A security analysis of business models for digital products

INDICARE Workshop on DRM

3rd February 2005

Prof. Dr. Rüdiger Grimm
Institute for Media and Communication Study
Technische Universität Ilmenau
and
Fraunhofer Institute for Digital Media Technology

Content

1. Security
2. Digital Rights Management
3. Role of payment
4. New business models
5. PotatoSystem
What Can Happen in the Internet

- Eavesdropping
- Theft
- Change, delete
- Identity fraud
- Repudiate

  - Loss of access: No music
  - Loss of control: No payment
- Viruses
- Privacy attacks: No trust
- SPAM

IT Security

- The aim of an „attack“ is a personal advantage of the attacker on the cost of the attacked.
- Security problems stem from conflicts of interest between human actors.
Digital Rights Management - Aims

- To imitate physical properties of goods
- Uniqueness
- No cheap copy
- Or to behave as specified by rights owner

Rights and Usage Rules

- Rights are encoded within media format
- Copy protection
- Usage restriction
  - Loss of quality (copies, pre-listening)
  - Number of copies
  - Number of replays
  - Time limits for replays
  - Usage environment for replays
Rights Enforcement

Content Provider

- Specifies rights
- Sells content
- Controls usage

User executes usage rules

User executes usage rules

User executes usage rules

User executes usage rules

Security Analysis for DRM

<table>
<thead>
<tr>
<th>Provider</th>
<th>Consumer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value / Goods</td>
<td>Value / Goods</td>
</tr>
<tr>
<td>Music data as product</td>
<td>Music data as quality product</td>
</tr>
<tr>
<td>Unpaid sharing</td>
<td>Unavailability</td>
</tr>
<tr>
<td>Attacks/Threats</td>
<td>Security Requirements</td>
</tr>
<tr>
<td>Integrity, Quality,</td>
<td>Integrity, Quality,</td>
</tr>
<tr>
<td>Product-Money-Binding,</td>
<td>Fair-Price, Availability</td>
</tr>
<tr>
<td>Uniqueness</td>
<td>Safe Distribution</td>
</tr>
<tr>
<td>Security Mechanisms</td>
<td>Copy protection</td>
</tr>
<tr>
<td>DRM</td>
<td>Forwarding → P2P</td>
</tr>
</tbody>
</table>

© Grimm TU Ilmenau 2005
Interest vs. Enforcement

- Content providers have interest in rights
- Content providers specify rights and policies
- Rights restrict usage
- Burdon on enforcement solely on users
- Users have interest in private use
- Users circumvent rights

Market is destroyed

Role of Payment

Payment System

fair exchange

Ginny
Consumer
Wants Product

Fred
Provider
Wants Money

© Grimm TU Ilmenau 2005
Requirements

- Immediate money flow
- Low transaction costs
  - Bank clearance of micromoney expensive
- Other models
  - credit cards, subscription, packaging, intermediaries
- Additionally: fair exchange protocols

Payment Models

- Prepaid
  - HW (Chipcard, GeldKarte) *
  - SW (Paysafecard, Micromoney, Paybest Telefone TANs) *
- Intermediary
  - Credit Card (SSL, Visa 3D Secure)
  - Accounting (Paypal, Moneybookers, Firstgate, Paybest) *
  - Escrows for fair exchange (S-ITT)
- Traditional
  - Invoice
  - Bank withdrawal

* good for micropayment
Payment + Purchase Integration

- Physical goods escrow
  - Product delivery and money transfer through third party (eBay)
- Download proxy
  - Firstgate, Paybest
- Virtual accounts
  - Multiple purchase
  - Packaged clearance
  - „Paid“ signal
  - Prepaid, accounting and escrow systems

PayBest

- Account Service for multiple purchase and packaged clearance
- Download proxy
- Multiple Payment methods included
  - Paypal, Moneybookers, Firstgate Click&Buy, Paysafecard, Micromoney
  - Original telefon TAN
- Integration of payment and purchase by Web Services
DRM and Alternative Models

