Part II

Content-Oriented Base Technologies for Networked Multimedia
## Outline

1. Introduction and Motivation
2. Interactive Web Applications
3. Web Programming with Java
4. Communities, the Web, and Multimedia
5. Digital Rights Management
6. Cryptographic Techniques
7. Multimedia Content Description
8. Electronic Books and Magazines
9. Multimedia Content Production and Management
10. Streaming Architectures
11. Web Radio, Web TV and IPTV
12. Multimedia Conferencing
13. Signaling Protocols for Multimedia Communication
14. Visions and Outlook

---

**Part I:** Web Technologies for Interactive MM

**Part II:** Content-Oriented Base Technologies

**Part III:** Multimedia Distribution Services

**Part IV:** Conversational Multimedia Services
5 Digital Rights Management

5.1 Media Rights

5.2 Rights Models

5.3 Principles of Encryption-Based DRM Systems

5.4 Watermarking

5.5 DRM Standards and Selected Commercial Solutions

Literature:


Ronan Deazley, Martin Kretschmer, Lionel Bently (eds): Privilege and property: essays on the history of copyright, Open Book Publishers 2010
Copyright / Intellectual Property Right (IPR)

• History:
  – “Intellectual property” unknown in ancient and medieval cultures
  – “Author privileges” (since 1486, Venice) (book printing since 1440)
  – Theory of intellectual property since approx. 1700

• Functions of copyright:
  – Securing rights for the author of a work to use it, publish it, benefit financially from it and to control its use
  – Copyright is established directly, independent of registration
    » Differently as with other forms of IPR (patents, trade marks)

• Principle of territoriality
  – Regional laws
  – Few international treaties
    » WIPO = World Intellectual Property Organisation (www.wipo.int)
    » 150 participating countries

www.copyrighthistory.org
Types of Copyrighted Works

- Literary works, e.g. newspapers, manuals, fiction, non-fiction, poetry, advertisements, ...
- Musical works, such as songs and instrumentals
- Dramatic works, such as plays
- Pantomime and choreographic works, such as dance and mime
- Pictorial, graphic and sculptural works, such as photographs, paintings, maps, drawings, ...
- Motion pictures and other audiovisual works
- Sound recordings
- Architectural works
- Audio-visual displays
- Software programs
IPR in the U.S. (1)

- Article 1, section 8 of U.S. Constitution:
  - “The Congress shall have Power […] to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.”

- Copyright Act of U.S. Congress 1976
  - Protects “…original works of authorship fixed in a tangible medium of expression, now known or later developed, from which they can be perceived, reproduced and otherwise communicated, either directly or with the aid of a machine or device”
  - **Fair-Use** Doctrine
    Use of the copyrighted work to a small extent which does not affect the market value of the work is admitted
  - **First-Sale** Doctrine
    Buyers get extensive rights to do everything they want with the physical copy bought, but they do not get the copyright for the content
  - **Public-Domain** Doctrine
    Works older than 70 years are free of copyright
IPR in the U.S. (2)

- Digital Millennium Copyright Act (DMCA) 1998
  - US response to world-wide copyright treaties
    (*WIPO Copyright Treaty* and *WIPO Performances and Phonograms Treaty*)
  - Section 1201: **Anti-circumvention provision:**
    It is prohibited to make or sell devices that
    » Are primarily designed or produced to circumvent technological measures to protect copyrights
    » Have only limited commercial significant purpose or use other than this kind of circumvention
    » Are marketed for such circumvention
  - Tacit admission that copy-protection technologies will never be perfect!
  - Problematic:
    » Where does fair use end? (e.g. circumvention for backup copies)
    » Can DMCA restrict the right of free speech? (e.g. for magazines publicizing protection-cracking software code)
IPR in the EU

- Original Idea: Harmonization of the individual regulations of the EU member states
  - “Green Book” 1997
- Basis: Article 94 of EU Treaty
  - “Harmonization of national provisions affecting Common Market”
- EU entered WIPO in 2001
- EU Copyright Directive (Info-Richtlinie) 2001
  - Gives a similar basis for Digital Rights Management as the DMCA in the U.S.A.
  - Strong emphasis on the rights of the creator (*droit moral*), less market-oriented
Urheberrecht in Deutschland

