A

Seminar report

on

Digital Rights Management

Submitted in partial fulfillment of the requirement for the award of degree of MCA

www.studymafia.org

SUBMITTED TO:

www.studymafia.org

SUBMITTED BY:

www.studymafia.org

Preface

I have made this report file on the topic **Digital Rights Management**,, I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to ……..who assisting me throughout the prepration of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

www.studymafia.org

Introduction

Digital Rights Management (DRM) systems restrict the use of digital files in order to protect the interests of copyright holders. DRM technologies can control file access (number of views, length of views), altering, sharing, copying, printing, and saving. These technologies may be contained within the operating system, program software, or in the actual hardware of a device.

DRM systems take two approaches to securing content. The first is "containment," an approach where the content is encrypted in a shell so that it can only be accessed by authorized users. The second is "marking," the practice of placing a watermark, flag, or a XrML tag on content as a signal to a device that the media is copy protected.

According to Professor Ed Felten, both approaches are vulnerable to cracking by individuals with "moderate" programming skills. DRM technology and legislation requiring the inclusion of copy control systems pose serious threats to privacy, open source software development, and the fair use of copyrighted content.

Some DRM technologies have been developed with little regard for privacy protection. The systems usually require the user to reveal his or her identity and rights to access protected content. Upon authentication of identity and rights to the content, the user can access the content.DRM systems can prevent the anonymous consumption of content.

DRM systems could lead to a standard practice where content owners require all purchasers of media to identify themselves. In other areas where individuals can borrow or purchase media, such as video rental stores or libraries, statutory and ethical protections prevent the transfer of personal information linked to the content acquired. Such protections do not exist in the music and growing electronic book markets. In these unregulated areas, artists and authors may have more difficulty in finding an audience for their work because of the privacy risks associated with linking identity to content consumption.

www.studymafia.org

What is DRM

DRM is the technology to protect rights of digital contents to prohibit illegal copy and ill contents and to let only authorized users use the contents.

Digital Rights Management (DRM) is an emerging and vital business concept driven by the need for secure electronic distribution of high-value digital content. In its purest form, DRM provides a technology platform to allow trusted packaging, flexible distribution and managed consumption of digital content over electronic networks.

DRM technology provides content owners, service providers, distributors and retailers with a safe, secure method for meeting the consumer's need for interactive, on-demand access to movies, online games, books, music, software and proprietary data — virtually any type of digital media.

www.studymafia.org

Architecture

1.Functional Architecture:

The overall DRM framework suited to building digital rights-enabled systems can be modeled in three areas:

- **Intellectual Property (IP) Asset Creation and Capture**: How to manage the creation of content so it can be easily traded. This includes asserting rights when content is first created (or reused and extended with appropriate rights to do so) by various content creators/providers.

- **IP Asset Management**: How to manage and enable the trade of content. This includes accepting content from creators into an asset management system. The trading systems need to manage the descriptive metadata and rights metadata (e.g., parties, usages, payments, etc.).

- **IP Asset Usage**: How to manage the usage of content once it has been traded. This includes supporting constraints over traded content in specific desktop systems/software.

While the above models comprise the broad areas required for DRM, the models need to be complemented by the Functional Architecture that provides the framework for the modules to implement DRM functionality

www.studymafia.org

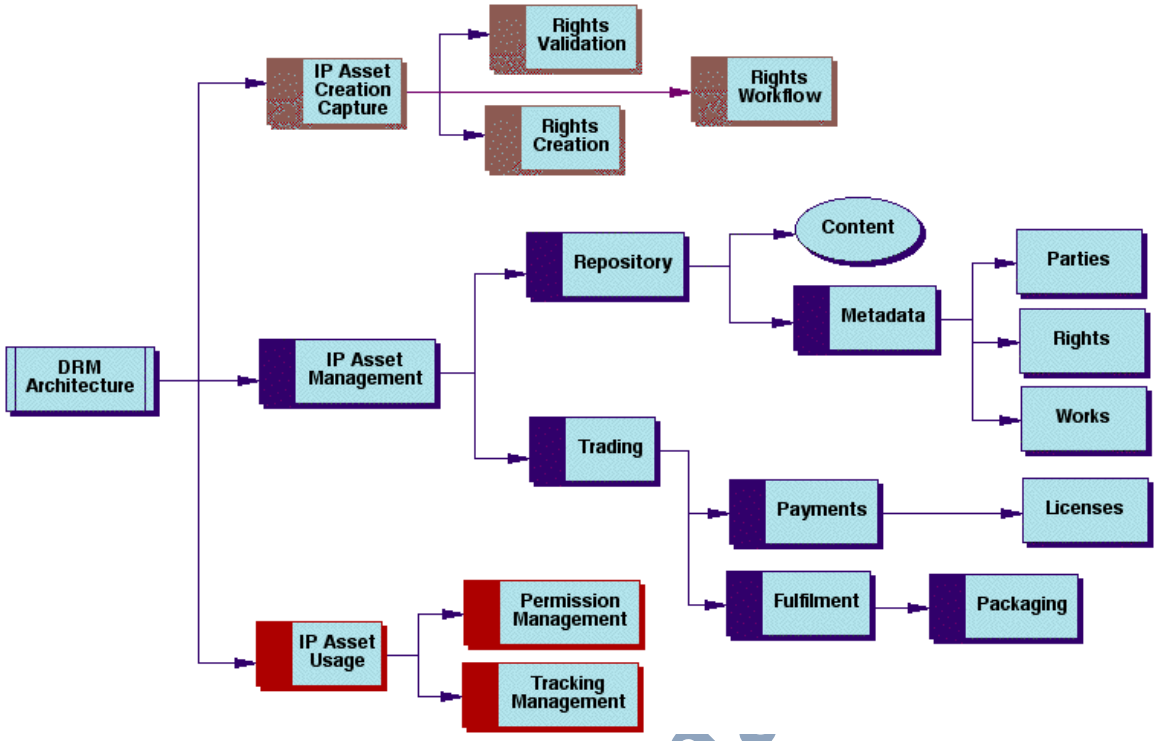


Figure 1 - DRM Functional Architecture

The Functional Architecture stipulates the roles and behavior of a number of cooperating and interoperating modules under the three areas of Intellectual Property (IP): Asset Creation, Management, and Usage.

The IP Asset Creation and Capture module supports:

- Rights Validation - to ensure that content being created from existing content includes the rights to do so.
- Rights Creation - to allow rights to be assigned to new content, such as specifying the rights owners and allowable usage permissions.
- Rights Workflow - to allow for content to be processed through a series of workflow steps for review and/or approval of rights (and content).

www.studymafia.org

The IP Asset Management module supports:

- Repository functions - to enable the access/retrieval of content in potentially distributed databases and the access/retrieval of metadata. The metadata covers Parties, Rights and descriptions of the Works. (See the Information Architecture section of this article for more details.)

- Trading functions - to enable the assignment of licenses to parties who have traded agreements for rights over content, including payments from licensees to rights holders (e.g., royalty payments). In some cases, the content may need to go through fulfillment operations to satisfy the license agreement. For example, the content may be encrypted/protected or packaged for a particular type of desktop usage environment.

The IP Asset Usage module supports:

- Permissions Management - to enable the usage environment to honor the rights associated with the content. For example, if the user only has the right to view the document, then printing will not be allowed.

- Tracking Management - to enable the monitoring of the usage of content where such tracking is part of the agreed to license conditions (e.g., the user has a license to play a video ten times). This module may also need to interoperate with the trading system to track usage or to record transactions if there is payment due for each usage.

www.studymafia.org

2 Information Architecture:

The Information Architecture deals with how the entities are modeled in the overall DRM framework and their relationships. The main issues that require addressing in the development of a DRM Information model include:

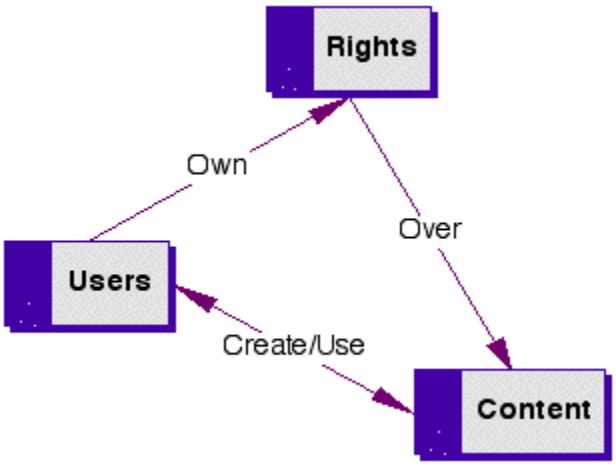
- Modeling the entities
- Identifying and describing the entities, and
- Expressing the rights statements

Modeling the entities:

It is important to adopt a clear and extensible model for the DRM entities and their relationship with other entities. Existing work in this area includes the <indecs> project. The basic principle of the <indecs> model is to clearly separate and identify the three core entities: Users, Content, and Rights as shown in Fig 2. Users can be any type of user, from a rights holder to an end-consumer. Content is any type of content at any level of aggregation.

The Rights entity is an expression of the permissions, constraints, and obligations between the Users and the Content. The primary reason for this model is that it provides the greatest flexibility when assigning rights to any combination or layering of Users and Content. The Core Entities Model also does not constrain Content from being used in new and evolving business models.

www.studymafia.org



`

Figure 2 - DRM Information Architecture - Core Entities Model

This model implies that any metadata about the three entities needs to include a mechanism to relate the entities to each other.

The Content itself also needs to be modeled. The key principle in the modeling of Content is that Content contains many "layers" from various intellectual stages or evolution of its development. Such a model will enable clearer (i.e., more explicit and/or appropriate) attribution of rights information.

studymafia.org

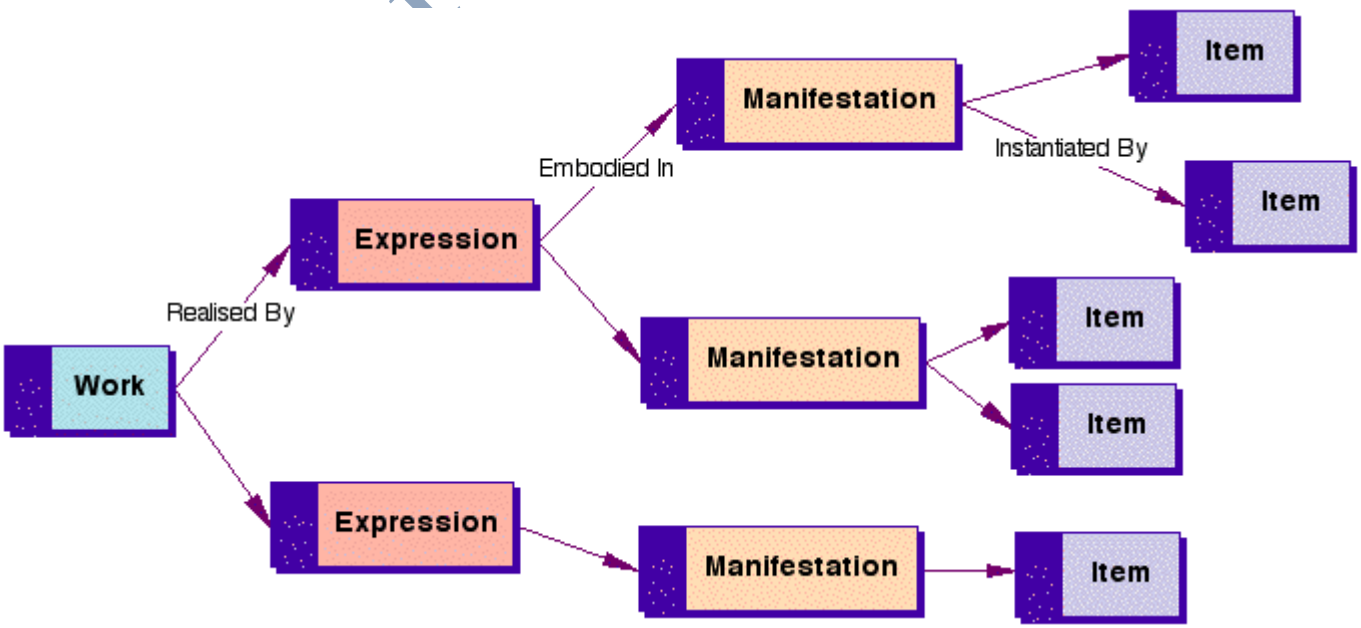


Figure 3 - DRM Information Architecture - Content Model

The layers of the Content defined as Work (a distinct intellectual or artistic creation) and Expression (the intellectual or artistic realization of a work) reflect scholarly or creative content. On the other hand, the other layers of Content, defined as Manifestation (the digital embodiment of an expression of a work) and Item (a single exemplar instantiation of a manifestation), reflect physical or digital form.

The important point in this style of content modeling is that at any of the points in the IFLA model, different rights holders can be recognized.

Another aspect that may affect rights is when Content is made of many parts. Some of these parts may have different rights associated with them that need to be recognized in the aggregated content.

Digital Millennium Copyright Act:

The Digital Millenium Copyright Act was passed in the United States, in an effort to make the circumvention of such systems illegal. Despite this law, which has received substantial opposition on constitutional grounds, it is now relatively easy to find DVD players which bypass the limitations the DVD Consortium sought to impose. The cryptographic keys themselves have been discovered and widely disseminated.

New DRM initiatives have been proposed in recent years which could prove more difficult to circumvent, including copy-prevention codes embedded A wide variety of DRM systems have also been employed to restrict access to eBooks.

Opponents of DRM, as currently envisioned and implemented, note that by delegating computer access (or control of the ability to execute some programs, or to execute programs only with certain data) to third parties, there is a very considerable risk of problems well beyond any control of intellectual property rights issues.

For instance, due to a bug (or misdesign, or misadministration of an otherwise 'reasonable' design) the protecting code implementing the local part of a DRM scheme

www.studymafia.org

may prevent a computer user from using his computer at all, or from using programs (or using data as an input to a program) when such use is actually completely legitimate and not a violation of any copyright holders' rights. Or, for another instance, a legitimately purchased copy of <a DVD containing a book or a movie, or a software program, or ...> might be blocked because it is being used on equipment which doesn't include the DRM function permitting access to it.

Security Protocols, software implementing security protocols, and sryptographt generally have historically proven extremely difficult to design without vulnerabilities due to bugs or design mistakes. This has been true of designs from experienced and well respected professionals.

Expressing rights statements:

The Rights entity allows expressions to be made about the allowable permissions, constraints, obligations, and any other rights-related information about Users and Content. Hence, the Rights entity is critical because it represents the expressiveness of the language that will be used to inform the rights metadata.

Rights expressions can become complex quite quickly. Because of that, they are also modeled to understand the relationships within the rights expressions.

As shown in figure 4, Rights expressions should consist of:

