Digital Rights Management Techniques

Nithin Dinker Kamath
nkamath@usc.edu

Submitted as partial fulfillment of the requirements of CSCI530 Security Systems Course, University of Southern California

ABSTRACT

We are currently living in a Digital Era. Because of this most of our sources of information and entertainment are digital in nature. While we want to have a hassle free and easy distribution of the digital content, unauthorized distribution and copying of data has become rampant over the years. While copyright holders try to protect their intellectual property from misuse and theft, many legitimate users feel that while doing so their right to "Fair Use" is been violated.

In such times, Digital Right Management comes in handy. What Digital Right management tires to do is to provide a way where digital content can be securely transferred from one person to another person without violating the copyrights or adding additional burden on the end user.

Various Digital Rights Management Techniques and Systems exist. What this paper tries to do is analyze current techniques, discuss future ones and suggest improvements to the same.

Over the course of this paper we will be not only be introduced the concept of Digital Rights Management but we will also try to understand them these concepts for apparent benefits and short comings.

1 INTRODUCTION

Digital Rights Management or DRM has today evolved form being just a requirement to being a necessity. During the past decade, there has been an exponential rise of internet and the speed at which users are connected to the internet. Days when people used to browse the internet on their 56kbps modems have long gone by. Currently many users are not just using DSL (speeds up to 3 Mbps) but cable (up to 6 Mbps) and gigabit LANs.

While internet has been successful in being the choice of many content providers for content delivery, piracy and copyrights violations is still a major concern. Also, since the data over the internet flows through various nations and territories, things have become complicated due to variations in copyrights law.

Currently downloads are not just limited to music files which range anywhere from 3 MB to 10 MB in size but are getting DVD copies of the latest movies. Also, newer P2P softwares have intuitive GUIs making it easier for everyday user to get files easily. Technologies like BitTorrent, Guntella and KaZaa which started off as softwares which developers can use to transfer big files have found their not so innocent uses.

Losses due to piracy of U.S. copyrighted materials around the world are conservatively estimated to reach $30-$35 billion annually.[1]

[1] International Intellectual Property Alliance (www.iipa.com)

2 DIGITAL RIGHTS MANAGEMENT

What exactly is Digital Rights Management? Generally speaking, a DRM system enables the secure exchange of intellectual property, such as copyright-protected music, video, or text, in digital form over the Internet or other electronic media, such as CDs, removable disks, or mobile networks. DRM allows content owners to distribute securely to authorized recipients and gives them control over the whole distribution chain.[2]

The basic objective of a DRM system is simple.

a. Provide enough security to the digital content so that the authorized user cannot modify, alter, reverse engineer or re-distribute the content illegally.

b. Allow "Fair Use" of the digital content by the authorized user.

Hence, DRM systems have to balance the requirements of the content owner and end user. The content owner is concerned with unauthorized use or distribution of his content while the end user is just concerned with the usability of the content he is entitled to.

3 DIGITAL RIGHTS MANAGEMENT TERMS

These are few of the terms associated with Digital Rights Management.

a. *Content:* In general, it is any product or property that is generated or produced by an individual or an entity. When we say digital content, it usually refers to digital data like music files, movies, text files or any general data file that is produced by a person or an entity.

b. *Content Owner:* Content owner is a person or entity which produces the content. For example, in case of music, the original composer or music artist, while in the case of movies it's the producer or the studio which produces it.

c. *Copyright:* It is the legal right of the content owner over the content. A person having a copyright over particular content can modify, alter or destroy that content. According to Digital Millennium Copyrights Act, the copyright to a digital content automatically belongs to the creator of that content.[3] There are different types of copyrights, some which expires after certain period while others never expire. A copyright holder can opt to transfer his copyright to another entity.

d. *License:* It is a right given to any person or entity to use, limitedly distribute or sell a content. This right is conferred by the Content Owner.

e. *Content Provider:* Generally, it is the entity which provides the user with the digital content. Usually the content provider has unlimited license over the content which he distributes or sometimes even has the copyrights to the content. Examples of content providers are online music stores: which have unlimited licenses or movie studios: which have complete or partial copyrights to the movie.

f. *Medium of Distribution:* It is the physical medium used to distribute the content. In case of digital contents the medium can be the internet, CD ROM disks, magnetic tapes or any data transfer medium.

g. *End User:* End user is the person or an entity which acquires the digital content with the purpose of using it. End User cannot re-distribute, modify or reverse

[2] "Digital rights management and watermarking of multimedia content for m-commerce applications" - Hartung, F. Ramme, F. Communications Magazine, IEEE Nov 2000

[3] United States Copyright Office (www.copyright.gov)

engineer the content. Examples include a person who buys music CD and listens to them, a company which buys software and installs it onto limited number of machines or a movie theatre which screens the movie for limited number of times.

4 LICENSE

What exactly is a license? It is a set of rights given to a particular person or entity by the content owner directly or indirectly through a content provider. It is a contract between these two parties, terms of which include:

a. *Length:* The length of time for which the end user can use the content.

b. *Number of Usage:* Number of times the end user can use the digital content. Like in case of software the number of machines onto which the software can be installed.

c. *Redistribution:* Specifies whether the content can be redistributed or not.

d. *Resale:* Specifies whether the content can be resold or not.

e. *Royalty:* The percentage of profit which the end user needs to pay the owner in case he resells the contents.

f. *Transferability:* Specifies whether this license can be transferred to third party.

g. *Delegation:* Specifies whether this license be delegated to a third party.

h. *Public Exhibition:* These terms specifies whether the content can be used in public or public performances.

h. *Other Legal Terms:* These terms include the current local and international laws, copyright laws, taxability, liabilities and export constraints.

By providing a license to a content the owner in no way parts or gives the copyright to the content to the end user. It should be understood that by acquiring a license to a content, an entity doesn't become its owner. It can be inferred that a license is part delegation of copyrights but not a complete delegation. Also, a license can be revoked by the owner at any time when he feels that the end user has violated the terms of the license.

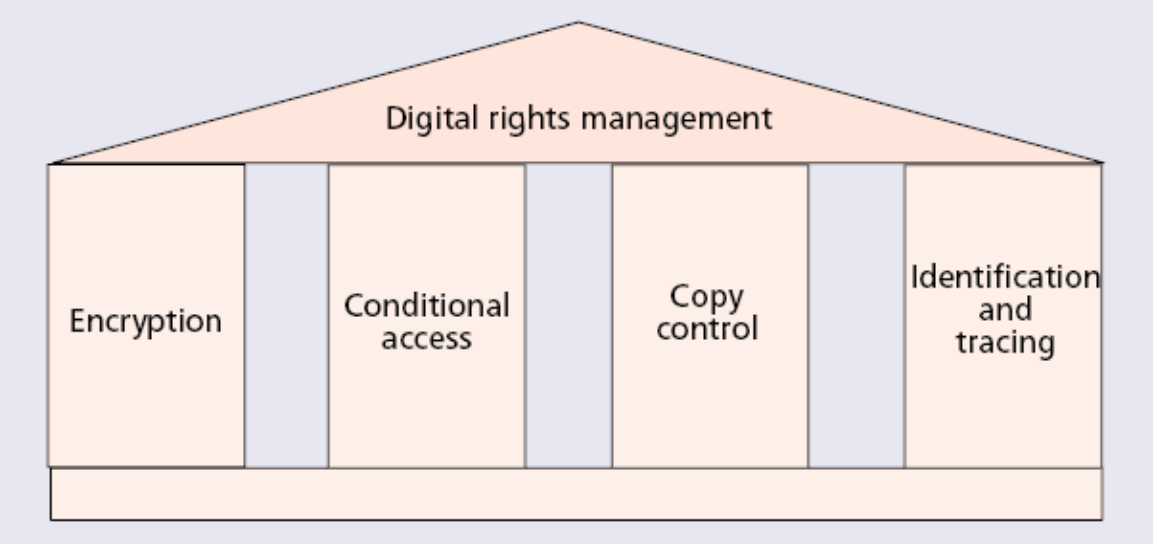

Figure 1: DRM Pillar model

5 DIGITAL RIGHTS MANAGEMENT SYSTEM

To ensure that the digital rights are not violated control over how the content is distributed is very much necessary.