Users behave correctly because of

1. Technical enforcement
   • „Classical“ DRM
   • Windows Media, Sony Connect, Apple’s iTunes

2. Identification of misuse
   • LWDRM, M2S

3. Incentives
   • Users and providers cooperate
   • PotatoSystem, M2S
Windows Media Rights Manager

1. Package Media
   - Digital Content
   - Protected Media

2. Post Media
   - Web Server
   - Streaming Media Server

3. License Terms
   - Clearing House License Server

4. Request and Receive Media
   - Request Licence
   - Download License

5. Transfer to Portable Device
   - License Terms
   - Media Player with Windows Media Rights Manager

iTunes Music Store, Apple

1. Server
   - Authorisation via Internet
   - Download to PC via Internet

2. Customer
   - Laptop
   - PC Desktop

3. Mobile Players, iPods
   - Copy to Player
   - Burn to CD

© Grimm TU Ilmenau 2005
**iTunes Music Store, Apple**

- Free copy of music in private home network
- Free private copies on CD
- Only 5 PCs authorized to play music
- Secial format with authorization id
- Warning if PC is not authorized to play music
- MP3 reproduction out of scope

**LWDRM® - Basic Idea**

- **Aims**
  - Respect of user interest (Fair-Use, Privacy)
  - No clear text on user site (encryption of content)
  - Identification of misuse

- Technically, a customer can copy and forward content, if he digitally signs it (SMF)
- Otherwise, content is bound locally to an individual end-user device (LMF)
Incentives

• Provision (Potato)
  – Users share income

• Services (Potato, M2S)
  – Users get more:
    – Cover, info, albums
    – „from radio/concert/pub to an album“

• Guarantee of quality, upgrade (M2S)

• Community (Potato)
  – Users get contact to other users (Matching Service)

The PotatoSystem brings Users and Providers together

• Users are motivated to pay for the good, because they can resell and earn money

• Users become active redistributors (good for both, users and providers)

• No copy protection mechanisms

• More user services: redistribution right, user matching, fan infos, combination with CDs and concert tickets
Sales Process

Fred is an Original Supplier

Ginny buys Fred’s Song

mysong.mp3

Ginny’s Browser

Payment-Server

HTML-Jacket-Server

Accounting-Server

SQL

Data Transfer

Song Selection

Payment - Server

HTML-Jacket - Server

Proxy

Payment - Server

HTML-Jacket - Server

Accounting-Server

Web File Server of Original Supplier

mysong.mp3

After Payment Ginny is registered Reseller

• She may publish her own sell link in the Web:
  https://www.potatosystem.com/process/sell?tan=88099176227

• Or embed a mini HTML page (per iframe-Code):

  frameborder='0' scrolling='no' marginheight='0' marginwidth='0'> </iframe>
Resale

Payment - Server

HTTP

HTML Jacket - Server

XML

Accounting - Server

Web - Service

SQL

Fred is an
Original Supplier

Web File - Server of
Original Supplier

Ginny’s Web Page

Payment - Server

Payment Server

Potato System

HTML - Jacket Server

Potato System

HTML Jacket - Server

Accounting - Server

Web - Service

SQL

Web - File - Server of
Original Supplier

Ginny’s Web Page

Resale

Payment - Server

HTTP

HTML Jacket - Server

XML

Accounting - Server

Web - Service

SQL

Web File - Server of
Original Supplier

Ginny’s Web Page

Resale

Payment - Server

HTTP

HTML Jacket - Server

XML

Accounting - Server

Web - Service

SQL

Web File - Server of
Original Supplier

Ginny’s Web Page

Resale

Payment - Server

HTTP

HTML Jacket - Server

XML

Accounting - Server

Web - Service

SQL

Web File - Server of
Original Supplier

Ginny’s Web Page

Provisions

35% to OS

15% to OS

5% to OS

B1

B2

B3

B4

B1 buys song “A” from F

B2 buys song “A” from B1

B3 buys song “A” from B2

B4 buys song “A” from B3

OS = Original Supplier (e.g., a Label), B1 ... B4 = Buyer 1 bis 4

Jürgen Nützel, 4FriendsOnly.com

© Grimm TU Ilmenau 2005

25/28
The PotatoSystem offers as Web service

• Account management for content owners and customers
• Payment clearance (Paybest)
• Delivery of purchased songs from provider server to the buyer via secure proxy
• Provision management
• Detailed receipts for providers
• Rights management (GEMA)
• Combinationen with real CDs and concert tickets
• More functions under construction …

Conclusion

• Users are ready to pay for fair use
• Providers are ready to deliver for payment
• The common bracket is „payment“
• Pure DRM is not sufficient
• Payment is integrated part of purchase
• Free usage after payment is required
• See, for example, Potato and Paybest: