Digital Asset Management
数字媒体资源管理

4. Digital Rights Management

任课老师：张宏鑫

2008-09-19

浙江大学计算机学院
数字媒体与网络技术

Agenda

- Overview
- Introduction of DRM (Sony & DRM)
- Protecting Digital Intellectual Property
- Rights Expression Language (REL)
- Case Study – Existing DRM systems

DRM - Overview

- History and background of DRM
- Functional Architecture for DRM
- Key Players in DRM
- Business Imperatives for DRM
- The divide between content industry and IT industry
- DRM standards initiatives: decoding the alphabet soup
- Digital copyright law developments
- State of DRM market development and its future

DRM

- **Set of technologies that enable content owners to specify and control:**
  - the access they want to give consumers and
  - the conditions under which it is given.
- **It includes:**
  - **Persistent Protection:**
    - Technology for protecting files via encryption and allowing access to them only after the entity desiring access has had its identity authenticated and its rights to that specific type of access verified
  - **Business rights:**
    - Capability of associating business rights with a content by contract, e.g. author's rights to an article or musician's rights to a song
  - **Access tracking:**
    - Capability of tracking access to and operations on content
  - **Rights licensing:**
    - Capability of defining specific rights to content and making them available by contract

DRM Functional Architecture

- **IP Asset Creation and Capture Module**
  - Rights Validation to ensure content being created includes the rights to do so
  - Rights Creation to allow rights to be assigned to new content
  - Rights Workflow to allow for content to be processed through series of workflow steps
- **IP Asset Management Module**
- **IP Asset Usage Module**

DRM Functional Architecture

- **IP Asset Creation and Capture Module**
- **IP Asset Management Module**
  - Repository functions to enable the access/retrieval of content in potentially distributed databases and the access/retrieval of metadata
  - Trading functions to enable assignment of licenses to parties who have traded agreements for rights over content, including payments from licensees to rights holders (e.g., royalty payments)

- **IP Asset Usage Module**
  - Permissions Management to enable usage environment to honor the rights associated with the content, e.g., if user only has the right to view the document, then printing will not be allowed
  - Tracking Management to enable monitoring of usage of content where such tracking is part of the agreed to license conditions, e.g., user has license to play video ten times

Interested Players in DRM

- **Government Agencies**
  - Interested in controlled viewing and sharing of highly secure and confidential documents, audio and video data.
  - "Need to know basis"
- **Private Corporations**
  - Want to limit the sharing of their proprietary information
  - Track accesses and any modifications made to it.
  - E.g. news agencies like Reuters
- **Owners of commercial content**
  - Content owners, artists, and publishers want to gain revenue through sale and promotions
  - Concerned about protecting their copyrighted works from illegal use

Interested Players in DRM (cont.)

- **Intermediaries (service providers, content distributors etc.)**
  - Concerned about minimizing costs of providing services
  - Cautious about protecting themselves from lawsuits over illegal distribution
- **Producers of end user equipment (PCs, players, etc.)**
  - Concerned about minimizing design and production costs
  - Unwilling to pay for features that only some users need
- **End users**
  - Interested in immediate access to desired content
  - Want to use the content conveniently

Business Imperatives for DRM:

- Control Access During Workflow
- Downstream Use
- Modification of Rights Over Time
- Regulatory and Business Standards
- Outsourcing
- Protection throughout Content Life-cycle

Business Imperatives for DRM: Downstream Use

- Companies need to deliver controlled access downstream so that content can be licensed, deployed and repurposed by business partners in accordance with the terms of agreements.
  - CASE: Music publishers license DRM-enabled content to online transactional or subscription services. The DRM-enabled content allows both distributors and consumers to choose from multiple fee/ free business models. For example, the content could be included in both the free-play list for one-time use on multiple devices, or it could be licensed on a fee-for play use by media companies, publishers corporate, government or institutional users. Further, with DRM-enabled content, owners may chose to permit licensees the ability to re-distribute or enter into republication agreements.

An Example of DRM Implementation

OzAuthors

(An online e-book store)

Rights Interface

Publish ebook

OzAuthors

7 *Usage rights & pricing*

Usage	Details		Price
Preview	5 pages	Low-resolution Image (GIF)	Free
☐ Read	◉ Secure	○ Not Secure	$0.00
☑ Read & Print	◉ Secure	○ Not Secure	$10.00

8 *Revenue disbursement*

	Member Name	Reason	%
☐	Libby Gleeson	By (author)	80
☐	Renato Iannella	Illustrated by	10
☐	Dale Spender	Edited by	10

The Division

- **The content development industry:**

  (e.g., the recording industry and the movie studios)

  – the need for immediate DRM solutions that stop all unauthorized copying and distribution.

- **The IT industry:**

  – DRM solutions should support the concept of "fair use,"

    - allows consumers to make copies of some types of copyrighted content for their own personal use.

The Division

content provider

IT

- In the US, these disagreements have led to an increase in both DRM-related **lawsuits** and new legislative initiatives.

Fair Use

- Copyright principle based on **the belief**:
  - the public is entitled to freely use **portions of copyrighted materials** for purposes of **commentary and criticism**.

- Unfortunately, if the copyright owner disagrees with your fair use interpretation, the dispute will have to be resolved by courts or arbitration.
- The four factors for measuring fair use:
  - the purpose and character of your use
  - the nature of the copyrighted work
  - the amount and substantiality of the portion taken, and
  - the effect of the use upon the potential market.

Examples of Fair Use Court Cases

- **Universal City Studios v. Sony Corp., 464 U.S. 417 (1984)**
  - The Supreme Court determined that home videotaping of a TV broadcast was fair use.
  - One of the few occasions when copying a complete work was accepted as a fair use.
  - Evidence indicated that most viewers were "time-shifting" and not "library-building“
  - *Important factors:* The Supreme Court reasoned that the "delayed" system of viewing did not deprive the copyright owners of revenue.

- **Kelly v. Arriba-Soft, 03 C.D.O.S. 5888 (9th Cir. 2003)**
  - A search engine’s practice of creating small reproductions (“thumbnails”) of images and placing them on its own website (known as “inlining”) did not undermine the potential market for the sale or licensing of those images. **I**
  - *Important Factors.* The thumbnails were much smaller and of much poorer quality than the original photos and served to index the images and help the public access them.

- **Religious Technology Center v. Lerma, 40 U.S.P.Q. 2d 1569 (E.D. Va. 1996)**
  - Entire publications of the Church of Scientology were posted on the Internet by several individuals without Church permission. The court held that the use was not fair, since fair use is intended to permit the borrowing of portions of a work, not complete works.

Digital Copyright Millennium Act (DCMA)

- 1998 law designed to increase copyright holders' rights.
- Creates civil and criminal penalties for creation or distribution of DRM circumvention tools.
- As a result, a user attempting to circumvent copyright protection, even for legitimate reasons, violates federal law.
- What this means?
  - Open-source software developers rely on reverse engineering to write programs that can interact with hardware. This practice is illegal under the DCMA.
  - Reverse Engineering and Cryptanalysis can also be interpreted as illegal under the DCMA.
  - Is Norton Anti-Virus illegal?

Microsoft Palladium

- A system that combines software and hardware controls to create a **"trusted" computing platform**.
  - purports to stop viruses
  - store personal data within an encrypted folder.
  - depend on hardware that has
    - either a digital signature
    - or a tracking number.
  - filter spam.
  - incorporate DRM technologies for media files of all types (music, documents, e-mail communications).
  - + purports to transmit data within the computer via encrypted paths.

Major Legal Developments: Dmitry Sklyarov and Adobe eBook Copy "Protection"

- In June 2001, a Russian programmer named Dmitry Sklyarov published a program that can defeat a DRM technology used to secure Adobe eBooks.
- In July, at the behest of Adobe, the Department of Justice arrested Sklyarov for violating the DMCA shortly after he presented a paper on cracking Adobe ROT-13 copy protection.
- Sklyarov remained in jail for several weeks and was released on $50,000 bail. The Electronic Frontier Foundation (EFF) assisted in his defense and in December 2001, federal authorities dropped charges against him.
- Federal authorities have now pursued ElcomSoft, Dmitry Sklyarov's employer. The case is being litigated in Federal District Court in California.

Major Legal Developments: Ed Felten and Suppression of Academic Inquiry into DRM Systems

- In April 2001, a team of researchers headed by Princeton Prof. Felten announced that they could defeat a DRM system developed by the Secure Digital Media Initiative (SDMI).
- SDMI and the Recording Industry Artists of America (RIAA) threatened Felten and his team with a lawsuit under the DMCA. Felten's team decided not to publish the paper.
- Ultimately, SDMI and RIAA retreated from the treat of lawsuit, fearing that the DMCA may have been stricken as constitutionally overbroad when applied against a group of professors presenting an academic paper.
- In June 2001, the Electronic Frontier Foundation (EFF) bought suit against RIAA to obtain a declaratory judgment that Felten could present the SDMI research. Additionally, EFF sought the invalidation of the DMCA as an unconstitutional restriction on free expression.
- In August 2001, Felten presented the SDMI paper at the USENIX conference. In November 2001, a Federal District Court dismissed EFF's case. In February 2002, Felton decided not to appeal the dismissal.