Therefore, DRM system must:
a. Encrypt the data to prevent unauthorized users form accessing and/or using the digital content.
b. Provide the decryption key(s) to the content along with the license.
c. Incorporate billing and payment methods and systems during license or content distribution.
d. Control access to the media.
e. Validate licenses.
f. Incorporate methods to prevent unauthorized copying.
The DRM Pillar model (Figure 1)[4] shows a simplified or ideal model for such systems.

6 DIGITAL WATERMARKING

Some of the required functions of a comprehensive DRM system, such as copy control and data identification and tracing, require that irremovable information be attached to multimedia data. A digital watermark is such information invisibly attached to multimedia data. If you have noticed protected mp3 files and aac files have something called as ID3 tags. These tags not just store the data about the content like artwork, artist and compilation information but also stores licenses for that media. In fact, this technique is implemented by most of online music distributors. Real Networks' (www.real.com) ram, rm and ramb formats have these so called tags and so does Microsoft's (www.microsoft.com) wmv and wma formats.
Digital watermarks have to fulfil the "CIA" requirements to be reliable. They have to provide
a. *Confidentiality*: Watermark data should be accessible only to the owner.
b. *Integrity:* The watermark data cannot be modified by anyone apart from the owner or the provider.
c. *Accessibility:* The watermark should be available for inspection and authentication.
There are various ways to add a digital watermark; some of them are listed below:
a. *Steganography:* Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message; this is in contrast to cryptography, where the existence of the message itself is not disguised, but the meaning is obscured.
b. *Digital Signatures:* It is a type of method for authenticating digital information analogous to ordinary physical signatures on paper.
c. *Spread Spectrum Watermarking:* This is a new technique. Here a watermark is inserted into the spectral components of the data using techniques analogous to spread spectrum communications, hiding a narrow band signal in a wideband channel that is the data.[5]
d. *Dither Modulation:* It is a new class of embedding methods, which we term quantization index modulation (QIM), and develop a convenient realization of a QIM system that we call dither modulation in which the embedded information modulates a dither signal and the host signal is quantized with an associated dithered quantizer.[6]

[4] Digital rights management and watermarking of multimedia content for m-commerce applications" - Hartung, F. Ramme, F. Communications Magazine, IEEE Nov 2000

[5] "Secure spread spectrum watermarking for images, audio and video" - Cox, I.J. Kilian, J. Leighton, T. Shamoon, T. Proceedings on Image Processing, IEEE Sep 1996

[6] "Dither modulation: a new approach to digital watermarking and information embedding" - Chen, B. Wornell, G.W. Proceedings Security

e. *Tagging:* It is a process of adding additional data at the beginning (header) or end (footer) of digital data. Example is ID3 tags in mp3s

7 ENCRYPTION

Encryption is the process of obscuring information to make it unreadable without special knowledge.

In Digital Rights Management, the digital content is encrypted and the end user decrypts the data before using it.

If *Public Key Encryption* is used, then the content is encrypted using the private key and the user decrypts the data using public key. The Rights Management is done by restricting access to the content it self or to the public key.

If *Private Key Encryption* is used then the key used for encryption is given to the end user along with his license.

8 DIGITAL RIGHTS MANAGEMENT IN DVD

8.1 DVD Copy Protection

In 1996, the Copy Protection Technical Working Group (CPTWG) was instituted because of the rising concerns with piracy. This work group came up with 3 components which are currently implemented in all "Compliant" devices that play DVDs. Also, while designing these components, the group had to consider that there maybe some content providers who may not wish to prevent copying of their disks. Like movies which are produced for educational or so called non profit purposes.

The 3 components are:[7]

a. *Content Scrambling System:* CSS is a low-cost method of scrambling MPEG-2 video, developed by Matsushita. Descrambling requires a pair of keys. One of the keys is unique to the disk, while the other is unique to the MPEG file being descrambled. The keys are stored on the leadin area of the disk, which is generally only read by compliant drives. Keys can be passed from a DVD drive to a descrambler over

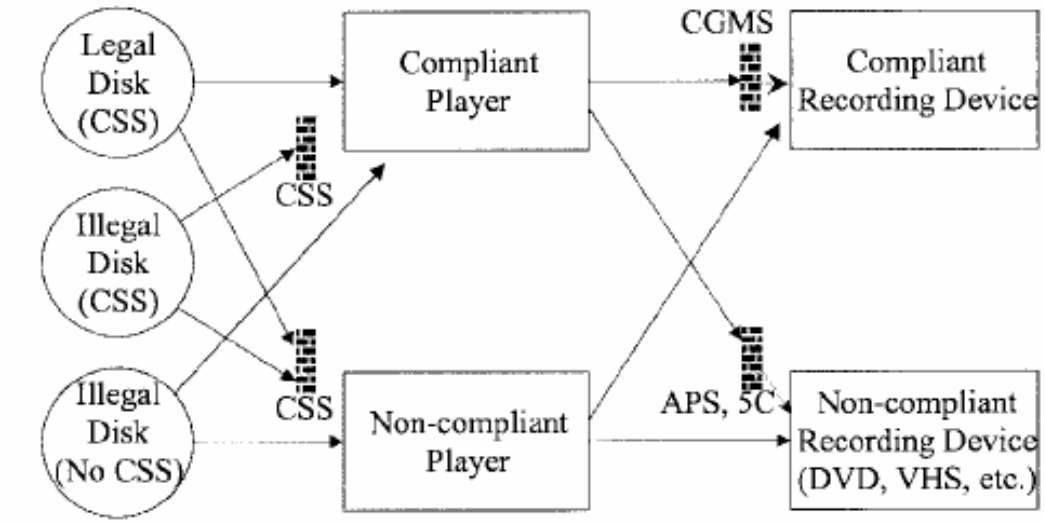

Figure 2: DVD Copy Protection

and Watermarking of Multimedia Contents, SPIE Apr 1999

[7] "Copy Protection for DVD Video" Bloom, J. Cox, I.J. Kalker, T. Jean-Paul, M. Linnartz, G. Miller, M.L. Brendan, C. Traw S.

a PC bus using a secure handshake protocol.

The purpose of CSS is twofold. First and foremost, it prevents byte-for-byte copies of an MPEG stream from being playable since such copies will not include the keys. Second, it provides a reason for manufacturers to make compliant devices, since CSS scrambled disks will not play on noncompliant devices.

