Digital Rights Management (DRM) for Establishing and Increasing Trust and Privacy

Workshop on Methods and Tools for Analyzing and Securing Trust and Privacy
SINTEF, Oslo, June 04/2004

Habtamu Abie
Norwegian Computing Centre
http://www.nr.no/
• Definitions of
  – Intellectual Property Rights (IPR)
  – DRM
  – The term Rights
• Core Rights Model
• A DRM Reference Architecture
• DRM as a multi-faceted concept
• How DRM affects Privacy
• Comments
• Conclusions
• References
Definition of IPR

• **IPR** (http://www.wipo.int) refers to creations of the mind:
  – inventions, literary and artistic works, and
  – symbols, names, images, and designs used in commerce.

• **Intellectual property (IP)** is divided into two categories:
  – **Industrial property**, which includes
    • inventions (patents)
    • trademarks
    • industrial designs, and
    • geographic indications of source
  – **Copyright**, which includes literary and artistic works:
    • literary works: novels, poems and plays, films, musical works
    • artistic works: drawings, paintings, photographs and sculptures, and architectural designs.

  – **Rights** related to copyright include those of
    • performing artists in their performances
    • producers of phonograms in their recordings
    • broadcasters in their radio and television programs.
Definition of DRM

• DRM system refers to the use of technologies, which
  – unambiguously describe and identify digital information objects protected by Intellectual Property Rights (IPR)
  – enforce fine-grained rules of usage for, and rights of access to, them
  – monitor and track them, and
  – provide a secure infrastructure for their preparation, distribution, storage, manipulation, and communication, and finally
  – protect the privacy of users.

• To achieve these, DRM must include
  – persistent digital data protection against unauthorised interception and modification
  – unique identification of recipients and content to enable access control for the digital content
  – effective tamper-resistant mechanism to process protected digital data

• Thus, DRM
  – protects IPR over digital assets
  – establishes and increases security, trust and privacy
The term **Rights**, according to Black’s Law Dictionary, is “an interest or title in an object property; a just and legal claim to hold, use, and enjoy it or to convey it or donate it”.

**Rights**: a user’s privilege on an object

**Conditions** specify terms, conditions, and obligations under which rights can be exercised

**Rights expressions** should consist of:

- **Permissions** (i.e., usages) - what we are allowed to do
- **Constraints** - restrictions on the permissions
- **Obligations** - what we have to do/provide/accept
- **Rights Holders** - who is entitled to what

The four core entities:
**Users, Content, Rights, and Conditions**
A DRM Reference Architecture

Based on Rosenblatt et al., Digital Rights Management: Business and Technology (2002)
DRM as a Multi-faceted Concept

- **Ubiquity** of digital content
  - DRM concerns everyone
  - All stakeholders must be winners

- **Factors** that affect the uptake of DRM
  - Legal, regulatory, private and public policies
  - Societal questions, ethics
  - Business processes and models
  - Technology

- **Laws** and **policies** pertaining to IPR protection
  - Vary widely between countries and are likely to remain different, regardless of efforts to harmonise them
  - Must interoperate and be reconciled
DRM as a Multi-faceted Concept

• **Societal** questions
  – privacy, information access, digital divide
  – fair-use, private-use, community-use
  – cultural issues, freedom of speech
  – general use acceptance or customer’s benefits from DRM

• **Business** processes and models
  – fine-grained usage control: fair use, private use, super-distribution, payment
  – IPR negotiation, contracting, licensing
  – usage tracking and monitoring

• **Technology**
  – **Trust**
    • providers need to establish trust and confidence in their products and services
    • consumers need to trust providers, and protect their privacy and information
  – **Privacy** (individuals, groups, organisations)
All Stakeholders are Winners

• **Content creators/owners**
  – (artists, authors) win by getting fairly paid for their efforts

• **Content distributors**
  – (publishers, retailers) win by getting paid to distribute content.

• **Technology Providers**
  – (Telecos, ISPs, DRM providers: IBM, Sony, Microsoft, InterTrust, ContentGuard, Adobe) win by getting paid for enabling distribution of content

• **Manufactures**
  – (soft + hardware) win by getting paid for producing end-devices (Computers, PDA, CD-Player, Mobile phones)

• **Users/Consumers**
  – (businesses, schools, libraries) win by getting good and authentic service at a reasonable price.

• **Education and learning sector**
  – **double** winner for being the major creator and consumer of IPR

Norsk Regnesentral
Norwegian Computing Center
How DRM Affects User Privacy

• Potential threats to user privacy occur
  – monitoring of content and rights acquisition
  – the need to update rights
  – the collection of usage data

• Provision of web services,
  – monitoring user’s activity (e.g., through client side cookies, server-side logs) for post-download control.

• Distributing persistent, complete DRM metadata with digital content,
  – rights metadata is added to the collectible, information about the user
  – no effect on user privacy in the actual use of content

• Tying content to a particular device or set of devices,
  – tracking for the purpose of tying content to a set of devices

• Tying the content to the user
  – user tracking can be much greater
  – collectible and minable information about a user includes his complete usage pattern (e.g., listening, reading, viewing history)
The ability of DRM to track and monitor will lead to a need for
  more efficient mechanisms for the protection of personal privacy,
  protection that the DRM system itself must ensure

Although there are those who claim that this is a red herring on
the basis that such privacy is protected and guaranteed by law,
  it should be pointed out that unscrupulous manufacturers and
  individuals may be technically capable of violating privacy
  undetected and therefore unpunished.

Solved by technology, legal contracts, or combination of them
  in DRM trust model,
  it is not possible to separate honest and dishonest users

If properly designed, implemented, and used, DRM can
  provide user-privacy protection
  increase trust
Conclusions: DRM Business Mascot

- DRM is Key to Offering Secure Multimedia Services

With data traffic and premium content revenues over the mobile channel forecast to rise from $9 billion in 2003 to almost $40 billion by 2007, DRM plays an essential role in protecting these revenues and facilitating the means to boost them through super-distribution. Players just cannot afford not to implement DRM.

[Source: Ovum, “Digital Rights Management: How to Sell and Protect Content”, 7/2003]
References

• **Books**

• **General resources**
  – Cover Pages: http://xml.coverpages.org/drm.html

Does DRM help rights-holders’ gold rush into a new market?