References

- *"Integrating Content Management with Digital Rights Manangement"*, Bill Rosenblatt and Gail Dykstra, May 14 2003
- http://www.epic.org/privacy/drm/
- http://www.dlib.org/dlib/june01/iannella/06iannella.html
- http://www.eff.org/IP/DRM/

Agenda

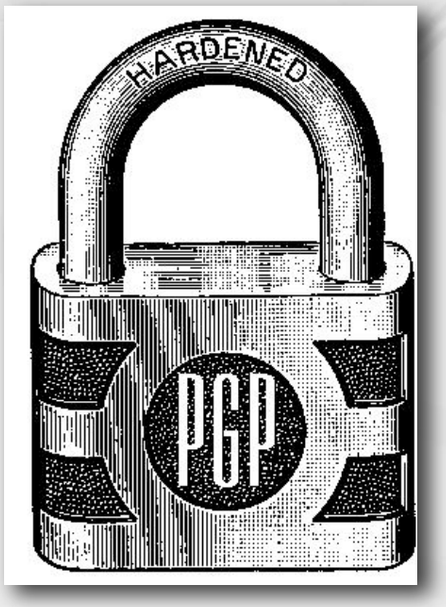
- Overview
- Introduction of DRM (Sony & DRM)
- Protecting Digital Intellectual Property
- Rights Expression Language (REL)
- Case Study – Existing DRM systems

DRM －Introduction (Sony & DRM)

- History
- DRM & Sony
- DRM Technology
- Sony Aftermath
- Review - Moral of DRM

Previous Technologies

- PKI – Public Key Infrastructure
- PGP – Pretty Good Privacy
- S/MIME
- Access Control Systems
- Smart Cards
- Biometrics



How are these technologies different to DRM?

- Only protect the data in transit
  - E.g. over the Internet or on CD
- Once the data is opened, it can be:
  - edited
  - copied
  - printed
  - saved as an unprotected file

And then

- Redistributed to anyone else in an unprotected format.

Rely on TRUST once the content is delivered

Sony & DRM

Sony's Problem:

- One of the big 4 music companies.
  - Copies of its music are easily made by **ripping** from CD's.
- BMG's music was continuously being illegally downloaded and shared across the internet.
  - Large sales being lost.
  - Hard to track popularity data

Sony's Response

"The industry will take whatever steps it needs to protect itself and protect its revenue streams...It will not lose that revenue stream, no matter what … **Sony is going to take aggressive steps to stop this**."

Sony's Solution:

- DRM!
- More specifically:
  - A **rootkit** concealing a software called 'Extended Copy Protection' was installed on every CD user's machine.

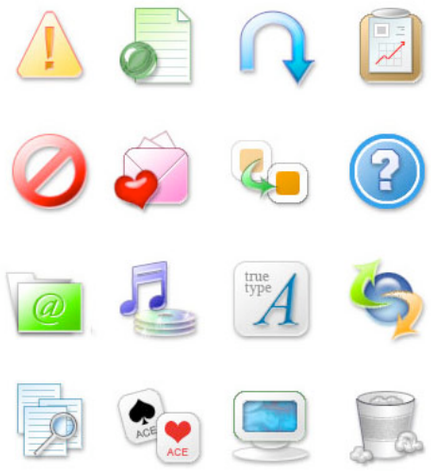
The Rootkit:

- Remains resident in the user's system
  - intercepting all accesses of the CD drive to prevent any media player or ripper software other than the one included with XCP-Aurora from accessing the music tracks of the Sony CD.
- Player software will:
  - Play songs
  - Allow only a limited degree of other actions
    - e.g., burning the music onto a certain number of other CDs or
    - loading it onto certain supported devices, e.g., a few portable music players. (iPod not supported)

So how technically does the Rootkit act as DRM?