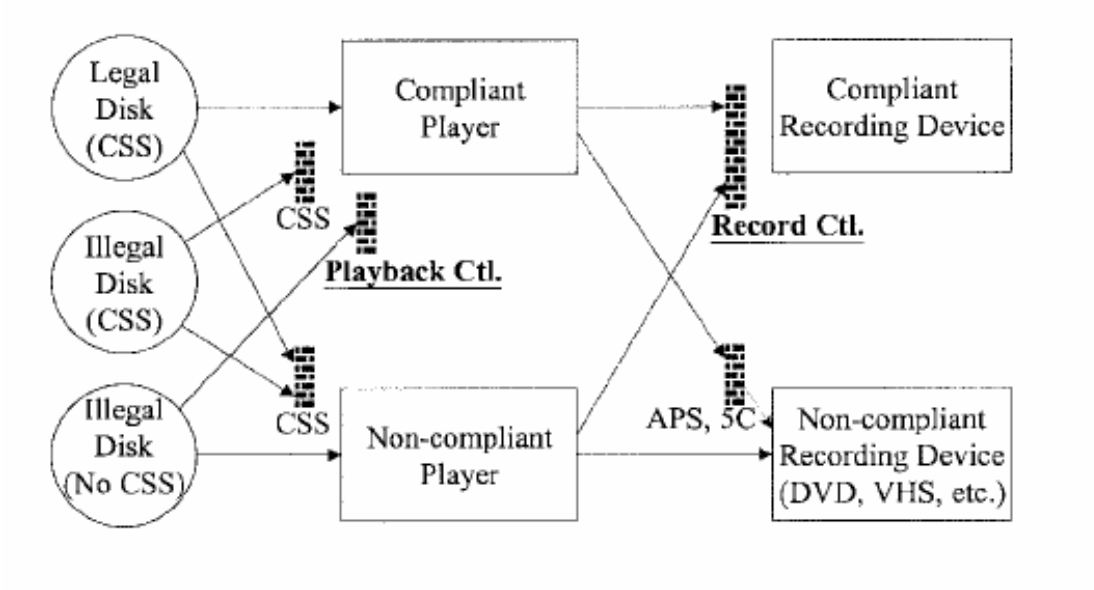

Figure 3: DVD Copy Protection with Watermarking

Anyone wishing to build compliant devices must obtain a license, which contains the requirement that the rest of the copy-protection system be implemented.

b. *.APS system:* It was developed by Macrovision, is a method of modifying NTSC/PAL signals so that they can be displayed on televisions but cannot be recorded on VCR's. It works by confusing the automatic gain control in VCR's, and this usually leads to a severe degradation of the content quality. Before being adopted for DVD, it has been widely used on videocassettes and in set-top boxes (STB's). Of course, the data on a disk are not NTSC/PAL encoded, so APS has to be applied by the NTSC/PAL encoder in a DVD player. The information of whether a given video stream should have APS applied and details about how it should be applied are stored in the MPEG stream header.

c. *CGMS:* CGMS is a pair of bits in the header of an MPEG stream that encode one of three possible rules for copying:

"copy_freely" (the video may be freely copied);

"copy_never" (the video may never be copied); or

"copy_once" (a first-generation copy may be made, but no copies may be made of that copy).

The "copy_once" case is included to support such uses as time shifting, where a copy of broadcast media is made for later viewing. "Copy_once" is unlikely to appear on recorded disks, but it is important for DVD recorders to support it.

Figure 2 demonstrates its working.

The content protection transmission system, 5C, provides a mechanism for compliant devices on a bus to exchange keys in an authenticated manner, so they can send encrypted data to one another

that no other devices can decrypt. The system is more robust than the handshake used for CSS.

In DVD, watermarks are added with the intention of providing more secure form of CGMS. The CGMS bits do not survive digital to analog conversion, and can be trivially stripped from an MPEG stream. Watermarks encoding the same information will not be so easily stripped in normal video processing. A secondary purpose of watermarking is to encode the bits used for controlling APS, which have the same weaknesses as the CGMS bits.

Figure 3 demonstrates the copy protection with watermarking and 5C.

Since the delivery method for DVD is disk, the only concern is preventing unauthorized copying and alteration of DVD contents. The copy protection scheme does that. Other considerations like payments royalties and content delivery do not come into the picture because of the physical transfer of the disk.

8.2 DVD REGION CODES

Each DVD-Video disc contains one or more region codes, denoting the area[s] of the world in which distribution and playback are intended. The commercial DVD-Video player specification dictates that a player must only play discs that contain its region code. In theory, this allows the motion picture studios to control the various aspects of a release (including content, date and price) on a region-by-region basis. In practice, many DVD players allow playback of any disc, or can be modified to do so. Entirely independent of encryption, region coding pertains to regional lockout. Regional lockout is the programming practice, code, chip, or physical barrier used to prevent the playing of media designed for a device from the country where it is marketed on the version of the same device marketed in another country.

9 DIGITAL RIGHTS MANAGEMENT IN MUSIC CD

Like DVDs, CDs also require physical transfer. Hence CDs, like DVDs also employ copy protection techniques like the DVDs.

Most of the music CDs contains small disk errors which are added during the disk's manufacture. These data errors, introduced into discs during manufacturing to cause incompatibility with PCs without affecting ordinary CD players.

10 DIGITAL RIGHTS MANAGEMENT FOR ONLINE DIGITAL CONTENT

Like discussed earlier the major cause of evolution of DRM techniques was the exponential rise of internet. Internet today has evolved into being the number one choice for content delivery. The reasons for this are:

a. Removes the need to physically transfer the content.

b. Instantaneous transactions and delivery.

c. Easy inventory and license management.

d. Digitization of any type of data is easy - books, music or movies.

e. Providing subscriptions based content is possible. Hence, no need of providing long term licenses.

With this ease comes the costs.

Some of the requirements include:

a. Maintenance of databases of authorized users.

b. License management.

c. Authorization and authentication of users.