• Urheberrechtsgesetz (UrhG) 1965
• Novelliert 2003 in Anpassung an die EU-Info-Richtlinie und die WIPO-Abkommen ("Erster Korb")
  – Künstlerische und ästhetische Interessen des Urhebers an seinem Werk
    (nur natürliche Personen, nicht wie in den USA auch juristische)
  – Anreiz für Urheber, weiter Werke herzustellen
  – Sicherung einer angemessenen Vergütung
  – Eigentümerstellung des Urhebers fast so stark wie bei einer materiellen Sache
• Zweierlei Rechte:
  – Urheber-Persönlichkeitsschutz
    » Nicht veräußerlich (kann nicht verkauft, verschenkt, vererbt werden)
  – Verwertungsrechte
    » Urheber bestimmt, ob Werk vervielfältigt werden darf
    » Privatkopie (Vervielfältigung zum eigenen Gebrauch) im Prinzip immer erlaubt (§53) – aber eingeschränkt durch §95a!
Aktuelle Entwicklung im deutschen Urheberrecht

Weitere Reform des UrhG („Zweiter Korb“), Gesetz seit 2008

• Privatkopie und Tausch:
  – Privatkopie kopiergeschützter Materialien verboten (§95a)
  – Tausch von urheberrechtlich geschützten Inhalten über Netzwerke verboten
  – Pauschalvergütung für Privatkopien (Abgaben auf Geräte, mit denen Kopien angefertigt werden können)
  – Vergütungshöhe unter den Beteiligten auszuhandeln, bei technischem Kopierschutz entfällt der Anspruch auf Vergütung
  – Keine Bagatellklausel (Kabinettsbeschluss 22.3.2006): Auch Privatpersonen prinzipiell mit bis zu drei Jahren Haft bedroht

• Urheberrecht in Wissenschaft und Forschung:
  – Relativ großzügige Regelung in §52a gilt nur befristet bis Ende 2012 (§137k)
  – §52b: Digitalisierte Bibliotheksbestände nur an Leseplätzen der Bibliothek nutzbar
    (Ausnahme: Explizit weitergehende Rechte erworben)

http://www.gesetze-im-internet.de/urhg
Rights Management Terminology

- **Rightsholder**: A party owning rights in intellectual property
- **User**: A party that intends to make use of intellectual property rights. May be a *licensee* or a *buyer* (or *grantee*).
- **Content owner**: Like rightsholder, but less strict. May own the rights only partially, e.g. only for specific countries.
- **Rights transaction**: Transaction establishing a new rights situation
  - Example: Buying a newspaper, buying the right to re-publish content from the newspaper, buying the publishing house
- **Agent**: A legal entity authorized by a rightsholder to enter into a rights transaction on behalf of the rightsholder
- **Royalties**: Monetary compensation to a rightsholder or his agent for the use of intellectual property rights
- **Rights management**: Business processes that for legal and commercial purposes track rights, rightsholders, licenses, sales, royalties, and associated terms and conditions
- **Digital rights management (DRM)**: Rights management using digital technology
Traditional Rights Management Solutions (1)

- The solution found for photocopying: Copyright Clearance Center
  - Obtains the rights from publishers to make photocopies (relating to over 1.75 million works)
    - US: Copyright Clearance Center (CCC), www.copyright.com
    - Germany: VG WORT (Verwertungsgemeinschaft Wort, www.vgwort.de)
      - 2009: Income 434 Mio EUR, distributed to over 148,000 receivers
      - 2010: Income 131 Mio EUR, distributed to over 154,000 receivers
    - International Federation of Reproduction Rights Organizations (IFRRO)
    - Represents German position in the "Google Books settlement" law case
      - Bundles these rights into an offer to users like copy centers
      - Publicly available photocopy machines can obtain a license from CCC
        - Similar system in Germany
      - Corporate organizations are charged according to survey data for a given industry branch
      - Recent development: Individual “Pay-per-use” via Internet
- Rather successful, low overhead
- Not the only possibility for rights transactions of this kind
  - Separate agreements with publishers always possible
Traditional Rights Management Solutions (2)

- Voluntary collective music licensing
- Organizations for collecting fees from commercial music use
  - U.S.:
    American Society of Composers, Authors and Publishers (ASCAP, www.ascap.com),
    Broadcast Music International (BMI, www.bmi.com),
    SoundExchange (www.soundexchange.com)
    since 2000, for digital performance
  - Germany:
    “Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte” (GEMA, www.gema.de)
- Music is played commercially at a high number of occasions:
  - Radio broadcasting, concerts, restaurants, shops, airlines, soundtracks for movie broadcasts, sound on websites, hold music for telephones, ...
  - This use is not covered by the license obtained with e.g. a CD – Additional fees are collected
Traditional Rights Management Solutions (3)

• In the schemes discussed above, the rightsholder is free to admit a certain use or not, depending on a rights transaction.

• **Compulsory licensing:**
  – Government-regulated pricing
  – As soon as user pays an established fee (possibly to a governmental organization), he has certain rights of use
  – Frequently used for patents the broad use of which is needed for the society welfare
    » Compulsary licensing of “clean air” technologies
    » Compulsary licensing of unique pharamaceutical products
    » Sometimes also applied to media (e.g. for National Public Radio in US)
  – Pricing scheme is likely to be “flat”, e.g. monthly fee independent of actual degree of usage and used works
Public Domain

- Complete refrainment from copyright-based usage restrictions
  - Enables free collaboration and "remixing" of content and knowledge
- Some content is in the public domain automatically:
  - National anthems, traditional songs, ...
  - Content the last creator of which has died 50/70/75 years ago
- Various initiatives:
  - Projekt Gutenberg (gutenberg.org): Free electronic books
  - Wikibooks
  - See publicdomainworks.net
- Various legal formulations:
  - Open Content License
  - Free Art License
  - Free Music Public License
  - Open Publication License
  - GNU Free Documentation License
Some Rights Reserved: Creative Commons

- Web culture requires new forms of copyright rules
  - Keep the copyright but allow certain uses by others
- Creative Commons (CC):
  - Non-profit organization offering "legal tools"
  - Spectrum of possibilities between public domain and full copyright
- License Conditions identified by CC:
Creative Commons Licences

- Attribution
- Attribution Share-Alike
- Attribution No Derivatives
- Attribution Non-Commercial
- Attribution Non-Commercial Share Alike
- Attribution Non-Commercial No Derivatives ("Free advertising")
Position of the Music Industry

2002:

WASHINGTON-The Recording Industry Association of America (RIAA) announced today that the number of units shipped domestically from record companies to retail outlets and special markets (music clubs and mail order) fell 10.3 percent in 2001.

Specifically, total U.S. shipments dropped from 1.08 billion units shipped in 2000 to 968.58 million in 2001-a 10.3 percent decrease. The dollar value of all music product shipments decreased from $14.3 billion in 2000 to $13.7 billion in 2001-a 4.1 percent decrease, according to figures released today by the RIAA.

"This past year was a difficult year in the recording industry, and there is no simple explanation for the decrease in sales. The economy was slow and 9/11 interrupted the fourth quarter plans, but, a large factor contributing to the decrease in overall shipments last year is online piracy and CD-burning," said Hilary Rosen, President and CEO of the RIAA. "When 23 percent of surveyed music consumers say they are not buying more music because they are downloading or copying their music for free, we cannot ignore the impact on the marketplace."

http://www.azoz.com/music/features/0008.html

IFPI Germany press release 21.3.2002: “Mass music copying and music piracy in the Internet threatens music markets”
Music Sales Statistics (1)

Units shipped
Data: RIAA (riaa.com)
Music Sales Statistics (2)

Retail value
Data: RIAA (riaa.com)