Lets take a look at:
the DRM Technology Building Blocks

- rights holder
- end customer

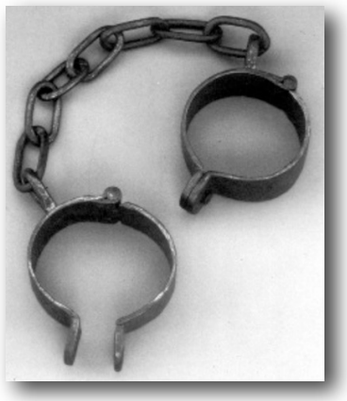


User

create/use

Content

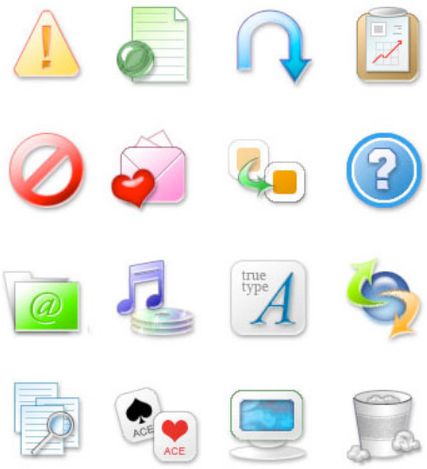
DRM basic Model



Rights

own

- rights holder
- end customer

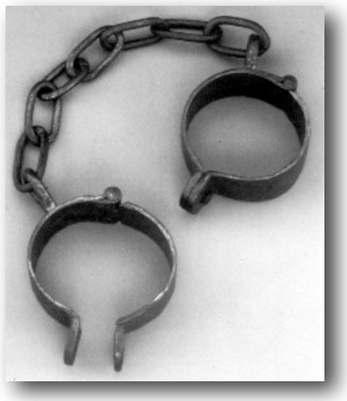


create/use

User

Content

DRM basic Model

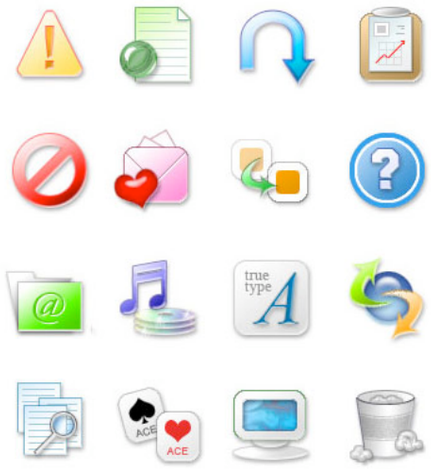


Rights

own

over

- rights holder
- end customer

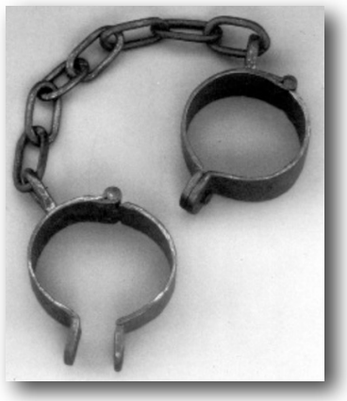


create/use

User

Content

DRM basic Model



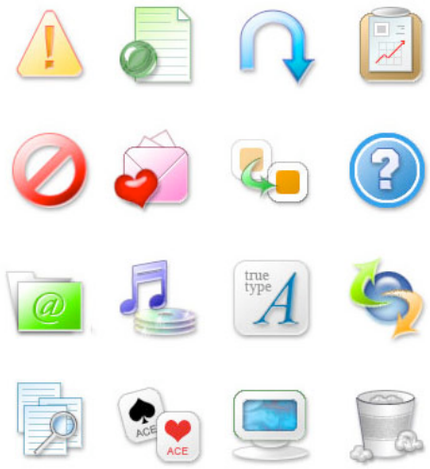
- permission
- restriction
- obligation

Rights

own

over

- rights holder
- end customer



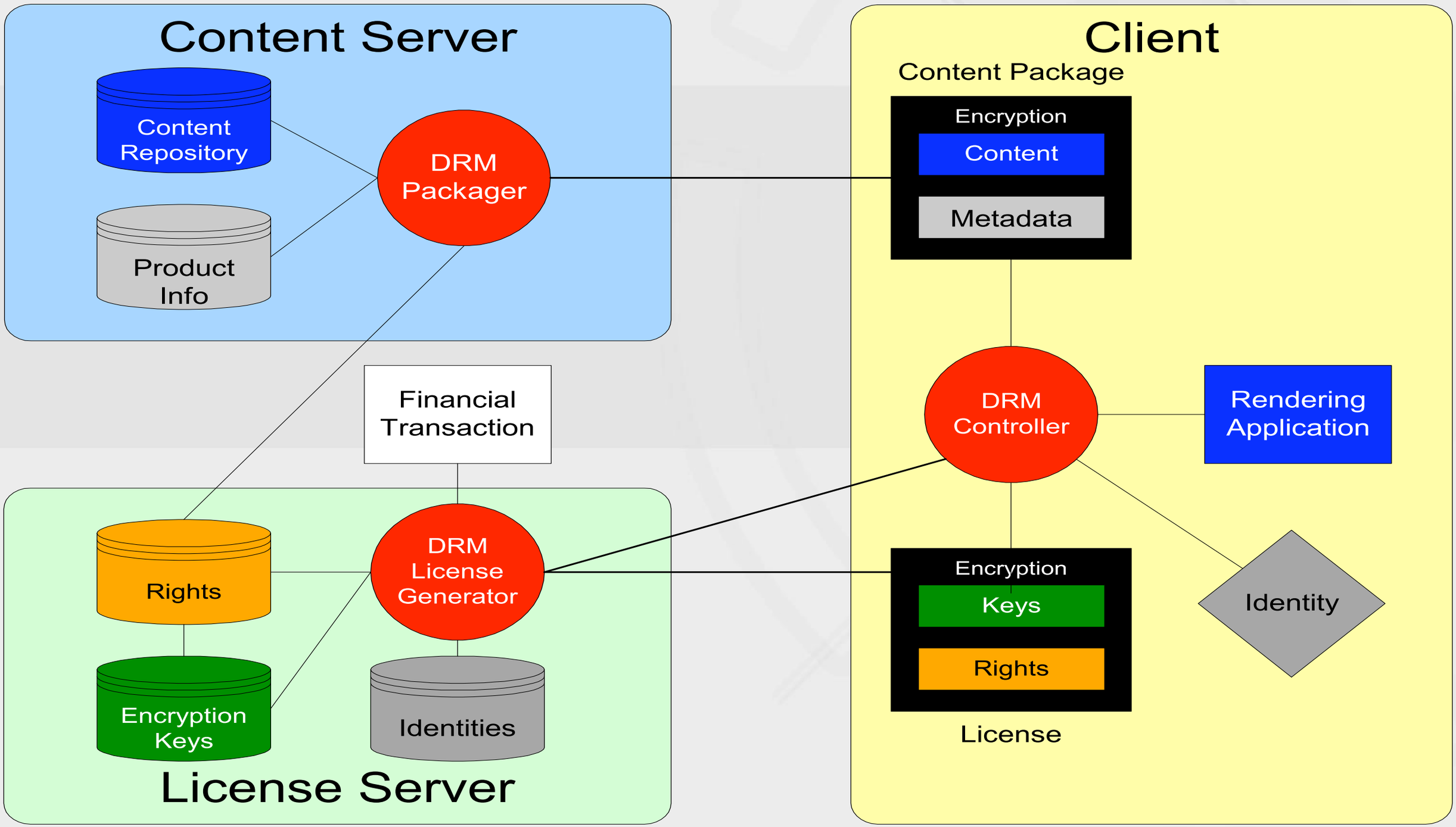
create/use

User

Content

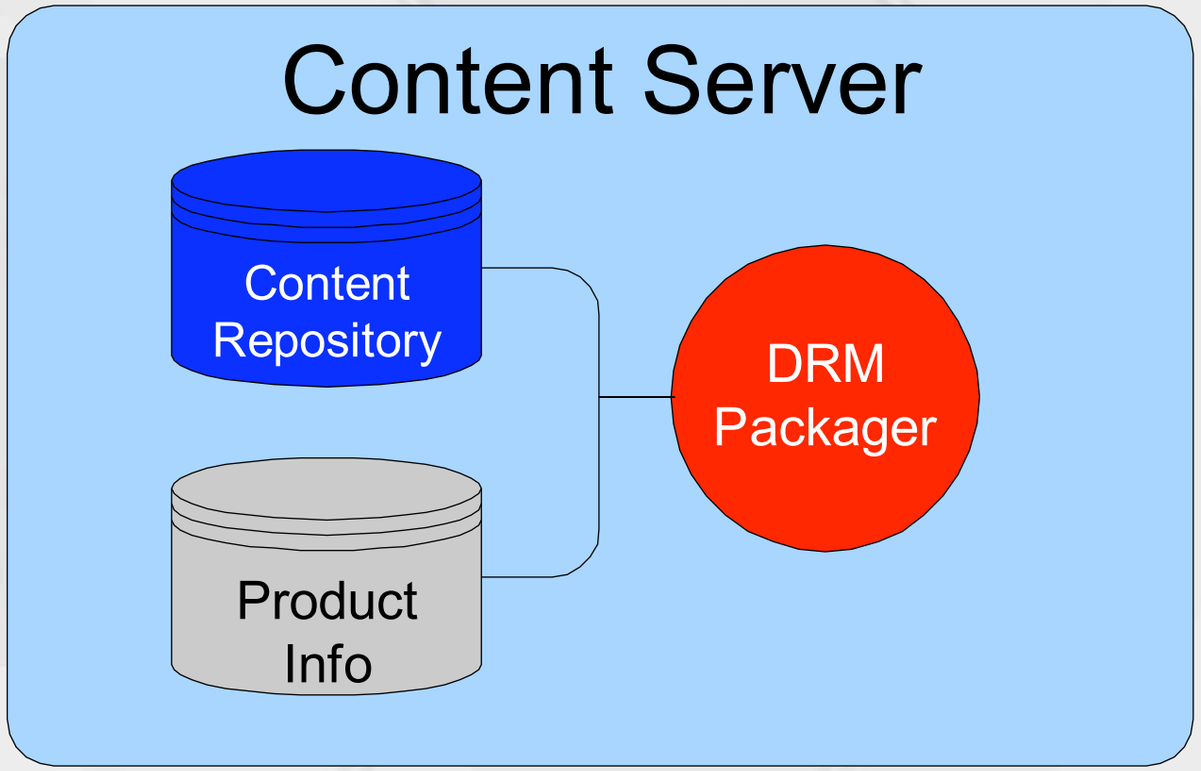
DRM basic Model

DRM Reference Architecture



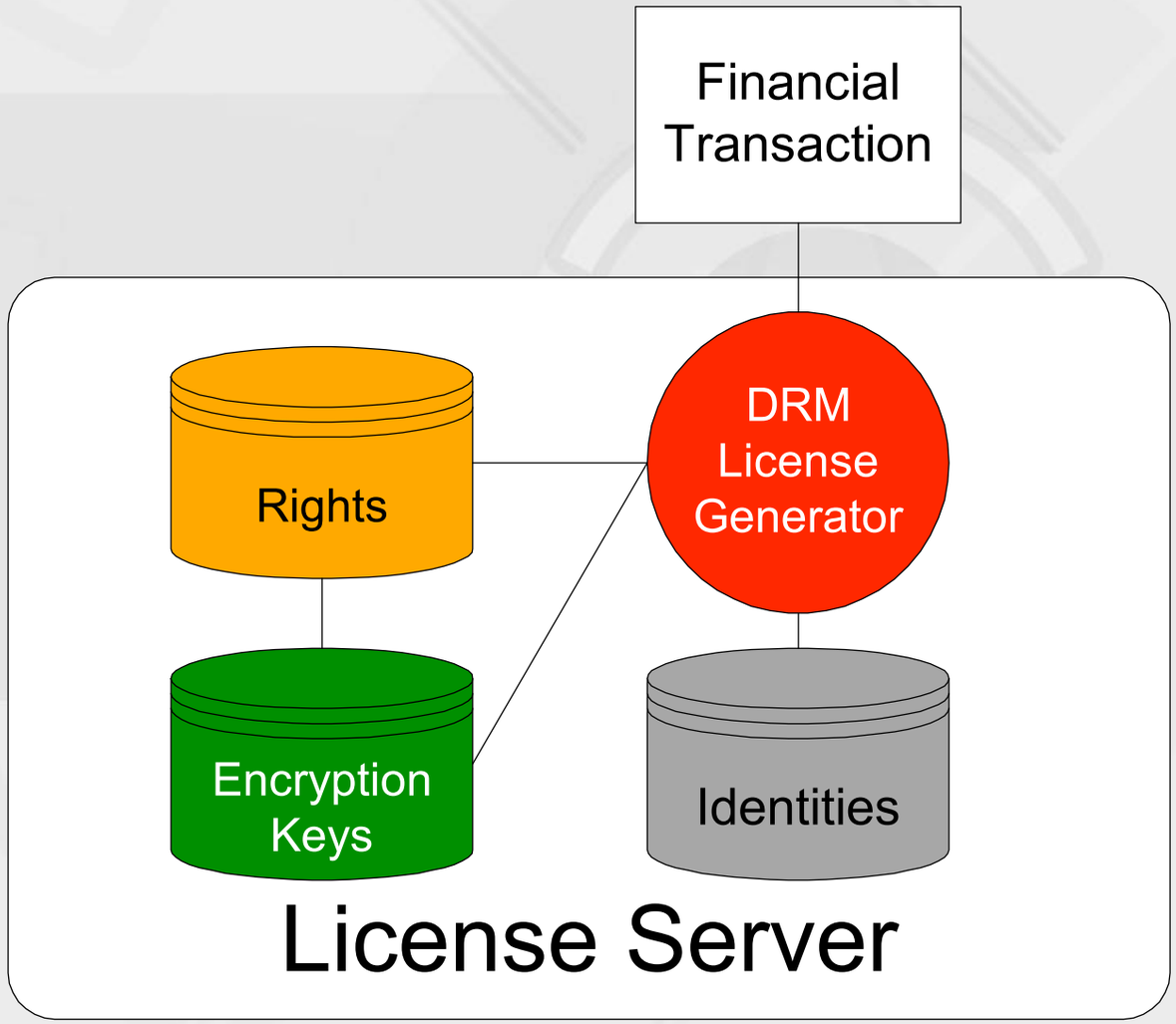
Content Server

- Content Repository
  - Content Management system
  - Digital Asset Management system
  - File server
- Product Info
  - **Rights**
  - Product metadata
- DRM Packager
  - Packages content with metadata
  - Encrypts



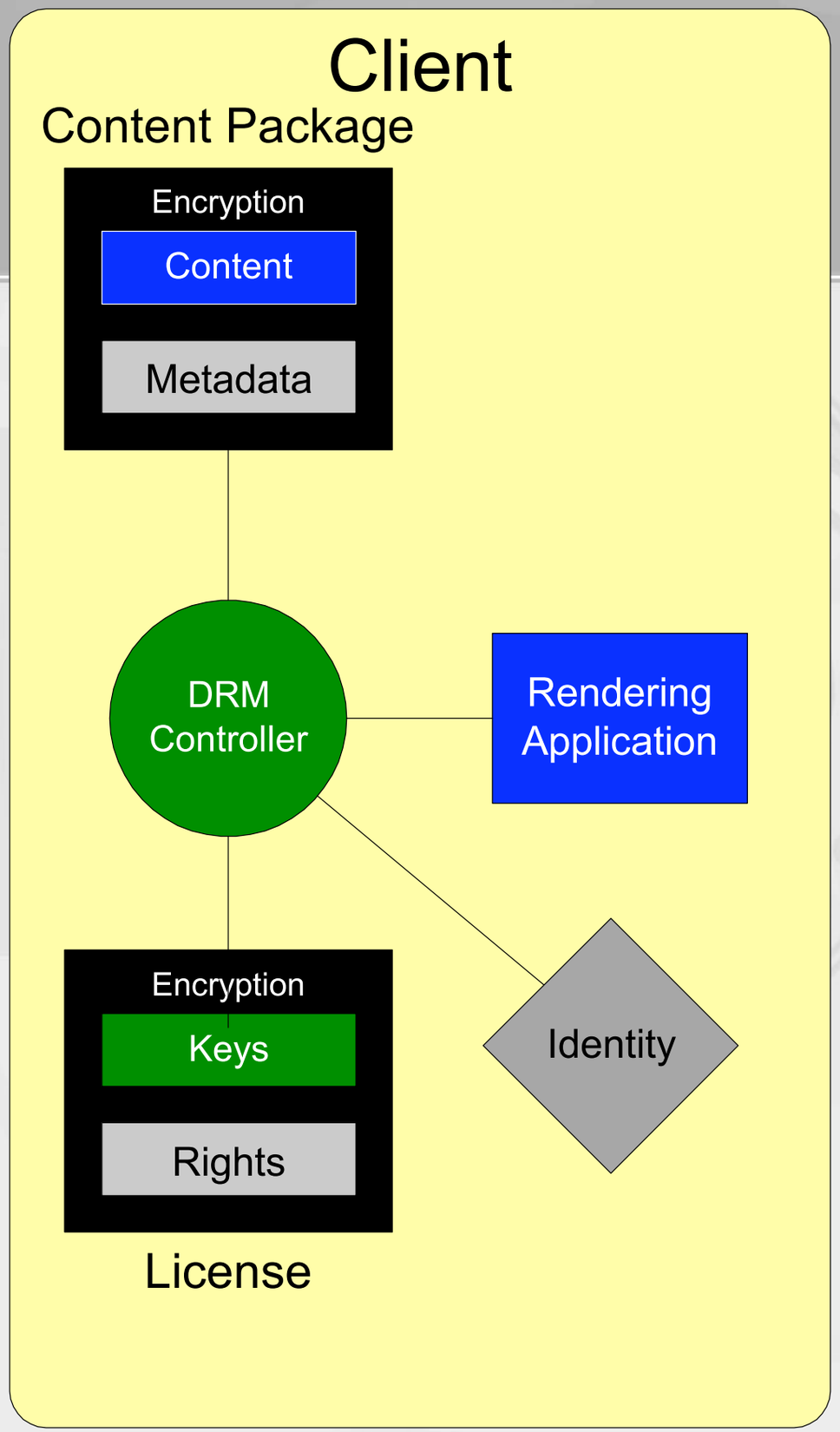
License Server

- Encryption key repository
- User identity database
  - Usernames
  - Machine IDs
- DRM License Generator



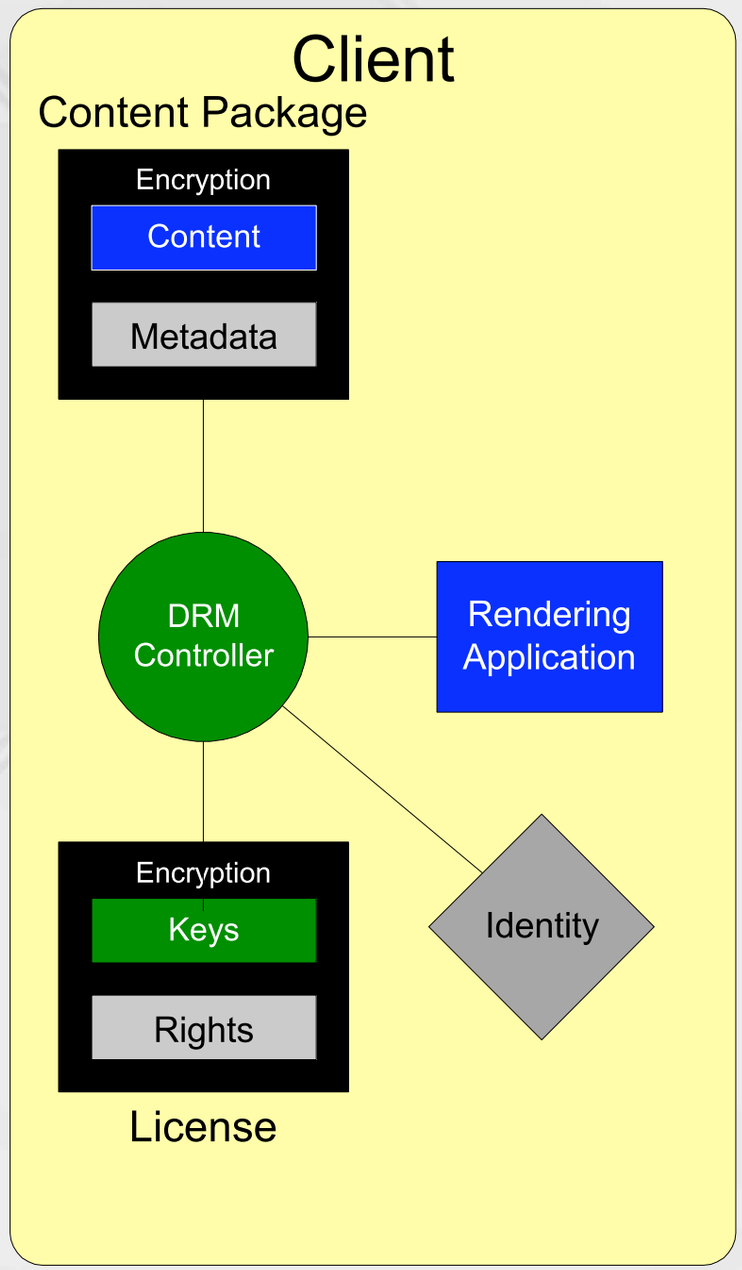
Client

- DRM Controller
  - Nerve center of process
- Rendering application
- Content packages
- Licenses
- Identity