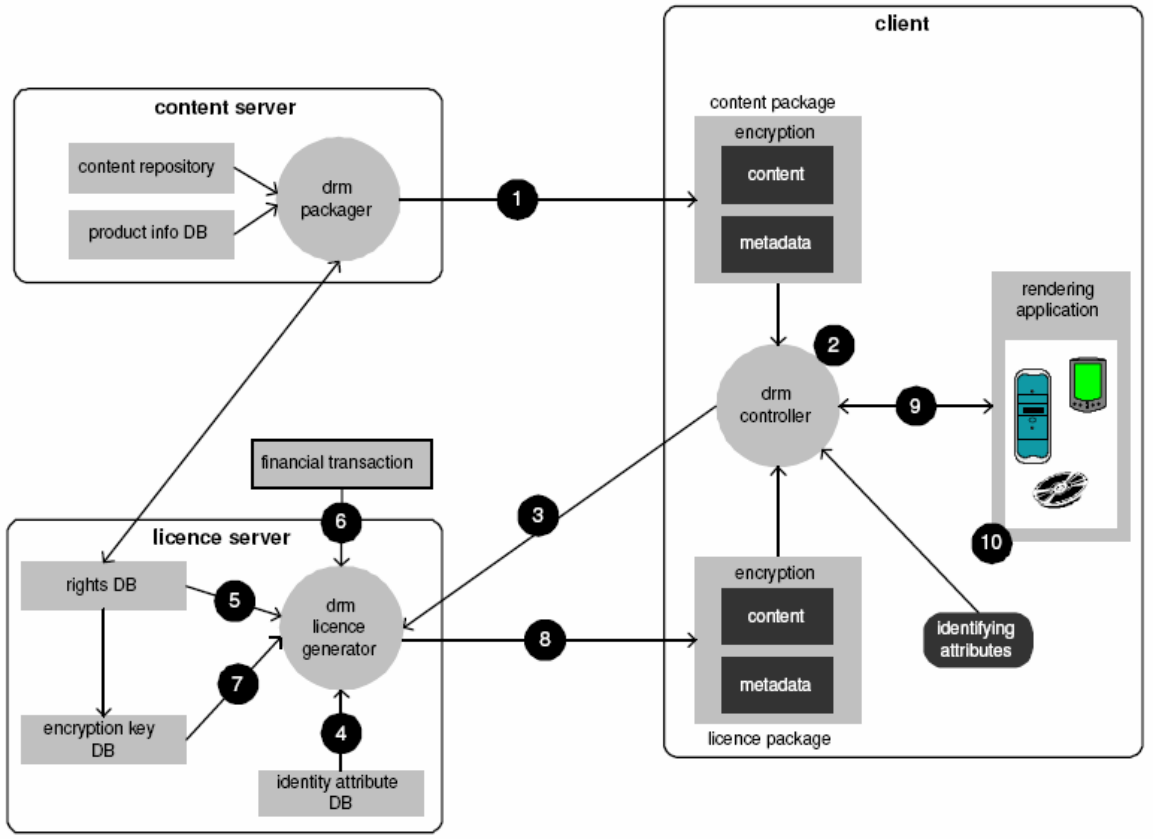

Figure 4: A typical DRM Model

Also, along with the content delivery, one has to even track payments and other financial considerations. Some of the online services are subscription based and as such we have to see that the user doesn't use the content after his license expires.

11 DIGITAL RIGHTS MANAGEMENT MODELS AND ARCHITECTURES

Various different models and architectures have been pruposed for Digital Rights Management.

11.1 Rosenblatt Model[8]

Figure 4 shows one such model[9]

1. User obtains content.
2. User attempts to use/render the content in some way. This triggers the DRM controller. Once activated, the DRM controller gathers information necessary for generating a license. This includes identity information for the user and/or client device and information from the content package, including the content identifier.
3. DRM client makes rights request.
4. The license server verifies the submitted client identification or attributes credentials against an identity database.
5. The license server looks up rights specifications (rules) for the content.

[8] "Digital Rights Management: Business and Technology" - Rosenblatt, B.Trippe W. Mooney S., Wiley; 1st edition (Nov, 2001)

[9] "Interoperability challenges for DRM systems" - Schmidt, A.U. Tafreschi, O. WolfIn R., International Workshop for Technology, Economy, Social and Legal Aspects of Virtual Goods, Ilmenau, Germany, 2004

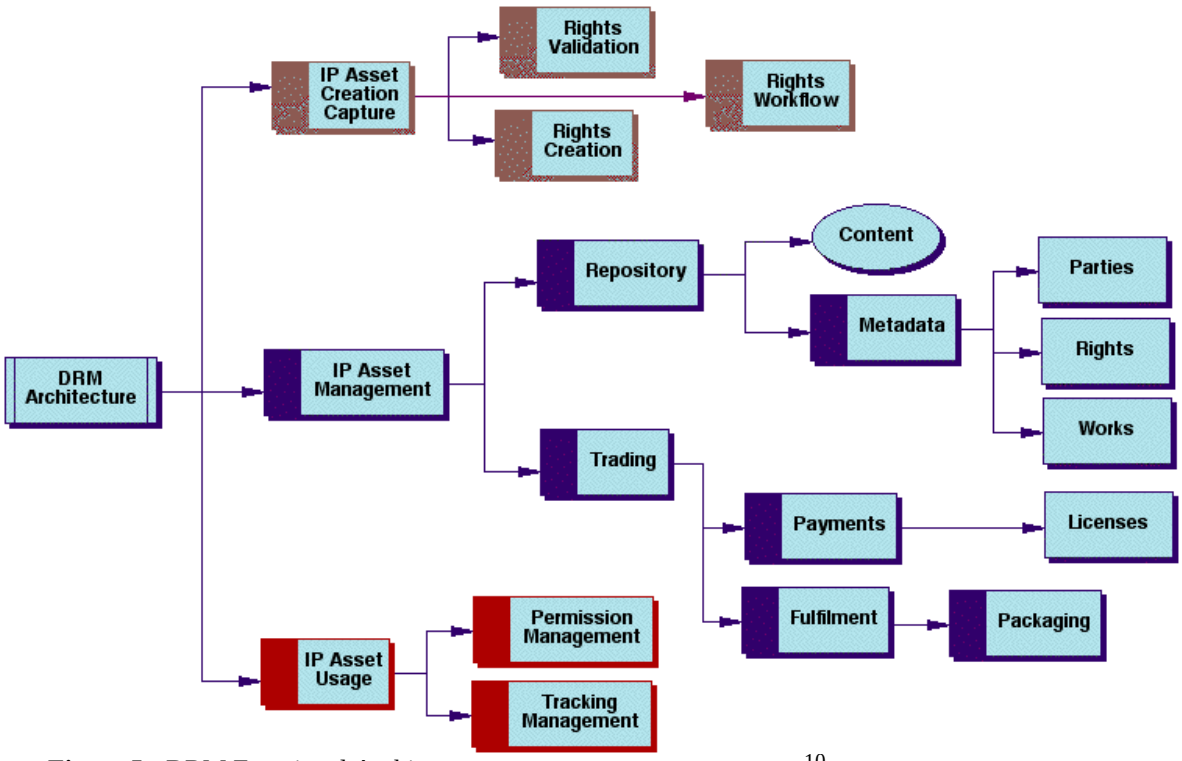

Figure 5: DRM Functional Architecture

6. A financial transaction is launched, if none has been recorded and the rules require it.

7. The license generator compiles rights information, client identity information, and encryption keys, and creates a license, which is itself encrypted or at least tamper proofed.
8. The license is sent back to the client.
9. After the license is generated and any authentication steps are completed, the DRM controller can decrypt the content and release it to the rendering application.
10. Finally, the rendering application plays or shows the content to the user.

11.2 Iannella Architectures

Renato Iannella, Chief Scientist IPR Systems had proposed various different architectures for Digital Rights Management.[10] While designing a DRM system we should consider two architectures. The first is the Functional Architecture, which covers the high-level modules or components of the DRM system that together provide an end-to-end management of rights. The second critical architecture is the Information Architecture, which covers the modeling of the entities within a DRM system as well as their relationships.

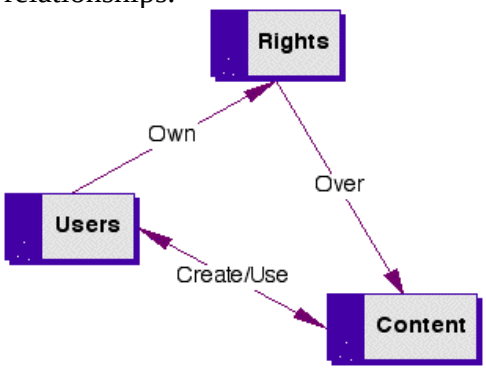

Figure 6: DRM Information Architecture

[10] "Digital Rights Management (DRM) Architectures" - Iannella, R., D-Lib Magazine, Volume 7 Number 6

Figure 5 shows a Functional Architecture while, Figure 6, below, shows an Information Architecture.

