
Privacy for Digital Rights Management Products and their Business Cases

Rüdiger Grimm,

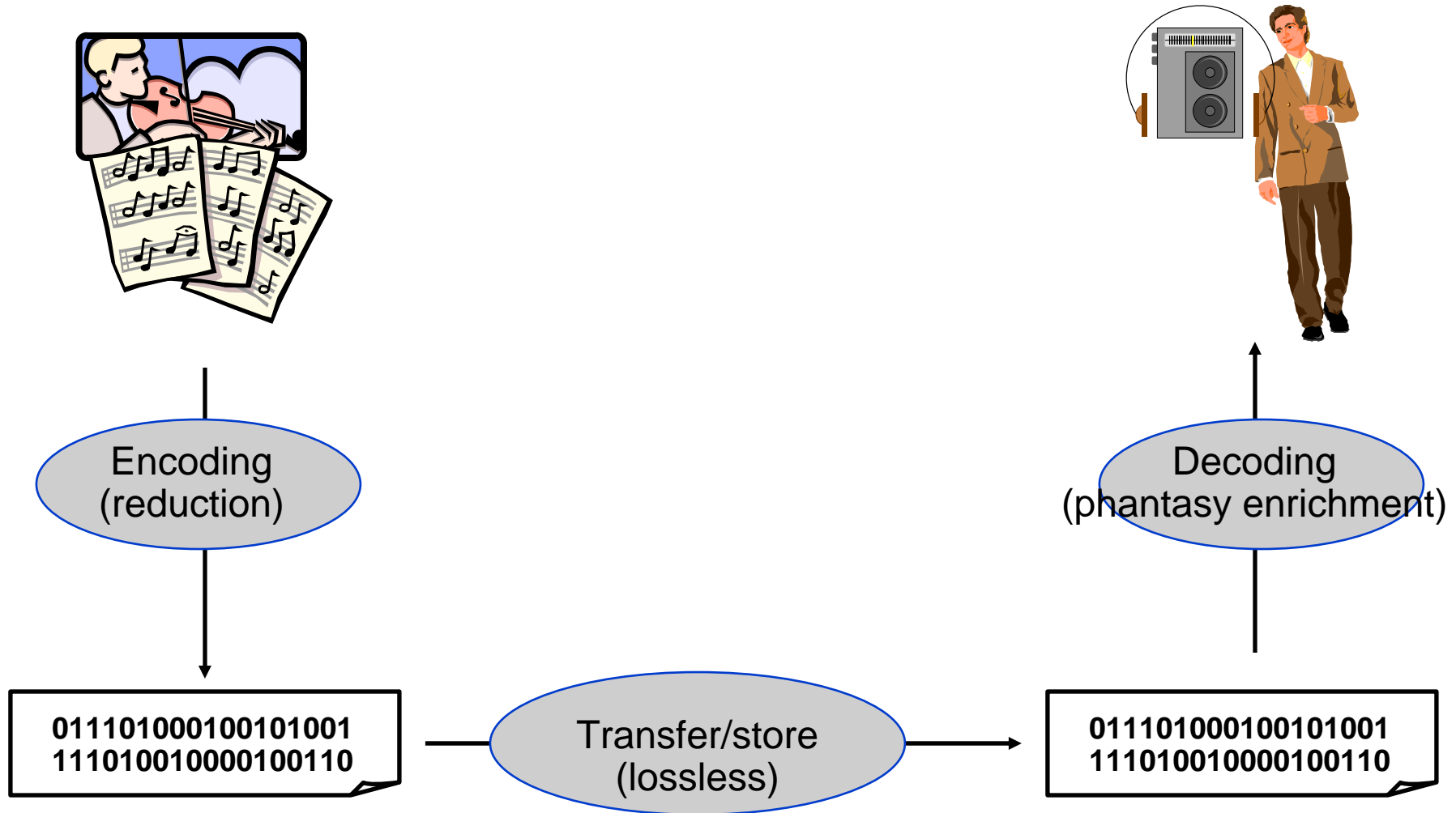
University Koblenz and
Fraunhofer IDMT Ilmenau

Florence, December 2nd, 2005

Overview (17 slides)

- 1. The problem of digitized intellectual property**
2. Privacy principles and analysis structure
3. Process model and data traces (example: iTunes)
4. Conclusion

Production, distribution, consumption of digitized goods



Virtual goods

Content more important than medium
Lossless unbinding from original medium
Cheap transfer/storage by customer

However:

Production of media remains expensive
Distribution of content is cheap
Content has no price on the market

Three ways of copyright protection

Classical DRM:

- Technology enforces copyright protection

Second line of defence:

- No enforcement, but recognition of behavior
- Personalized watermarks
- Link clickstream data with contractual data
- Privacy problem

Incentives:

- Business model allows free copy, but rewards payment

Overview

1. The problem of digitized intellectual property
- 2. Privacy principles and analysis structure**
3. Process model and data traces (example: iTunes)
4. Conclusion

The European Directive 95/46/EC on privacy (1)

Quality (Art. 6): personal data must be lawful, fair, adequate, relevant

Legitimation (Art. 7): personal data must be bound to the purpose of the service, they may be used only by consent of the data subject or by a legal obligation

Purpose binding (Art. 7): personal data must be necessary for the purpose, e.g. a contractual cooperation or the administration of a service, etc.

Transparency (Art. 10-12): the right of access by the data subject

User control: beyond transparency, the right of access, esp. the right of rectification (Art. 10-12), the right to object (Art. 14)

The European Directive 95/46/EC on privacy (2)

Confidentiality (Art. 16): the organization must ensure the confidentiality of the personal data

Correctness and security (Art 17 on security, and the right to rectify the data, in Art. 10-12): the organization must protect the personal data against loss, distortion, and correctness with respect to the content

Supervision (Art. 18-19, and 28-30): regulations on a supervisory authority

Remedies, liability, and sanctions (Art. 22-24); regulations on the sanctions in case the service provider does not comply with the principles

Do music shops comply with the privacy principles? (1)

Data flow before concluding a deal:

- while preparing a purchase
- during user registration
- when placing a product into the shopping cart

Data flow at conclusion of a deal:

- at end of selection (closing the shopping cart),
- for payment of the products,
- for delivery of the products

Data flow by checking the right to use a product:

- at first initialization of a player
- at repeated usage
- for rights update

Do music shops comply with the privacy principles? (2)

Data flow through service functions, e.g.:

- improvement of service,
- direct marketing,
- security functions such as encryption