Processes - User Initiation

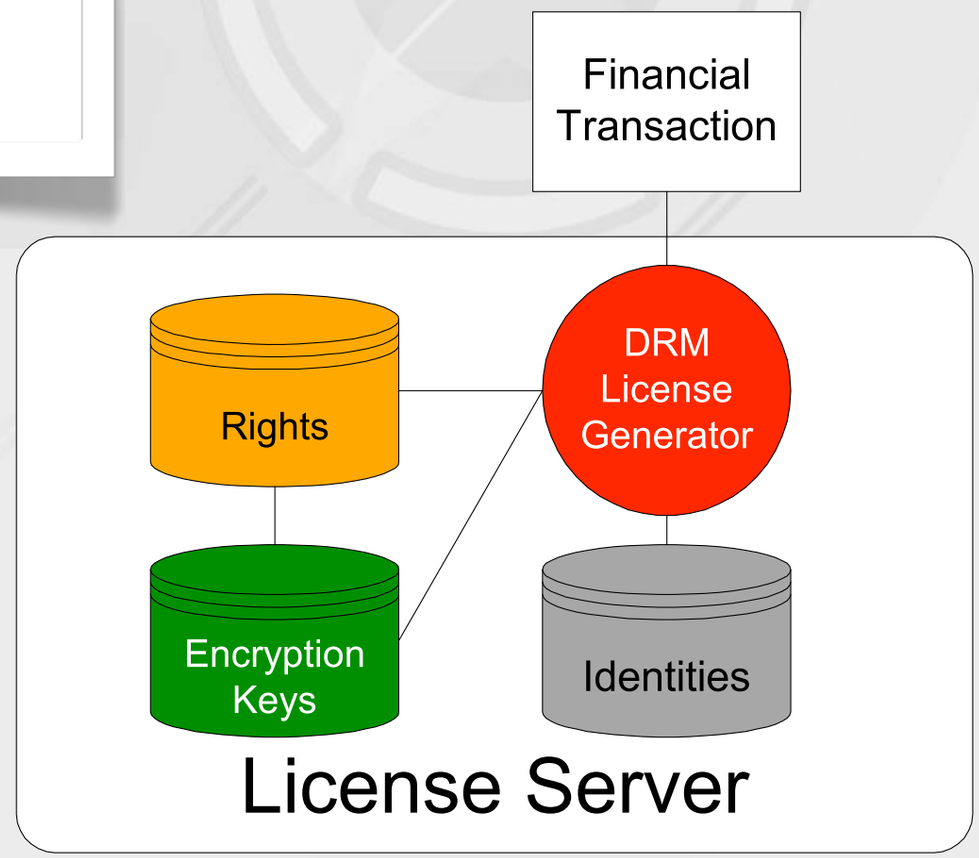
- User obtains content package
- User requests operation
  - –view, play
- DRM controller collects info
  - –Content
  - –Identity
  - –Requested rights
- DRM controller:
  - –license generator



Processes - License Generation

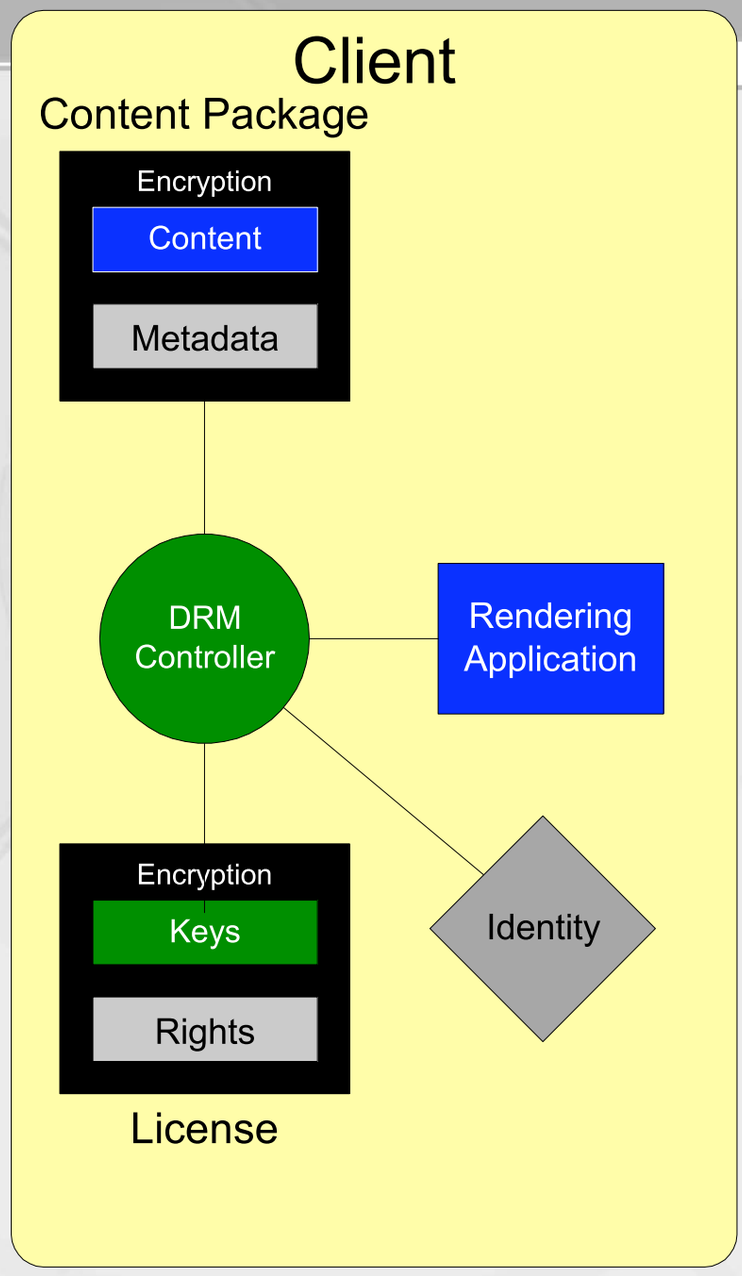
DRM License Generator…

- Checks content & identity
- Obtains keys from key repository
- Creates & sends license to client
- Generates financial transaction, where necessary

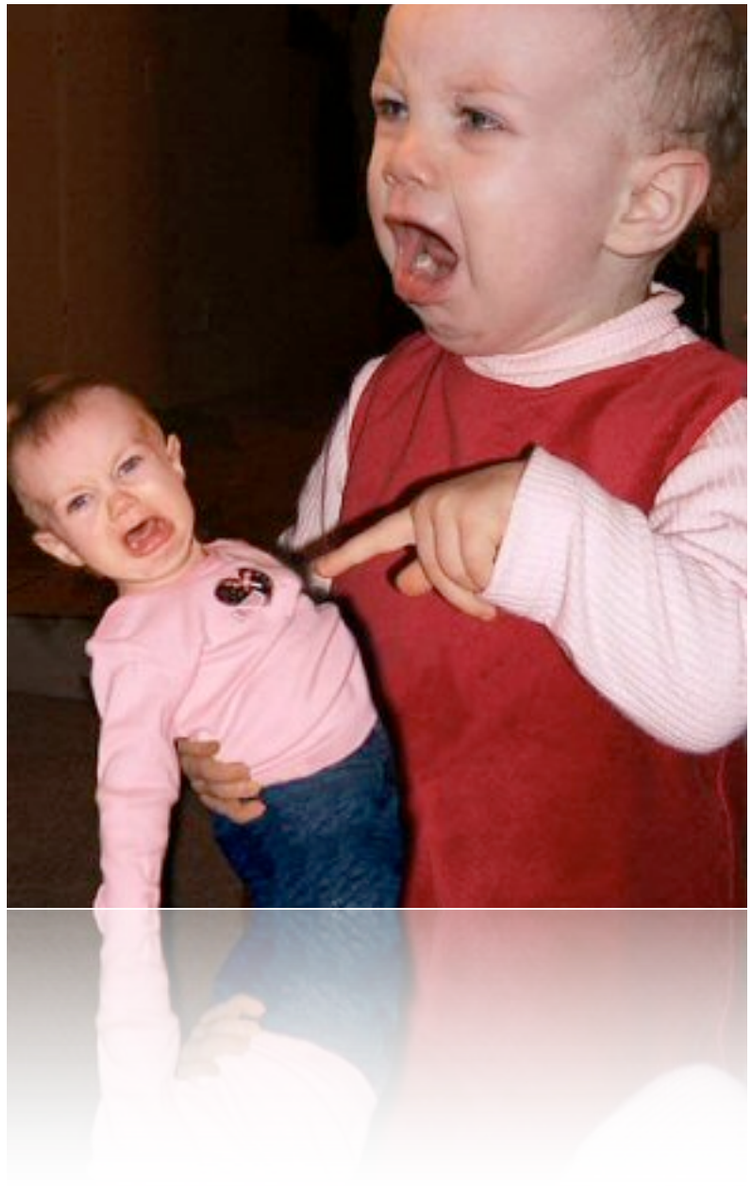


Processes - User Completion

- DRM Controller…
  - Receives license
  - Extracts keys from license
  - Decrypts content
  - Generates financial transaction, where necessary
  - Hands content to rendering application
- Rendering application plays content



What were the results of Sony's attempt at DRM?