11.3 Safavi-Naini Model

A Third model was pruposed by R. Safavi-Naini *et al* in their workshop presentation[11]

This model is shown below

This Model has 4 components

a. *The Content provider:* This maybe an online shop or a content source.

b. *The distributor:* Provides distribution channels, such as an online shop or a web retailer. The distributor receives the digital content from the content provider and creates a web catalogue presenting the content and rights metadata for the content promotion.

c. *The consumer:* Uses the system to consume the digital content by retrieving downloadable or streaming content through the distribution channel and then paying for the digital license. The player/viewer application used by the consumer takes charge of initiating license request to the clearinghouse and enforcing the content usage rights.

d. *The clearinghouse:* Handles the financial transaction for issuing the digital license to the consumer and pays royalty fees to the content provider and distribution fees to the distributor accordingly. The clearinghouse is also responsible for logging license consumptions for every consumer.

12 CURRENT DIGITAL RIGHTS MANAGEMENT SYSTEMS

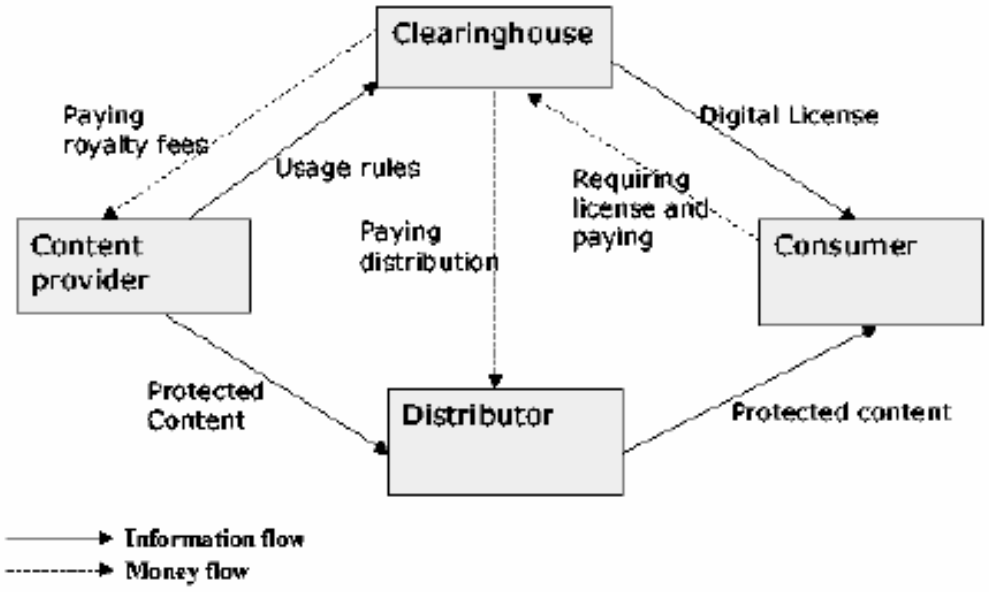

Figure 7: Another DRM Model

12.1 Microsoft's Windows Media Rights Management[12]

(The following contents taken from Microsoft's website)

[11] "Digital rights management for content distribution" - Liu Q. Safavi-Naini R. Shepperd N.P., Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003

[12] Microsoft (www.microsoft.com)

Windows Media Rights Manager lets content providers deliver songs, videos, and other digital media content over the Internet in a protected, encrypted file format. Windows Media Rights Manager helps protect digital media (such as songs and videos) by packaging digital media files. A packaged media file contains a version of a media file that has been encrypted and locked with a "key." This packaged file is also bundled with additional information from the content provider. The result is a packaged media file that can only be played by a person who has obtained a license.

The basic Windows Media Rights Manager process is as follows:

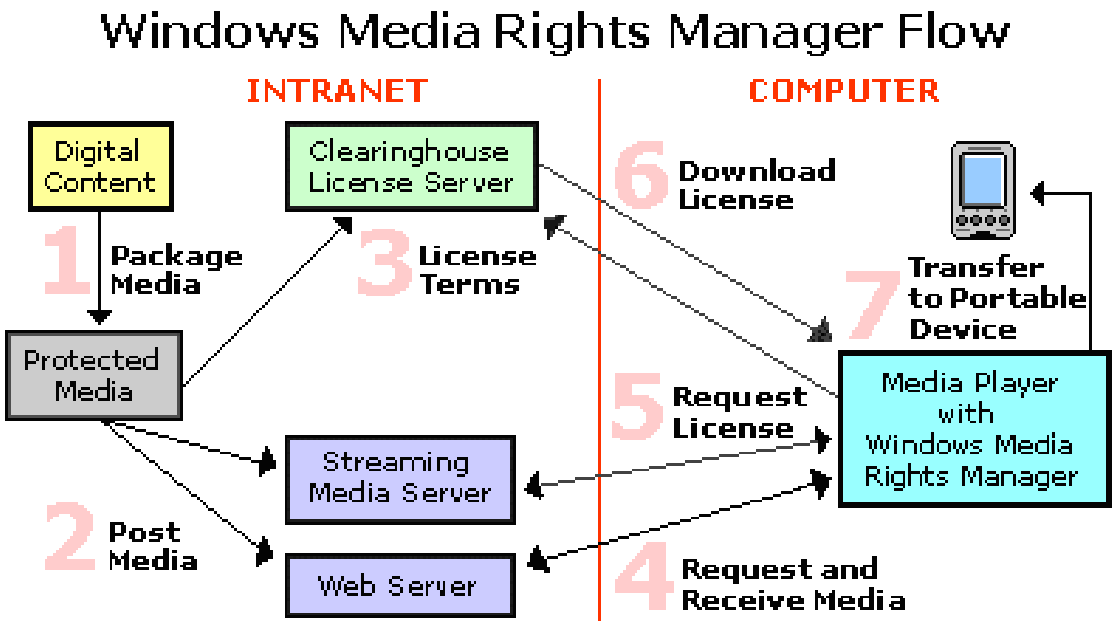

Figure 8: Microsoft's WMRM

a. *Packaging:* Windows Media Rights Manager packages the digital media file. The packaged media file has been encrypted and locked with a "key." This key is stored in an encrypted license, which is distributed separately. Other information is added to the media file, such as the URL where the license can be acquired. This packaged digital media file is saved in Windows Media Audio format (with a .wma file name extension) or Windows Media Video format (with a .wmv file name extension).

b. *Distribution:* The packaged file can be placed on a Web site for download, placed on a media server for streaming, distributed on a CD, or e-mailed to consumers. Windows Media Rights Manager permits consumers to send copy-protected digital media files to their friends, as well.

c. *Establishing a License Server:* The content provider chooses a license clearing house that stores the specific rights or rules of the license and implements the Windows Media Rights Manager license services. The role of the clearing house is to authenticate the consumer's request for a license. Digital media files and licenses are distributed and stored separately, making it easier to manage the entire system.

d. *License Acquisition:* To play a packaged digital media file, the consumer must first acquire a license key to unlock the file. The process of acquiring a license begins automatically

when the consumer attempts to acquire the protected content, acquires a pre delivered license, or plays the file for the first time. Windows Media Rights Manager either sends the consumer to a registration page where information is requested or payment is required, or "silently" retrieves a license from a clearing house.

e. *Playing the Media File:* To play the digital media file, the consumer needs a media player that supports Windows Media Rights Manager. The consumer can then play the digital media file according to the rules or rights that are included in the license. Licenses can have different rights, such as start times and dates, duration, and counted operations. For instance, default rights may allow the consumer to play the digital media file on a specific computer and copy the file to a portable device. Licenses, however, are not transferable. If a consumer sends a packaged digital media file to a friend, this friend must acquire his or her own license to play the file. This PC-by-PC licensing scheme ensures that the packaged digital media file can only be played by the computer that has been granted the license key for that file.