Music Sales USA

- Total Physical
- Total Digital
- Total Digital and Physical

Retail value

Data: RIAA (riaa.com)
### RIAA Music Sales: Physical 2009-2010

<table>
<thead>
<tr>
<th>Physical</th>
<th>CD</th>
<th>292.9</th>
<th>225.8</th>
<th>-22.9%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Units Shipped</td>
<td>Dollar Value</td>
<td>4,274.1</td>
<td>3,361.3</td>
<td>-21.4%</td>
</tr>
<tr>
<td>CD Single</td>
<td>0.9</td>
<td>1.2</td>
<td>31.2%</td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>3.3</td>
<td>7.2%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LP/EP</td>
<td>3.2</td>
<td>4.0</td>
<td>25.9%</td>
<td></td>
</tr>
<tr>
<td>60.2</td>
<td>87.0</td>
<td>44.4%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vinyl Single</td>
<td>0.3</td>
<td>0.3</td>
<td>-3.9%</td>
<td></td>
</tr>
<tr>
<td>2.5</td>
<td>2.2</td>
<td>-9.4%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Music Video</td>
<td>11.8</td>
<td>9.1</td>
<td>-22.6%</td>
<td></td>
</tr>
<tr>
<td>212.0</td>
<td>178.8</td>
<td>-15.7%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DVD Video</td>
<td>11.2</td>
<td>8.7</td>
<td>-22.4%</td>
<td></td>
</tr>
<tr>
<td>206.9</td>
<td>175.3</td>
<td>-15.3%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Units</td>
<td>309.2</td>
<td>240.5</td>
<td>-22.2%</td>
<td></td>
</tr>
<tr>
<td>Total Value</td>
<td>4,555.9</td>
<td>3,635.1</td>
<td>-20.2%</td>
<td></td>
</tr>
</tbody>
</table>

- Physical records with increase: LP/EP (Vinyl albums), CD Single
- DVD Video is decreasing also!
- DVD Audio and SACD are almost neglectable
### Background for Digital Rights Management?

#### RIAA Year-End Statistics

<table>
<thead>
<tr>
<th>% of Shipments</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>66 %</td>
<td>59 %</td>
<td>53 %</td>
</tr>
<tr>
<td>Digital</td>
<td>34 %</td>
<td>41 %</td>
<td>47 %</td>
</tr>
</tbody>
</table>

#### Trends:
- Physical distribution (CDs) is decreasing rapidly
- Virtual distribution will soon be the mainstream
- "Digital performance royalties" (SoundExchange) are increasing rapidly (50% increase from 2008 to 2009, 60% from 2009 to 2010, $250 mio)
- Overall music market is shrinking

#### Independent positions:
- The process of finding new music is closely coupled with sharing and copying (it is a social activity)
- Sharing often leads to later purchases
  - Not only physical copies (CD), but concert tickets, merchandise etc.
  - See e.g. Singh et al.: Downloading vs. Purchase, DRMTICS 2005 Conference
5 Digital Rights Management

5.1 Media Rights

5.2 Rights Models

5.3 Principles of Encryption-Based DRM Systems

5.4 Watermarking

5.5 DRM Standards and Selected Commercial Solutions

Literature:


Mark Stefik: Internet Dreams - Archetypes, Myths, and Metaphors, MIT Press 1996
Examples for Content Rights Transactions

• Buying a book, the buyer gets:
  – The right to read one copy of the physical book arbitrarily often
  – The right to sell or give the book to someone else
  – He does not get the rights to, e.g.:
    » To perceive the book in a different technology (eBook, audio book)
    » To quote from the book in own publications beyond fair use

• Buying a cinema ticket, the buyer gets:
  – The right to see the movie once (or sometimes until the theatre closes)
  – He does not get the rights to, e.g.:
    » Let a friend see the movie
    » Make a video recording of the movie

• Listening to a song on the radio, the listener gets (without paying)
  – The right to listen to the song
  – The right to record it for personal use
Fundamental Types of Rights

- According to Mark Stefik, Xerox PARC ("Letting Loose the Light")

<table>
<thead>
<tr>
<th>Render Rights</th>
<th>Transport Rights</th>
<th>Derivative Work Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Print</td>
<td>Copy</td>
<td>Extract</td>
</tr>
<tr>
<td>Play/View</td>
<td>Transfer</td>
<td>Edit</td>
</tr>
<tr>
<td>Export</td>
<td>Loan</td>
<td>Embed</td>
</tr>
</tbody>
</table>
Utility Rights

• Additional types of rights which exist for technological reasons rather than to support publishers’ business models

• Backup rights:
  – Right to make a copy as a safety means against technical failure

• Caching rights:
  – Right to make temporary local copies to improve performance

• Data integrity rights:
  – Right to create redundant code information etc. to ensure that the data does not get corrupted
Rights Attributes

- Rights attributes are additional specifications added to each of the fundamental rights
- Rights model = fundamental rights + rights attributes

Consideration
(what to give in return)
- Money
- Personal data

Types of users
(subscribers vs. visitors, regular vs. student, ...)