What were the results of Sony's attempt at DRM?

Results of Sony's DRM Project:

- The rootkit was uninstallable
- Installing software without permission is illegal in many countries
- Rootkit left backdoors that could be exploited by viruses
- Sony under class action lawsuit

Public Outcry

- The head of Sony BMG's global digital business, Thomas Hesse, told National Public Radio

> "Most people, I think, don't even know what a rootkit is, so why should they care about it?"

- Turns out people did care
  - –Class action lawsuit in place against Sony
  - –Uninstaller finally released for the rootkit

Discussion:

- What is the fine line between acceptable restrictions on Digital Rights?

Moral of the story:

- A company has the right to protect their assets, but must do it within the boundaries of the law.

- DRM is an expanding technology, but it begins to infringe on other human rights. Paths around these controversial topics will need to be discovered before it goes truly mainstream.

Agenda

- Overview
- Introduction of DRM (Sony & DRM)
- Protecting Digital Intellectual Property
- Rights Expression Language (REL)
- Case Study – Existing DRM systems
  - InterTrust
  - IBM EMMS
  - Microsoft RMS
  - MacroVision for VHS tapes
  - Apple's FairPlay technology for ITunes

Protecting Digital Intellectual Property

- Understand technical background of Napster, DVD DeCSS, Sklyarov cases
- Representing and distributing digital IP
  - Compression
  - Distribution: CD's and DVD's
  - Distribution via the Internet
- Protecting digital IP
  - Encryption basics
  - DVD CSS, and how it was cracked
  - eBooks, and how they were cracked
- Social and legal issues
- Discussion: "Napsterizing" other industries

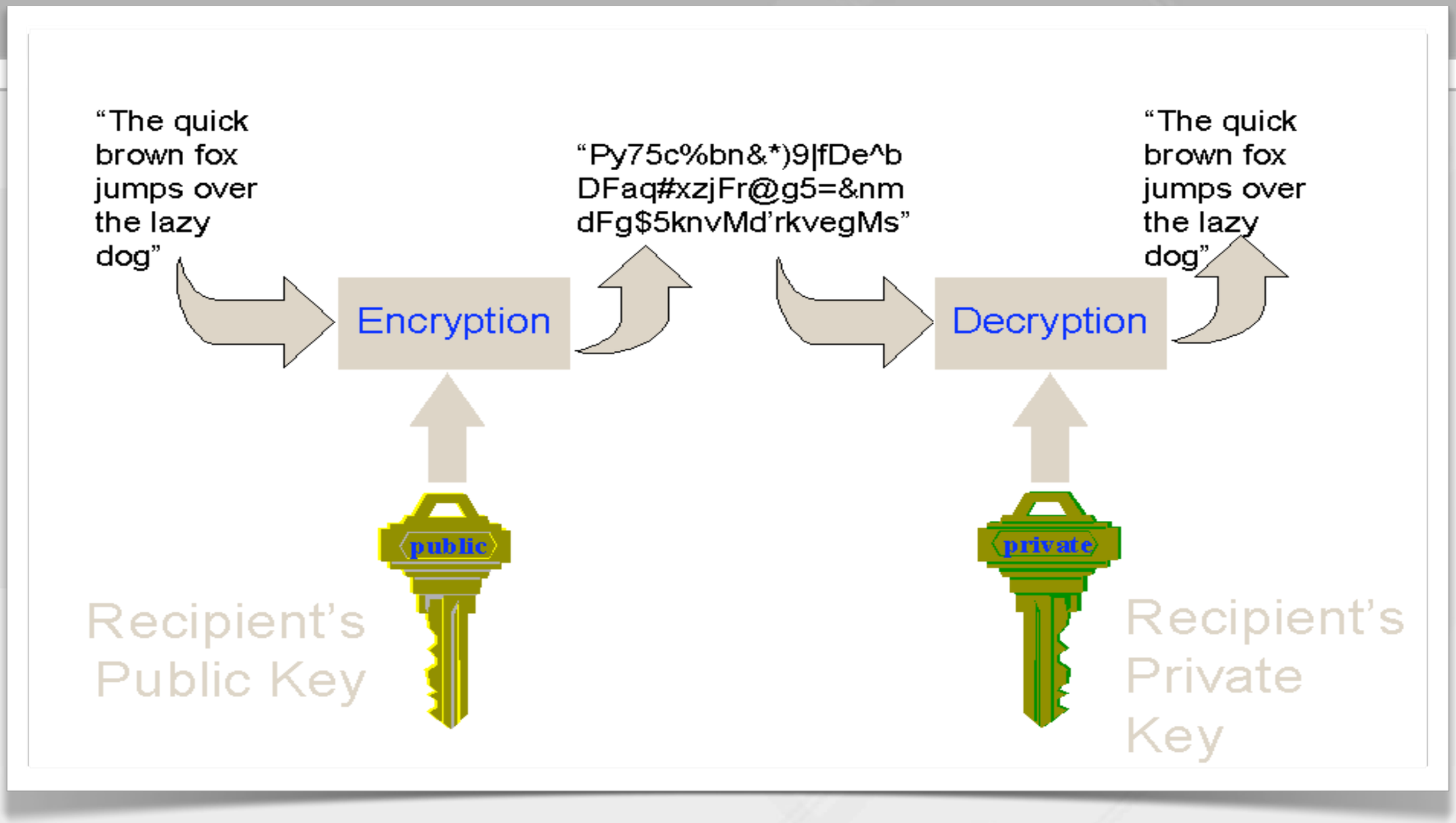
IP Protection Tactics

- Prevent Copying through technological means
  - Disallow copying in the first place
  - Use combination of encryption and trusted clients
- Prevent copying through legal means (DMCA)
  - Usually targeted at large scale piracy
  - Why is this hard to enforce against individuals?
- Track copies
  - if illegal copy detected, punish those who make/distribute them
  - Find the original owner of illegal copies
  - Uses digital watermarking

Preventing Copying With Encryption (加密)

- Encryption is the scrambling of a message
  - Simple one is Caesar encryption
  - To decrypt (decode) message, you need one or more *Keys*
  - Also need an encryption *algorithm*, that specifies how to apply the key to the message to produce the scrambled message
- Symmetric key crypto: same key used for encrypt/decrypt
- Public key (we'll talk about the details later…):
  - Keys come in matched pairs: one encrypts, other decrypts
  - Given one key, you cannot deduce the other

Basic Idea of Cryptography



Think of encryption key as sealing an envelope, and decryption key as unsealing it.

How do you “break” encryption?

- Usual assumptions of cryptography…
  - Adversary knows details of algorithm (not in WWII!)
  - Adversary may know something about nature of messages (why would this help?)
  - Adversary *doesn’t know decryption key(s)*
- Hard: exploit mathematical weakness in the algorithm
- Hard: guess key by (educated) trial and error
- Usually easier: attack some weaker part of the system
  - Usually, trick system into revealing a key
  - Chain is only as strong as weakest link!

DVD Content Scrambling System (CSS)

- To each **licensed DVD player** corresponds a **decryption key**:
  - P1, P2, …, Pn
- Each disc is encrypted under its own key, call it D
  - n copies of D are stored on the disc; each copy encrypted with one player's P
  - Player finds a D that it can decrypt, then uses D to play disc

- DVD player is a trusted client
  - It's not supposed to ever reveal any D, or its own P
  - What happens if either of these occur?
  - Why can't you convert DVD to another format?
  - Why can't you make direct copies of a DVD onto another disc (copying the D keys along with the content?)

Early DeCSS timeline...

- Sep ’99, DeCSS released as open-source Linux DVD player
- Dec ’99, DVDCCA sues 500 individuals in California for hosting DeCSS, alleging trade-secret violations
- Jan ’00, MPAA sues 2600.com in New York under DMCA’s copyright protection circumvention laws
- Jan ’00, DVD Source Code Distribution Contest
- Jan ’00 Jon Johansen arrested in Norway, later released
- Aug 00 MPAA wins DMCA suit in NYC

How Was CSS cracked?

- Idea =>
- P must appear somewhere in the decryption code of a trusted player
  - Hardware players difficult to reverse-engineer/probe
  - Software players maybe easier? …turns out yes!
  - Later analysis revealed weaknesses in CSS…it probably could have been broken *without* first recovering a key

- Original goal of CSS: even if one P is compromised, others are still sound
- Flaw: weakness in the algorithm allowed *all* P's to be compromised once a single P was found
  - Why wasn't this flaw discovered *before* the algorithm went into production players?