12.2 Real Networks' RealSystems Media Commerce Suite[13]

RMCS (RealNetworks 2001) offers a packaging server, streaming server, license server and a secure file format plug-in for RealPlayer. This system provides Windows and UNIX solutions and supports subscription, video on demand and other business models.

12.3 Real Networks' Helix DRM[14]

Helix is a comprehensive and flexible platform for the secure media content delivery of standards-based as well as leading Internet formats, including RealAudio, RealVideo, MP3, MPEG-4, AAC, H.263 and AMR. Helix DRM makes it possible to deliver these formats not only to PCs but also to a wide array of non-PC devices, including mobile devices and home appliances.

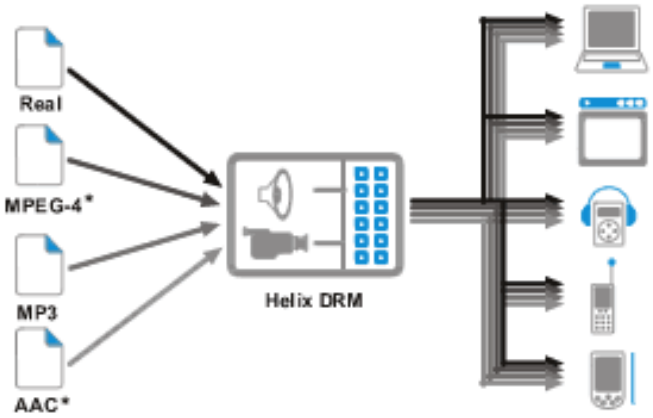

Figure 9: Real Networks' Helix DRM

Helix DRM includes a set of products and services enabling business models through secure rights managed distribution of movies, music and other digital content to millions of media player users worldwide.

12.4 IBM's Electronic Media Management System

IBM has developed a DRM platform, entitled Electronic Media Management System (EMMS), which provides extensive functionality to content owners, distributors and consumers. EMMS is really a set of components which can be mixed and matched to make up a full DRM solution to suit a particular environment or application. By creating the software as a set of components, which interact with each other, IBM has provided content owners, businesses, retailers and consumers with

[13] Real Networks (www.real.com)
[14] Real Networks (www.realnetworks.com)

a group of solutions to meet their digital distribution and consumption needs.
The components of the EMMS suite comprise the following modules[15]:
a. *Content Preparation:* It enables content owners to encode their content (using encryption techniques), set the rules under which it can be accessed and distribute it, either directly to consumers or through distribution partners. Peer-to-peer distribution is also enabled.
b. *Content Mastering:* It enables music content owners to enforce rights, which can be flexibly set. The software enables compression of the source material, which can be economically batch handled, and the inclusion of metadata. Content can be either streamed or downloaded.
c. *Web Commerce Enabler*: It enables the integration DRM based services into web applications, including the presentation of metadata in user-friendly form. Enables tracking, rule based usage to provide for rich business models.
d. *Clearinghouse program:* It enables the logging and reporting of all licensing transactions based on secure encryption and enforcement of rules.
e. *Content Hosting Service:* It enables the secure hosting of prepared content. Content is distributed on request from a customer and reports back to the rights controller.
f. *Multi-device server:* It enables the distribution of secured content to intelligent devices, such as kiosks. The software converts content into the format appropriate to the requesting device. The software is capable of delivering secure content to the wireless environment.
As of 15th September, 2005 IBM has stopped this service.

12.5 InterTrust's Rights|System[16]

InterTrust Technologies Corporation was founded by Victor Shear in 1990 to develop and market technologies for DRM Rights|System offers a solution for content packaging, distribution and rights management based on a packager program and rights server technology. This system supports pay-per-use, rentals, sales, and try-before-buy business models.
Also this system not only works on PCs but other devices like PDAs and cellphones.

12.6 Apple Computer's FairPlay[17]

(Copyright: FairPlay, iPod, iTunes and iTunes Music Store are trademarks of Apple Computers and as such they hold copyrights to the same)
FairPlay is Apple Computer's name for its digital rights management (DRM, alternately: "Digital Restrictions Management") built in to the QuickTime multimedia technology and used by the iPod, iTunes, and the iTunes Music Store. Every file bought from the iTunes Music Store with iTunes is encoded with FairPlay. It digitally encrypts AAC audio files and prevents users from playing these files on unauthorized computers.
FairPlay is a fairly simple implementation of common DRM techniques. FairPlay-protected files are regular MP4 container files with an encrypted AAC audio stream. The audio stream is encrypted using the Rijndael algorithm in combination with MD5 hashes. The master key required to decrypt the encrypted audio stream is also stored in encrypted form in the MP4 container file. The key required to decrypt the master key is called the "user key".

[15] Europe 4 DRM (www.europe4drm.com)

[16] InterTrust Technologies (www.intertrust.com)
[17] Apple Computers (www.apple.com)

Each time a customer uses iTunes to buy a track a new random user key is generated and used to encrypt the master key. The random user key is stored, together with the account information, on Apple's servers, and also sent to iTunes. iTunes stores these keys in its own encrypted key repository. Using this key repository, iTunes is able to retrieve the user key required to decrypt the master key. Using the master key, iTunes is able to decrypt the AAC audio stream and play it.

When you authorize a new computer, iTunes sends a unique machine identifier to Apple's servers. In return it receives all the user keys that are stored with the account information. This ensures that Apple is able to limit the number of computers that are authorized and makes sure that each authorized computer has all the user keys that are needed to play the tracks that it bought.

When you deauthorize a computer, iTunes will instruct Apple's servers to remove the unique machine identifier from their database, and at the same time it will remove all the user keys from its encrypted key repository.

The iPod also has its own encrypted key repository. Every time a FairPlay-protected track is copied onto the iPod, iTunes will copy the user key from its own key repository to the key repository on the iPod. This makes sure that the iPod has everything it needs to play the encrypted AAC audio stream.

At this time, it looks like the restrictions mentioned above are hard-coded into QuickTime and the iTunes application and not configurable in the protected files themselves.[18]

In July 2004, RealNetworks introduced their Harmony technology. The Harmony technology is built into RealPlayer and allows users of the RealPlayer Music Store to play their songs on the iPod. Before the introduction of Harmony this was not possible, because the RealPlayer Music Store uses a different scheme, called Helix DRM, to protect their content that was incompatible with that used by Apple. While using RealPlayer to transfer a Helix DRM-protected song onto the iPod, Harmony transparently converts it to a FairPlay-compatible protected file. Real argued that Harmony was a boon to consumers that "frees" them "from the limitation of being locked into a specific portable device when they buy digital music."[19]

13 DIGITAL RIGHTS MANAGEMENT FOR PUBLISHED WORK

Published work has been so far been least affected by piracy. This is for coupe of reasons. People still like to buy them in printed format and secondly the libraries for such content have not been extensive.