Extents (Time period, repetitions, number copies, ...)
Examples (Basic Rights Language) (1)

- **Buying a book:**
  - **Render rights:** Print
    » Consideration: Price of the book
    » Extent: Forever, one copy only
    » Type of user: No distinctions
  - **Transport rights:** Sell, give away, loan
    » No restrictions
  - **Derivative rights:** None

- **Buying a cinema ticket:**
  - **Render rights:** Play
    » Consideration: Price of movie ticket
    » Extent: Once or rest of the day
    » Type of user: Adult or child
  - **Transport rights:** None
  - **Derivative rights:** None
Examples (Basic Rights Language) (2)

• Listening to a song on the radio
  – Render rights: Play
    » Consideration: None
    » Extent: Once for each receiver
    » Type of user: No distinction
  – Transport rights: Copy for personal use
    » Consideration: Percentage of the cost of the recording media
    » Extent: Personal use only
    » Type of user: No distinction
  – Derivative rights: None
Chains of Rights Transactions

- Rights transactions always take place in chains
- Each transaction creates a new set of rights
- Example:

\[
\begin{align*}
\text{Musician} & \quad \text{Record Company} & \quad \text{Radio Station} & \quad \text{Listener} \\
\text{Royalties} & \quad \text{License Fees} & \quad & \quad \\
\end{align*}
\]

Render: CD,...
Extents: .., distributor, ...
Derivative: publishing (cover vsns.)

Render: Play
Extents: arb.
Derivative: 30 s samples

Render: Play
Transport: Copy for personal use ...

Royalties
License Fees
Rights Transactions May Change Rights

• Recording a tape from radio is a step in a chain of rights transactions
• After recording, the rights on the record change:
  – Extent of the render right is now “forever”
  – New derivative rights are added, e.g.:
    – **Derivative right**: Extract and embed rights for commercial use
      » Consideration: None
      » Extent: Only 30 seconds samples
      » Type of user: Commercial
Rights Models and Digital Media

• Example: Music or video download service
  – Render rights: View
    » Consideration: Price of the download
    » Extent: Forever
    » Type of user: No distinction
  – Transport rights: None
  – Derivative rights: None

• Practical questions:
  – How to ensure that the transport rights are obeyed (i.e. the file is not copied to other people)?
    » Legal measures: How to prove from where the file came?
    » Technical measures: How to make content viewable only for uniquely identified users?
  – These are technical challenges of DRM technology
Superdistribution

- Basic idea (Ryoichi Mori): *A software object cannot easily determine whether it has been copied or not, but it can easily be built to do some extra things when run.*
  - "Extra things" may be: metering, billing, requiring a license, …
- Superdistribution needs to be enabled at:
  - Content: "Wrapped" with superdistribution component
  - Computer: Executes superdistribution routines when accessing content
Superdistribution for Web 2.0: Research Ideas

Deutsche Telekom Laboratories

Superdistribution 2.0

Selbst erstellte digitale Inhalte sicher in Communities verteilen

Superdistribution 2.0 demonstriert ein innovatives Geschäftsmodell, das die Superdistribution ungeschützter und rechtegeschützter digitaler Inhalte ermöglicht. Basierend auf Web 2.0-Technologien können Nutzer selbst erstellte Inhalte über Festnetz, Mobilfunk und zwischen verschiedenen Endgeräten einfach, schnell und legal an andere Nutzer weitergeben und erhalten durch die Community-Plattform Feedback zu ihren Inhalten.


MediaNet LMU
Implementing Rights Models

- Mark Stefik, Xerox Labs
  - Digital Property Rights Definition Language (DPRL) (Lisp-like syntax)
- ContentGuard (Xerox spin-off company, partially owned by Microsoft)
  - DPRL idea in XML syntax: XrML (Extensible Rights Management Language)
    - Current version: 2.0 (www.xrml.org)
    - Submitted to OASIS, ContentGuard holds key patents
- Impact of XrML:
  - Microsoft implements XrML in its Unified DRM solution
  - ISO standard MPEG-21 “Rights expression language” (REL) based on XrML
  - Open eBook Forum adopted MPEG-21 REL
- Two key questions, to be separated:
  - How to specify the rights which are adequate in a certain situation
    - Addressed by Rights Modeling Languages
  - How to enforce that the usage obeys the rights
XrML Terminology: Grant

- Principal: Identification of a party to which rights are granted
- Right: A “verb” that the principal is granted to execute on a resource
- Resource: Object to which the grant refers (e.g. audio file or service)
- Condition: Specifies the terms under which the grant is valid

From XRML 2.0 Technical Overview
XrML Terminology: License

- *License* defines a set of grants
  - plus identification of issuer(s)
  - plus additional information like description, validity date, ...

From XrML 2.0 Technical Overview
XrML Content Extension

• Specific XrML language elements for digital multimedia content

• Specific rights:
  – File Management Rights (accessFolderInfo, backup, delete, ...)
  – Render Rights (export, play, print)
  – Transport Rights (copy, loan, transfer)
  – Derivative Work Rights (edit, embed, extract)
  – Configuration Rights (install, uninstall)

• Specific resources:
  – DigitalWork
  – DigitalWorkMetadata

• Specific conditions:
  – Helper (software to exercise a right)
  – Renderer (device to render a work)
  – Watermark (information to be embedded)

From XRML 2.0 Technical Overview
XrML Example (1)

- From: http://www.devshed.com
  (Trust, Access Control, and Rights for Web Services, Part 2)
XrML Example (2)

```
<license>
  <grant>
    <keyHolder licensePartId="Alice"> digital signature </info>
  </keyHolder>

  <service:use/>

  <serviceReference>
    WSDL definition of StockQuotes Online
  </serviceReference>

  <sx:fee>
    <sx:paymentPerUse>
      <sx:rate>
        <sx:amount>2.00</sx:amount>
        <sx:currency>US</sx:currency>
      </sx:rate>
    </sx:paymentPerUse>
    <sx:to> payment info </sx:to>
  </sx:fee>
</grant>
</license>
```
ODRL

- Open Digital Rights Language ODRL (www.odrl.net)
  - International initiative of various supporters (e.g. Nokia)
  - Officially accepted by the Open Mobile Alliance (OMA) (formerly known as WAP Forum)
  - XML language, standardized through W3C
ODRL Example

```xml
<permission>
  <play>
    <constraint>
      <container type="in-or">
        <cpu/>
        <storage/>
      </container>
    </constraint>
  </play>
  <requirement>
    <container type="ex-or">
      <prepay>
        <payment>
          <amount currency="AUD">200.00</amount>
        </payment>
      </prepay>
      <peruse>
        <payment>
          <amount currency="AUD">1.50</amount>
        </payment>
      </peruse>
    </container>
  </requirement>
</permission>
```
5 Digital Rights Management

5.1 Media Rights
5.2 Rights Models
5.3 Principles of Encryption-Based DRM Systems
5.4 Watermarking
5.5 DRM Standards and Selected Commercial Solutions

Literature:
Seth Schoen: Trusted Computing - Promise and Risk, http://www.eff.org/Infrastructure/trusted_computing
Encryption-Based DRM

• Content is transmitted to users only in \textit{encrypted} form
  – Not readable/playable without decoding using appropriate \textit{keys}
• A \textit{license} contains keys, coupled with \textit{rights}
  – Rights specified according to a rights model
  – Keys have to be inseparable from rights
  – Licenses can and should be separate entities from content files
    » Different licenses for same content
    » One license for many pieces of content
• \textit{User identities}
  – Ensure that rights are granted to a specific person or organization
  – Corresponds to the “principals” of XrML
• \textit{Device identities}
  – Ensure that restrictions on device usage are checkable
  – E.g. using some content only on a limited number of devices
A DRM Reference Architecture

Content Repository

Product Info

Content Packager

Encryption

Content

Metadata

License Server

Rights

Decryption Keys

Identities

 DRM License Generator

Encryption

Keys

Rights

License

Client

Content package

DRM Controller

Rendering Application

Identity

Content package
10 Steps To Play Protected Content (1)