About eBooks

- **Secure eBooks** (and Adobe eBook Reader software)
  - User requires password to read/copy/print a document
  - Author of text controls what user is allowed to do…at fine grain!
  - Allows secure sale of electronic books without fear of piracy
  - Critics: disallows Fair Use (excerpting, making legitimate copies)

- **Dmitry Sklyarov**'s Russian company, **ElcomSoft**
  - 6/22 releases program that removes encryption from eBooks
  - 7/3 stops selling under pressure from Adobe, but continues to distribute demo version
  - 7/16 Sklyarov arrested in USA after speaking at DEFCON meeting
  - 8/28 Sklyarov faces 5 counts of violating DMCA, possible penalties up to 5 years imprisonment + $500K

How Were eBooks cracked?

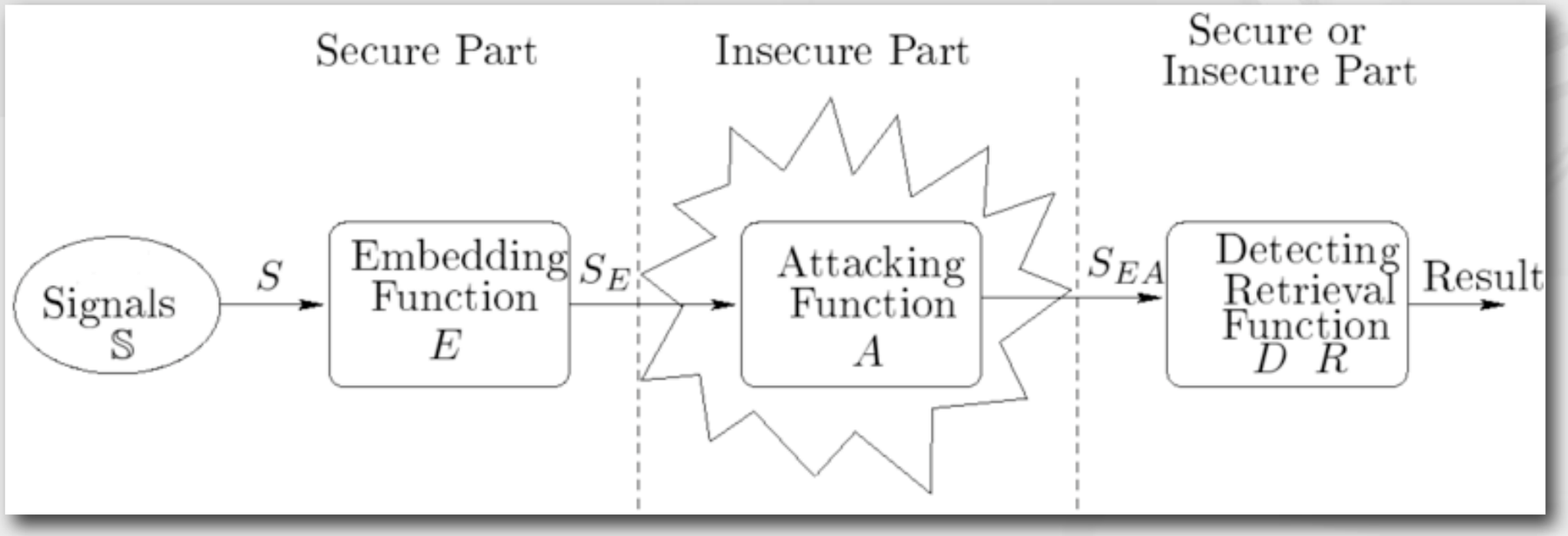
- eBooks encryption algorithm seems strong so far
  - Brute-force password guessing futile
- Idea: **Key must appear somewhere in eBook Reader**
  - Just as P keys must live somewhere in licensed players
  - Problem: only Adobe-certified “trusted” plug-ins are allowed to inspect Reader code
  - Flaw: plug-in certification mechanism is insecure
  - ElcomSoft hacked a trusted plug-in to do its bidding
- Another trusted client whose security was only as strong as the weakest link!

DeCSS and Sklyarov Issues

- Technical
  - Can there be perfect digital IP protection? (…no)
  - How to enable it on the Internet?
  - Loaded question: Does CSS prevent the unauthorized copying of DVD's? (pre-cracking)
- Legal
  - Fair Use: how should it apply to digital media? To what extent should content creators be allowed to control use of their content?
  - Is computer code considered protectable free speech?
  - How about wearing a t-shirt containing the code?
  - How about linking to a page containing code? (Is that more like telling a friend, or more like being a distributor?)
  - Prosecuting foreign nationals under DMCA?

Preventing Copying With Watermarking (水印)

- digital art
- 票据防伪
- 数据隐藏
- 隐蔽通讯



Agenda

- Overview
- Introduction of DRM (Sony & DRM)
- Protecting Digital Intellectual Property
- Rights Expression Language (REL)
- Case Study – Existing DRM systems

Digital Rights Management – Rights Expression Language (REL)

Rights model

- Render rights
  - View, Print, Play or Execute
- Transport rights
  - Copy, Move, Loan
- Derivative work rights
  - Edit, Embed, Extract
- Utility rights
  - Backup, Caching, Data integrity

Digital Rights Expression Languages

- Rights may be managed using digital rights expression languages.
- DRELs specify the permissions given to
  - users, distributors and repositories
  - and the conditions and obligations that have to be satisfied for these permissions to be exercised.

Rights Expression Language (REL)

- A standard way to express and interpret rights specification for interoperability.
- Comprehensive, generic, precise and extensible.

- eXtensible rights Markup Language (**XrML**).
  - XrML 2.0 : MPEG REL
- Open Digital Rights Language (**ODRL**).
  - ODRL 1.1 : OMA (Open Mobile Alliance) REL

General description of RELs

- A rights expression language (REL) is a type of policy authorization language.
  - Focus is on expressing rights granted by one party to another.
  - Issuance and delegation rights for other grants are core concepts.
    - Can be used to model lending, loans, transfers of rights.

- REL design goals:
  - Provide a flexible, extensible mechanism for expressing authorizations.
  - Enable interoperability across various policy evaluation systems.
  - Make it easy for policy authors (e.g. content owners) to express their desired policies.

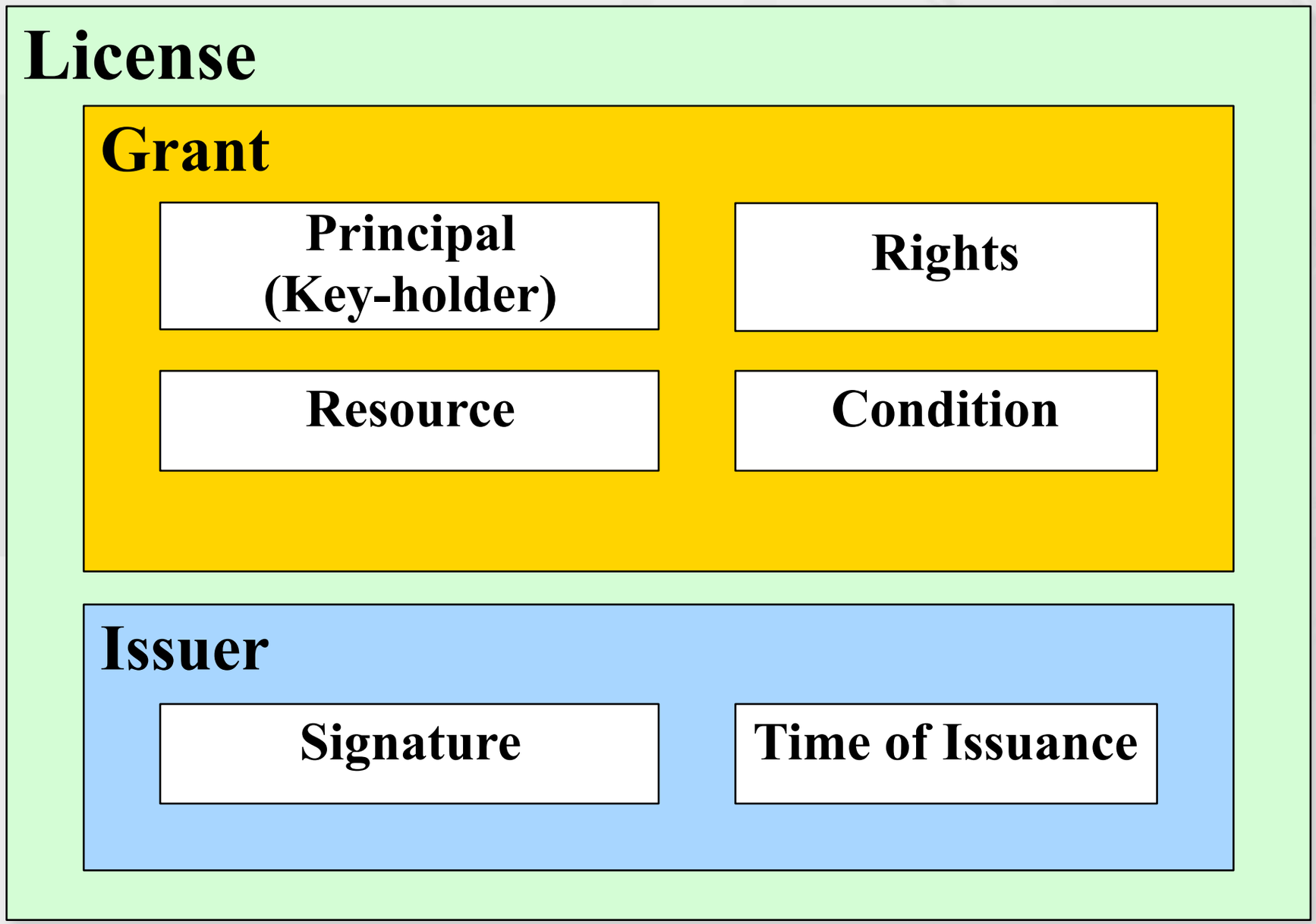
An example REL: XrML 2.X

- XrML, the *XML Rights Management Language*, is a standard currently under development

XrML introduction

- The only REL in working DRM systems.
- Specification language:
  - Programmers specify high-level rights in a license file.
  - An XrML interpreter parses the license file.
  - REL SDK for building an XrML interpreter.
- Data model:
  - License, grant, principal, right, resource and condition

XrML license



XrML 2.X

- In the RM context, XrML 2.X allows content owners a systematic way to express their intent for distribution and consumption.
- Like other policy languages, XrML 2.X **licenses** (statements) declare authorizations, but cannot enforce compliance.
  - Systems that consume XrML 2.X licenses must be trusted by the license issuer to properly enforce the grants specified within the license.
- Licenses are digitally signed by the issuer to protect their integrity.
- Licenses may be embedded within content or move independently.

Semantic of a Grant

- Every XrML 2.X grant has the following form:
  - Issuer authorizes principal to exercise a right with respect to a resource subject to conditions.
  - A license is a collection of one or more grants made by the same issuer.

- Grants may be chained together:
  - Bill's RM system trusts Tom and his delegates.
  - Tom delegates the right to license printing to John.
  - John issues a license: "Bill has the right to print the book."
  - Therefore Bill can print the book.

Sample XrML 2.X License

```
<?xml version="1.0" encoding="UTF-8" ?>
 <license>
 <grant>
  <keyHolder>  …  </keyHolder>
 <mx:play />
 <mx:diReference>
 <mx:identifier>urn:mpeg:example:2002:twotonshoe:album</
  mx:identifier>
 </mx:diReference>
</grant>
<issuer> … </issuer>
```

XrML authorization model

- Input
  - Principal
  - Right
  - Resource
  - Time interval
  - Licenses
  - Designated “root grants” (implicitly trusted)

- Output
  - “No”
  - “Yes,” unconditionally
  - “Maybe,” if a set of conditions are also met

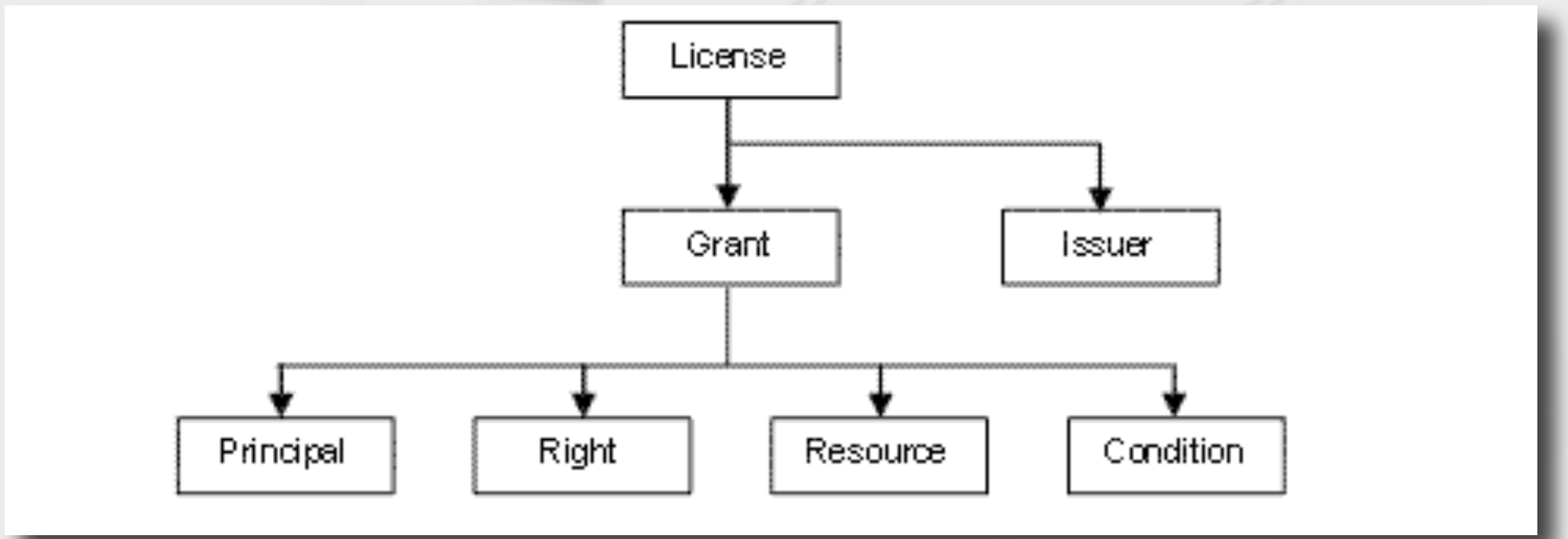
XrML Key Language Features

- Mechanisms for enhanced expressivity
  - Patterns, variables and quantifiers
  - Grouping grants
  - Delegation
- Meta-rights
  - Issue
  - Obtain
  - Revocation
  - PossessProperty
- Linking conditions
  - PrerequisiteRight

MPEG-21 REL

- Derived from XrML
- 3 Components:
  - Kernel set
  - Standard extension
  - multimedia extension

structure of a simple license



Agenda

- Overview
- Introduction of DRM (Sony & DRM)
- Protecting Digital Intellectual Property
- Rights Expression Language (REL)
- Case Study – Existing DRM systems

Case Studies

InterTrust

- Original DRM vendor (with IBM)
  - May have coined the term
  - Originally called Electronic Publishing Resources
  - First implementations in hardware
  - Major patent portfolio
- New technology: Rights|System
  - Framework for multiple devices
    - Rights|Desktop for PCs
    - Rights|TV for settop boxes
    - Rights|PDA for handheld devices
    - Rights|Phone for Symbian mobile phones
  - Public encryption algorithms

IBM EMMS

- Developed in IBM labs over period of 8 years
- Cross-device, like InterTrust
- Integration with IBM server components
  - WebSphere
  - DB2
  - Service Provider Delivery Environment (SPDE)

Microsoft

- 1st generation: Windows Media Player
- 2nd generation: Digital Asset Server
  - Server for Microsoft Reader E-Books
  - Uses subset of XrML
- 3rd generation: “Unified DRM” (RMS)
  - One DRM for all devices & platforms
  - Open API for rendering app developers
  - XrML based

MacroVision (1985-)

- Copy protection technique for VHS tapes
- Inserts special signals into the vertical blanking interval of NTSC protocol
  - affects automatic gain control in most VCRs, but is ignored by most televisions
  - difficult to remove from the original signal
- Makes subsequent recordings shake and have periods of bright and dark frames

Apple's FairPlay Technology

- DRM for iTunes
  - playing, recording, and sharing of files
- Moves beyond "protection only"
  - allows media to be shared among devices
  - allows others to listen to (but not copy) music
  - allows music to be burned to an audio CD, which loses the DRM protection

How FairPlay Works

- iTunes uses encrypted MP4 audio files
- Acquire decryption key by trying to play song
  - player generates a unique ID
  - sends this ID to the iTunes server
  - if there are fewer than N authorizations in your account, the server responds with decryption key
- The decryption key itself is encrypted so cannot be given to another machine

Discussion

- Is FairPlay too lenient, too stringent, or just about right?
- What is your experience with this DRM?
- What happens if Apple decides to stop supporting FairPlay?