However the situation is changing as more and more books, journals and publications are converted into digital format because of ease in indexing them, referencing them and storing them.

While we consider digital publish work, we have to consider that unauthorized copying doesn't mean copying it from one digital storage to another but we can convert so called soft copies into printed hard copies.

pdf format by Adobe Systems[20] and Microsoft's word are currently the most used formats to store text files. These formats have in their recent versions

[18] Wikipedia (en.wikipedia.org/wiki/FairPlay)

[19] Real Networks' Press Release, 2004 (http://www.realnetworks.com/company/press/releases/2004/harmony.html)

[20] Adobe Systems (www.adobe.com)

have added Digital Rights Management features into them. They are
Printability, Content Extraction, Copying, Modification, Password Protection, Template Creations, Digital Signatures and finally Encryption.
While the delivery method for these files are same as any other digital content and can follow any model possible, the delivery method for subscription based system is different.
Most of these digital libraries have so called search features. Example are Amazon (www.amazon.com) or Google Scholar and Google Books (www.google.com) These digital libraries have indexed the complete contents of their digital liberary so that when a user uses for a particular book or publication using keyword we have to see that a malicious user is not able to extract a book's complete text using this key word search. This is usually done buy limiting the number of pages a user can see for a particular key word search. However it is technically possible for a person to do repeated searches with different key pages, it will be literally impossible for him to do so. Consider an example here. If there are 500 pages in a book and at max 4 pages are displayed, then the minimum number of searches required will be 125 excluding the fact that the key words must be substantially be different, exclude conjunctions and all and also the fact that no pages are repeated. It would be difficult to come up with a automated system because the keyword selection is important.
For example we cannot have the keyword cake if we are searching for a book on the French Revolution.

14 DIGITAL RIGHTS MANAGEMENT FOR SOFTWARES

Softwares after music and movies are the next most pirated items. The reson for this being the cost of softwares is pretty high, especially for a person residing in Economically backward regions.
Digital Rights Management for softwares are divided into two parts.
a. *Pre-Delivery:* This depends on what delivery method is employed to deliver the content to the end user. If the delivery method is physical, that is the software is delivered on a physical medium like a DVD, CD or other storage device, then the software vendor employs copy protection scheme on to physical medium. Also, sometimes like in video games, the software requires the presence of the disk for proper running. If the delivery medium is online, then various other content delivery management is done same way as for other digital content distribution. That is providing the end user with a digital copy of the license and delivering the software using a secure channel.
b. *Post-Delivery:* After the software is delivered several steps is employed to prevent unauthorized use like:
Asking the user to enter a license number or product key while installing the software. This key comes along with the license and is usually generated using a fixed algorithm similar to a hashing algorithm with input that of a serial number.
Asking the user to activate his software after installation.
Software companies like Microsoft (www.microsoft.com), Adobe Systems (www.adobe.com), Real Networks (www.real.com) and Symantec (www.symantec.com) have special activation requirements.
The copy of software is then uniquely associated with a particular computer, thus preventing pirating of the software

by using the same disk to upgrade multiple machines.
This is one of the highest controversial features of such software but of lately more and more software vendors have started using this method.

15 SHORTCOMINGS OF CURRENT DIGITAL RIGHTS MANAGEMENT TECHNIQUES

Even though current Digital Rights Management provide robustness and fulfill all the requirements:
a. Provide enough security to the digital content so that it cannot be altered, modified or copied without authorization.
b. Have a reliable and robust channel for delivery.
However these techniques are not low on shortcomings Some of them are listed below.
a. *Fair Use:* The major shortcoming is that most of the end users feel that Digital Rights Management violates their Fair Use rights. Fair Use means that a user can use a content however he wants and whenever he wants until he is honoring the license agreement. Also he can make back up copies of his content until he is not re-distributing it.
Most of the digital contents which have undergone Digital Rights Management techniques do not support Fair Use.
For example you cannot make copies of your digital music or movies on DVDs. You cannot make back up copies your softwares.
Also, some of the subscription based services like Napster (www.napster.com) or Audible (www.audible.com) need you to log in once in a while to validate your subscription status. If such server is down, you cannot use your content even if you have licence to do so.
b. *Interoperability:* Due to proprietary nature of some of the techniques they are not interoperable or compatible with each other.
For example a music file purchased from Apple's iTunes (www.apple.com/itunes) cannot be played on Microsoft's Windows Media Player. Even if you have license for the file, the DRM Techniques employed by Apple is different from that employed by Microsoft.
Apple will want people to use their iTunes software to play music purchased from their online shop, while Microsoft will want users to use their media player to play contents which use WMRM.
c. *Portability:* Digital Rights Management doesn't provide portability, at least not completely.
That is the digital content downloaded onto one computer cannot be used onto another computer or device.
This is a real problem because there maybe more than one device which can be used to play a digital content. A person may not want to be restricted to playing music on his computer or playing his movie on a particular player.
DVD Region Codes prevent a person from playing 1 region's DVD in another region's player. So what to do if you are traveling abroad?
iTunes prevents users from playing a file until that computer is associated with your account.
d. *Privacy:* Is a major concern of the end user. To acquire a license or a digital content one has to divulge their imformation ranging from just names to their credit card information. Also, software activation features "scan" the computers for identifiers.
So privacy is a major concern. It is a fine balance because, DRM techniques

require authentication to verify or give out license.

f. *Monopolistic Behavior:* Some of the entities which provide Digital Rights Management systems or solutions also manufacture their own hardware or software. Hence they will tend to make the DRM system such that they can market their own products. They can prevent other hardware/software vendors from using their technique or not support other vendor's hardware/software.

According Adam L. Penenberg "What's hardest for the consumer to swallow, then, is that anti-piracy schemes like DRM look like the subtle tactic of the monopolist. Neither Apple nor Microsoft is hurt by music piracy. Instead, they use it as a marketing ploy to force people to use their products. It doesn't have to be this way. The companies could agree on one standard that allows people to play the music they lawfully purchase on whichever player they choose. The music industry is supposed to sell music, not the medium it comes in, right?"[21]

16 REQUIREMENT FOR STANDARDIZATION

It can be inferred that all the short comings of Digital Rights Management comes from there not being a common standard. While each standard - MPEG, OMA, W3C and DVD CCA specifies how to provide Digital Rights Management for their formats, there is no common standard which a technique has to comply to conform to above mentioned standards.

The commercial environment increasingly relies on standards. In the global economy, where a common infrastructure of understanding is essential, standards are used both to create markets and to maintain them in an efficient, interoperable state. This is true in both business and technical senses.