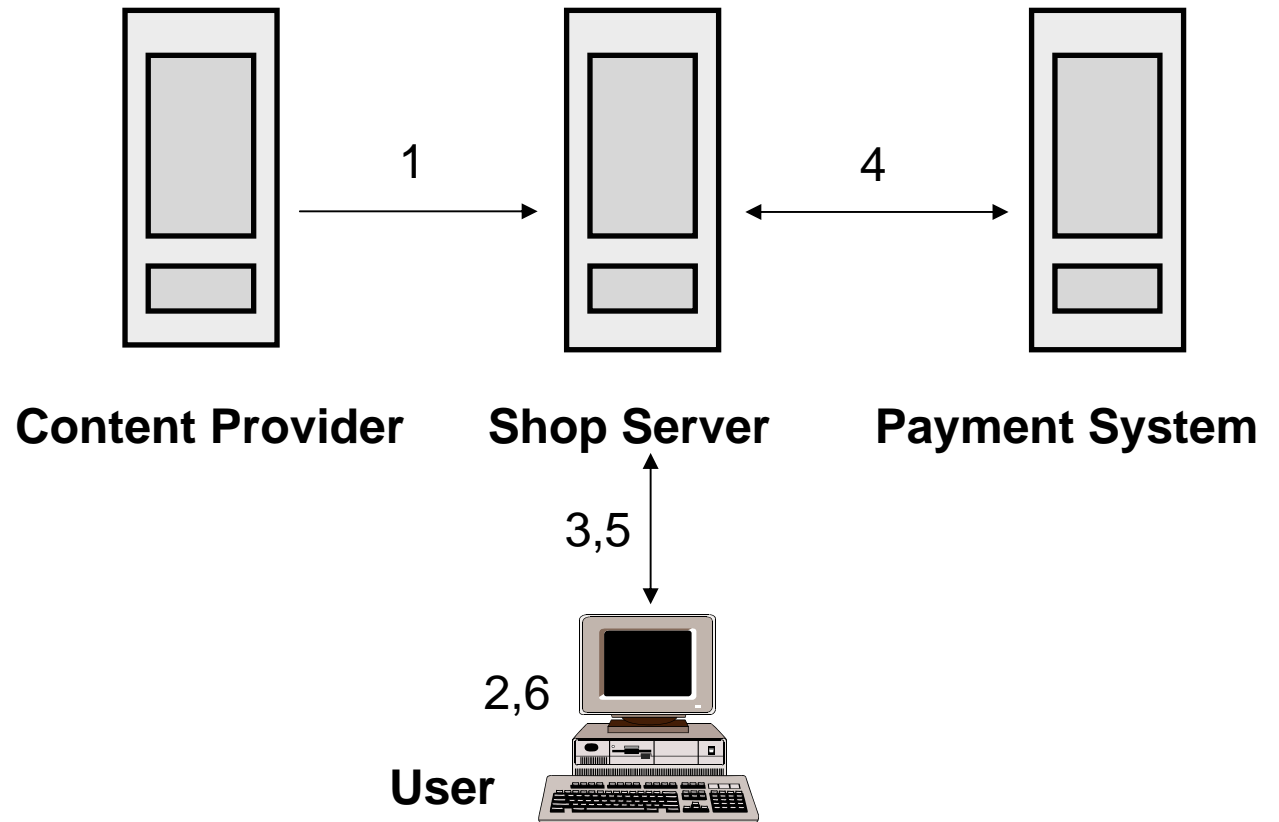
Data flow through hidden interfaces and by linkage of different functions:

- cookies
- pixel tags (web bugs)
- combining customer data with clickstream data such as IP addresses or encryption keys

Overview

1. The problem of digitized intellectual property
2. Privacy principles and analysis structure
- 3. Process model and data traces (example: iTunes)**
4. Conclusion

For example, iTunes



- 1 Provide content for sale
- 2 Install iTunes client
- 3 Select good
- 4 Organize payment and rights
- 5 Download good and rights
- 6 Check usage rights and play

iTunes product encryption

Products are encrypted

- Personalized decryption keys

During registration

- Provide customer info to iTunes server, esp. Apple user id (=email address!) and client device id
- Receive personalized key for decryption

User account at iTunes server keeps record of allowed client devices

For consumption

- Client uses locally stored personalized key to decrypt and play product

If Client device is not allowed: de-register another client device and register this new device

Data traces (1)

Concioulsy provided during registration

- Name, address, e-mail address, payment info

Automatically collected during any communication

- Client system info, including device id
- Cookie
- Session-id

Encoded within iTunes product

- Product id
- ***Apple User id = e-mail address!***
- Metadata about product
- (same association is stored by the Download shop)

Data traces (2)

Data flow through service functions

- iMix (favorites hit list by persona)
- Pocket money account
- Coupons
- metadata service, CDDDB run by Gracenote

Data flow through hidden interfaces and by linkage of different functions

- HTTP communication (IP address, language, referer, search keys)
- Association of clickstream data with contractual data
- Combined association with iMix (favourites), pocket-money account and metadata search

Conclusion

All Systems collect too many personal data

- Hidden interfaces, within products
- Links between clickstream data and contracts

Hidden interfaces provide „second line of defence“ against customers

Missing trust is a danger for the market

Recommendation to shops: transparency

More Systems to be analyzed

Bizer/ Grimm/Will et al.:

http://www.bmbf.de/pub/privacy4drm_studie.pdf

[July 2005]

**Thank you for your attention,
visit us in Koblenz and Ilmenau**



Campus Koblenz, Mosel River



Fraunhofer IDMT,
Ernst Abbe Zentrum, Ilmenau