1. DRM Packager
   - Encryption
     - Content
     - Metadata

2. Content package

3. DRM Controller

4. DRM License Generator
   - Encryption
     - Keys
     - Rights

5. Rights

6. Financial Transaction

7. License

8. License

9. Rendering Application

10. Identity
10 Steps To Play Protected Content (2)

(1) User obtains a content package, e.g. by download

(2) User makes request to exercise rights, e.g. to play or store the content

   Rendering software activates the DRM controller

(3) DRM controller determines identity of user and content and contacts license server

   May require user interaction, e.g. filling a registration form

(4) License server authenticates user against identities database

(5) License server looks up rights specification for the requested content

(6) If necessary, a financial transaction is started

   Financial transaction may happen also at another point in the process

(7) License generator combines rights information, client identity and decryption keys and seals them (packaged by encryption again)

(8) License is sent to the client

(9) DRM controller decrypts the content and hands it over to the rendering application

(10) Content is rendered for the user
Identification

- User identification
  - Supplied by user: User name, password
    » Can be passed on from user to user
  - Inherent: Biometric data
  - Supplied by trusted third party: Digital certificate

- Device identification
  - Serial number readable by software
    » Processor or other hardware components
  - IP address
    » Unsuitable, due to techniques like NAT (network address translation)
  - Combination of various identifying information
    » E.g. various serial numbers, MAC addresses, ...
Various Attacks on DRM

- Stealing encrypted content
- Stealing unencrypted content
- Stealing decryption keys
- Stealing identities
- Stealing licences
- Stealing rendered content
Integration DRM Controller – Rendering

• Coupling between DRM Controller and rendering application: has to be very tight
  – Intermediate storage of decoded data in file or socket would be harmful
• DRM Controllers in rendering software of high market domination
  – E.g. Adobe Acrobat, various eBook readers
  – E.g. Microsoft Windows Media Player, Apple iTunes & QuickTime
• DRM Controllers built into specialized devices
  – E.g. Apple iPod
• General problem:
  – Decoded digital signal has to be stored and transmitted somewhere (in the computer software)
  – Possibility to capture decoded signal on hardware or operating system level
    » Except with “trusted systems”…
Trusted Computing and DRM

• Microsoft initiative: “Palladium” architecture (later re-named “Next Generation Secure Computing Base (NGSCB)”)  
  – Bill Gates: “We came at this thinking about music, but then we realized that e-mail and documents were far more interesting domains.”  
  (Quotation according to Rüdiger Weis, cryptolabs)

• “Trusted Computing Platform Alliance” (TCPA), since 2003 called “Trusted Computing Group (TCG)”  
  (https://www.trustedcomputinggroup.org/)

• Authentication and validation of software and documents built into operating system and based on “tamper-proof” hardware  
  – Promises:
    » (Almost) unbreakable realization of DRM  
    » Complete control over software licensing  
    » Secure storage for sensitive information like electronic money or valuable keys  
    TPM = Trusted Platform Module
Key Concepts of Trusted Computing

- **Endorsement key:**
  - Unique key encoded in TPM hardware

- **Memory Curtaining**
  - Hardware-enforced memory isolation to prevent programs from reading or writing other program's memory
  - Excluding even the operating system from accessing curtained memory!

- **Secure Input/Output**
  - Secure hardware path to and from input/output devices

- **Sealed Storage**
  - Sensitive information like cryptographic keys is not simply stored but generated if authorized software runs on an authorized machine
  - Encrypted in a way including the identities of the encrypting program and the current hardware

- **Remote Attestation**
  - Unauthorized changes of software detectable from a remote system (before actually sending data to the suspicious system)
Pros and Cons of Trusted Computing

• Pro:
  – An effective countermeasure against threats by viruses, hackers etc.
  – Helps to ensure privacy and confidentiality of user data
  – Enables interoperability of systems over open networks
  – Respects privacy, keeps user in control

• Contra:
  – Can be misused for censorship and customer lock-in
  – Changing hardware becomes more difficult
  – Can create serious problems in case of failure (e.g. of TCM)
  – Collection and transmission of private data not transparent to users
  – Strengthens monopolies, reduces competition
  – Complicates the situation for open source software
  – Enables restrictive DRM