Development Kit (SDK) enables content owners to package content and license clearing houses to issue licenses.
  - Windows Media Format SDK enables independent software vendors (ISVs) to develop player applications. In addition, a key to Windows Media DRM Runtime is needed to decrypt content protected using Windows Media Digital Rights Management.
  - Windows Media Portable Device DRM v1 enables portable device manufacturers to develop devices that decrypt content protected using Windows Media DRM.
Microsoft® Windows Media® Data Session Toolkit

- An easy and secure way to deliver protected digital media content to a computer via physical medium (such as CD or DVD)

The power of the Windows Media Data Session Toolkit allows users to build a playlist, encode content, edit and insert meta data for optimal media library integration. Content owners can then assign business rules, encryption options, and specify the license acquisition location enabling innovative business models.
Microsoft® Windows Media®
Data Session Toolkit (cont.)

- Flexible business model
  - New business model
  - Different format on the same disk
  - Secure super distribution

- Low impact, low cost implementation
  - Broad reach (450 million installed computers)
  - Online and offline license acquisition

- Strong and persistent security
Microsoft Windows Media Rights Manager 9 Series – Live DRM

- Live DRM
  - For on-demand or live content, encryption can occur in real-time
  - Simultaneous encoding and encryption

- Broad Reach
  - The number of installed compatible media player is large

- Secure Distribution of Digital Media
  - System components can be renewed
System Requirements for WMRM

- Microsoft Windows® 2000 Server operating system
- 133-megahertz Pentium or higher central processing unit (CPU)
- 256 megabytes (MB) of RAM
- 4 MB of free hard disk space
Content Providers and Partners

- WMRM
  - BMG Entertainment
  - Cinemanow
  - EMI Recorded Music
  - Full Audio
  - Ifilm
  - Lionsgate Films Entertainment
  - Movielink
  - NHL.com
  - Pressplay Music Service
  - Sony Music Entertainment
  - Universal Music Group
  - Warner Music Group

- LiveDRM
- In US
  - CinemaNow
  - EmpireDRM
  - iStreamPlanet
  - SyncCast
- In Europe
  - DMD Secure
  - Servecast
  - Streamwide
- In Asia
  - Aboutmedia Technology
  - J-Stream
  - Keel
  - NTT-Com
  - VirtueBroadcasting
RealNetworks: Helix DRM

- The first multi-format digital rights management platform for secure delivery of media to any devices
- Unsurpassed security
- Supported formats
  - RealAudio, RealVideo, MP3, MPEG-4, H.263, AAC, NB-AMR
- Supported platforms
  - Win32, Sun Solaris, Linux, HP-UX, AIX
A widely distributed digital music service for streaming, downloading, and burning music online

A joint venture between RealNetworks, AOL Time Warner, Bertelsmann, AG, EMI Recorded Music, Zomba

Distribution partners
- AOL Time Warner
- RealNetwork
全球唱片產業拉警報，不少人怪罪盜版和網路檔案交換軟體風行，不過日前蘋果電腦史無前例成功整合五大國際唱片公司，推出低價音樂下載軟體iTune，消費者只要花0.99美元，就可以合法下載一首歌曲，果然這項音樂下載服務才推出，就寫下單周賣出一百萬首歌曲的驚人成績，連MP3播放機的新訂單都超過11萬台。

蘋果推出的iTune是第一個獲得唱片業認可的網路音樂商店，這項下載服務之所以能讓向來各自為政的唱片公司攜手，是因爲過去五大唱片公司雖然都推出音樂下載網站，不過限制較多，包括下載、燒錄都要另外付錢，而iTune改進這些缺點，不但整合五大國際唱片公司共同結盟，還制定統一的歌曲下載費用，不論天王巨星或是網路新秀的歌，統統平價下載，才會在推出首周就創下百萬首下載數字，如果這個榮景持續，一年的下載曲數就有5200萬首，比目前其他付費線上音樂服務網站1年下載總和3 500萬首要多得多。
The iTune Music Store

- Browse by genre, artist and album
- Transfer music to your iPods
- Burn music to CDs for personal use

10, 15 or 30GB models held up to 7500 songs

Lighter and thinner – weighs less than 2 CDs

All touch-sensitive, illuminated controls

New dock for easy charging, synching and line out

Free 30-second preview of every song

Exclusive tracks not available on CD