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

www.studymafia.org

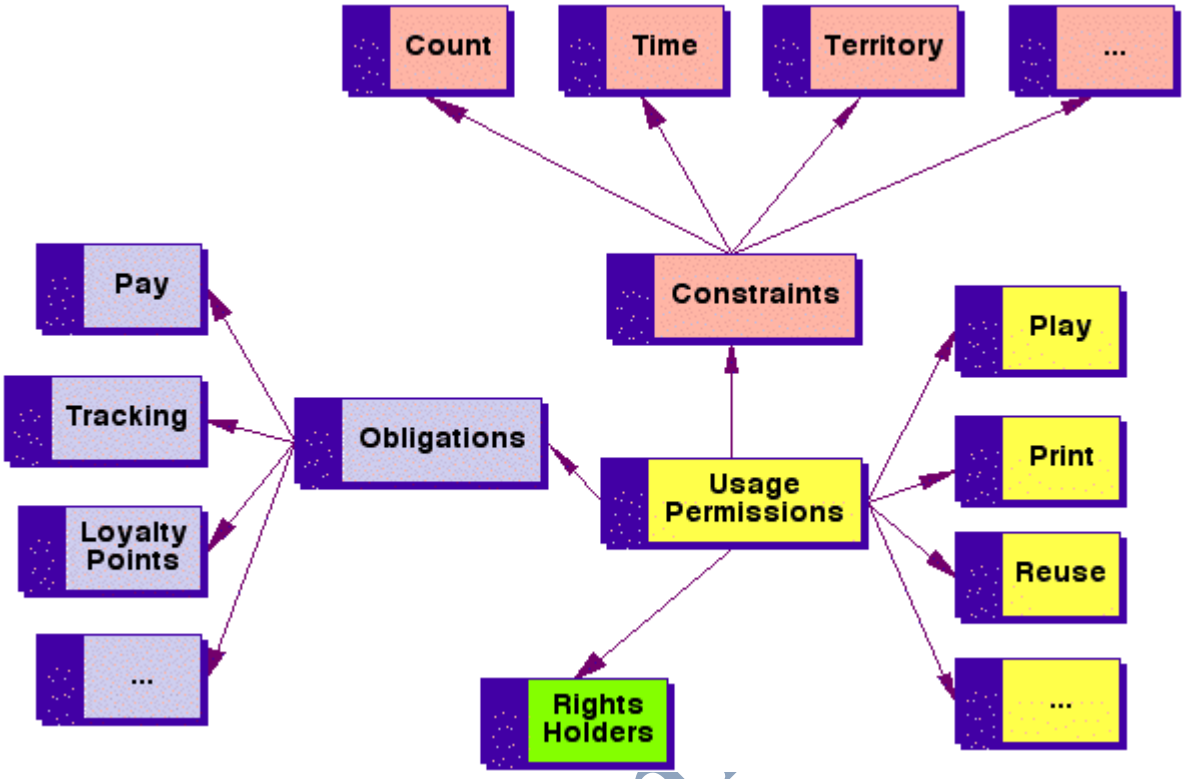


Figure 4 - DRM Information Architecture - Rights Expression Model

For example, a Rights expression may say that a particular video can by played (i.e., a usage permission) for a maximum of 10 times (i.e., a count constraint) in any semester (i.e., a time constraint) for a $10 fee (i.e., an obligation to pay). Each time the video is played, John, Mary, and Sue (the rights holders) receive a percentage of the fee. Usually, if a right is not explicit in an expression, it means that the right has not been granted. This is a critical assumption made by Rights languages and should be made clear to all Users.

www.studym

Advantages and Disadvantages

Advantages of DRM?

1. DRM attempts to protect the copyright holders intellectual property rights.
2. Does not generally use other forms of copy protection such as "serial keys" and "keyfiles".
3. Allows for secure content delivery for the consumer.
4. Allows for content providers to monitor sales of their products more efficiently.
5. Cuts down on the amount of piracy for a given piece of software .

Disadvantages of DRM?

1. 1.Is very restrictive to the consumer in usage.
2. Is heavily reliant on licenses which could expire, leaving the consumer with software .they paid for that no longer works.
3. It is fairly ineffective in stopping software piracy.
4. 4.Not popular with the majority of consumers.
5. Various compatibility issues.

www.studymafia.org

Some DRM Solutions & Products

MacroSafe™:

MacroSafe is an end-to-end DRM solution for packaging, distributing and managing the consumption of high-value digital media. MacroSafe's high security ensures that digital content, as well as the revenue streams it creates, are protected. Its transparent architecture causes little or no impact to existing content creation workflows, electronic delivery infrastructures nor to the consumer's viewing experience.

Its flexible design is adaptable to multiple applications, business models, distribution models and user devices.And, it is based on industry-standard programming languages, interfaces and protocols, so it cost-effectively integrates into existing e-commerce systems. MacroSafe's DRM solution provides the right combination of security, transparency, flexibility and investment protection to ensure the safe packaging, distribution and consumption of digital content throughout the DRM value chain.

Macrovision:

Macrovision develops and markets copy protection, digital rights management and electronic license management technologies for the home video, consumer software and enterprise software markets. Macrovision's mission is to develop, acquire and market proprietary technologies which enable video and audio content owners and independent software vendors to securely distribute and market their products to consumers and businesses, and to build significant new revenue models.

www.studymafia.org

Limitations of DRM?

- Most access control techniques are algorithm-based. This restricts subjective opinion (that can be exercised by human brain.)
- Some of the features can be construed to be against the fair-use-of-content.
- Different publishers and device makers follow different techniques to suit their own content/devices. This is not in the best interest of the consumer.
- There are just too many techniques and technologies available, and a worldwide standard has not yet been established.
- Many issues like fonts in regional languages can create challenges on some devices (through this problem cannot be attributed to DRM alone.)
- Some technologies permit remote disabling (or even deletion) of content. This is perceived to be against individual freedom. Organizations like Free Software Foundation are objecting to such features.
- Some DRM technologies can trace the original "registered buyer" of the content or can tag the "credit/debit card details" of original purchase, as a means to discourage distribution of the content. This is seen as compromising identity and privacy.

www.studymafia.org

Conclusions

This report confirms that DRM is currently being used in the Canadian marketplace in ways that violate Canadian privacy laws.

DRM is being used to collect, use and disclose consumers' personal information, often for secondary purposes, without adequate notice to the consumer, and without giving the consumer an opportunity to opt-out of unnecessary collection, use or disclosure of their personal information, as required under Canadian privacy law.

www.studymafia.org

REFERENCES

www.studymafia.org
www.google.com
www.wikipedia.com

www.studymafia.org