16.1 MPEG-4

In MPEG-4, all encoded media objects are accompanied by metadata called object descriptors (ODs). Part of an OD is the Intellectual Property and Management (IPMP) descriptor (IPMP-Ds) which carries information relating to rights management. General DRM information not related to specific objects is carried in IPMP elementary streams (IPMP-ESs). IPMP-Ds and IPMP-ESs provide a communication mechanism between IPMP systems and the MPEG-4 terminal. Certain applications may require multiple IPMP systems. When MPEG-4 objects require management and protection, they have IPMP-Ds associated with them. These IPMP-Ds indicate which IPMP systems are to be used, and provide information to these systems about how to manage and protect the content.[22]

16.2 W3C

World Wide Web Consortium (W3C) develops and promotes standard technologies for the Web, such as HyperText Markup Language (HTML), Extensible Markup Language (XML) and Cascading Style Sheets (CSS). Of these three standards, perhaps the most important to management of digital rights is XML, a baseline language that has been used extensively to support messaging for digital rights management technologies.

[21] "How Apple, Microsoft, and Sony cash in on piracy prevention" - Adam L. Penenberg, slate.com Nov 2005

[22] Digital rights management and watermarking of multimedia content for m-commerce applications" - Hartung, F. Ramme, F. Communications Magazine, IEEE Nov 2000

*(**Note:** Digital Rights Management using XrML is discussed later in the paper)*

14.3 OMA

The Open Mobile Alliance (OMA) was formed in June 2002 by nearly 200 companies including the world's leading mobile operators, device and network suppliers, information technology companies and content and service providers.

The scope of OMA "Digital Rights Management" is to enable the controlled consumption of digital media objects by allowing content providers to express usage rights, example, the ability to preview DRM content, to prevent downloaded DRM content from being illegally forwarded (copied) to other users, and to enable new business models with super distribution of DRM content.[23]

16.4 SDMI

SDMI (Secure Digital Music Initiative) was a forum formed in late 1998, comprised of more than 200 IT, consumer electronics, security technology, ISP and recording industry companies with the purpose of developing technology specifications that protect the playing, storing and distributing of digital music.

Specifically, the goals of the SDMI were to provide consumers with convenient access to music online and in new digital distribution systems, to enable copyright protection for the work of artists, and to promote the development of new music-related business and technologies. SDMI was a direct response to the widespread success of the MP3 file format.[24]

SDMI has been inactive as of May, 2001

This is a major concern because, the major digital content that has been affect by piracy has been music. There currently exists no standard for implementing Digital Rights Management in music. Also, each online music provider now follows his own format making them highly incompatible with each other.

16.5 DVD CCA

The DVD Copy Control Association (DVD CCA) is an organization primarily responsible for the copy prevention of DVDs. The content scrambling system (CSS) was devised for this purpose to make copyright infringement difficult. The association is also responsible for the much criticized regional playback control (RPC), the region encoding scheme which gives movie studios geographic control over DVD release dates to maximize their investments and also help thwart copyright infringement.[25]

All hardware manufacturers, especially DVD player/burner manufacturers, implement DVD CCA-mandated enforcement features on their products; Some even go beyond that and implement additional features to restrict ripping, for example:

a. *RIPLOCK:* Many manufacturers (NEC) put an artificial limit, or lock, on ripping speeds. Some of these drives have alternative 3rd-party firmwares that have this removed to enable faster ripping.

b. *RPC-2:* Many manufacturers put a limit on the number of times you can "change the region" of a drive, usually 5 times or less; after these number of changes, the drive becomes "locked" on the last region you set and you can't

[23] Open Mobile Alliance (www.openmobilealliance.org)

[24] Wikipedia (en.wikipedia.org/wiki/SDMI)

[25] Wikipedia (en.wikipedia.org/wiki/DVD_CCA)

change it anymore. Some alternative 3rd-party firmware have this limit removed to enable unlimited region changes like moving from the USA to Germany and back more than 5 times.

c. *RPC-1:* There is a region code present on the drive, and it will be changed if a DVD from another region is read. Usually, there is no limit on the number of changes that can be done to the DVD region.

d. *Bitsetting/Booktyping:* This is a feature which makes DVD+Rs readable by older DVD players that can play DVD-ROMS only. Some manufacturers disable this feature on their drives; Again, some alternative 3rd-party firmwares can enable this so that burned DVDs appear as DVD-ROMs and are playable by older DVD players.

17 FUTURE DIGITAL RIGHTS MANAGEMENT SYSTEMS

There are various proposed systems and system architectures for future implementation

17.1 ORDM

Current techniques have emphasis on protecting the content rather than managing rights. Hence we have all the short comings mentioned above. A solution to this is using Open Digital Rights Management. It should be confused with Open Source because even with similarity in names they have nothing in common.

ORDM is focused on interoperability across multiple sectors and support for fair-use doctrines.

The ODRM Framework consists of Technical, Business, Social, and Legal streams as shown in figure.

The ODRM Technical stream consists of an Architecture (ODRA) which includes a Trading Protocol (ODRT) and Protection (ODRP) mechanisms with the Language (ODRL) clearly focused on solving a common and extendable way of expressing Rights assertions within this Architecture.

It is envisaged that a rights language (ODRL) will "plug into" an open framework that enables peer-to-peer interoperability for DRM services. However, ODRL can also be used as a mechanism to express rights statements on its own and to plug into existing DRM architectures, for example, the Electronic Book Exchange framework.[26]

17.2 FDRM

Federated Digital Rights Management (FDRM) is a proposed DRM Solution for Research and Education.

FDRM is being pursued by members of the VidMid Video-on-Demand Working Group[27], a collaboration between the Internet2 Middleware Initiative and the Video Development Initiative[28].

FDRM is founded on directory services infrastructure and identity management principles currently in use and emerging in Higher Education today.

The features of FDRM are as follows[29]:

a. Interoperable with any authentication and authorization mechanism.

b. FDRM is designed to be extensible, include broader access controls in future phases, and to interoperate with commercial mechanisms for rights enforcement.

c. FDRM is designed to interoperate with existing enterprise directories, rights, descriptive and administrative

---

[26] "Open Digital Rights Management" - Iannella R., Position paper for the W3C DRM Workshop, W3C 2000

[27] VidMid (middleware.internet2.edu/video)

[28] The Video Development Initiative (http://www.vide.net)

[29] "Federated Digital Rights Management" – Martin M. Agnew G. *et al*, D-Lib Magazine, Volume 8 Number 7/8

metadata schemas, commercial DRM systems, and user-level Public Key Infrastructure (PKI).
d. FDRM is designed to scale for campus/enterprise implementations.
e. FDRM is designed to support secure messaging, maintain integrity of content, protect intellectual property, and ensure the integrity of rights and descriptive metadata.
f. FDRM uses open standards and protocols. New code or standards developed will be placed in the public domain.
g. FDRM is designed to be applicable to all media types, formats and standards.

17.3 XrML

XrML is a language in XML (eXtensible Markup Language) for describing specifications of rights, fees and conditions for using digital contents (or properties), together with message integrity and entity authentication. XrML documents are XML conforming so they are readily viewed, edited, and alidated with standard XML tools for example XML SPY. It is intended to support commerce in digital contents, and also intended to support specification of access and use controls for secure digital documents in cases where financial exchange is not part of the terms of use. In additionally, XrML supports and accommodates other industry standard, such as SSL, public/private key encryption and the DOI initiative.
XrML describe rights, fees and conditions appropriate to commerce models they select, provide standard terms for usage rights with useful, concise and easily
understandable meanings, offer vendors operational definitions of trusted systems for compliance testing and evaluation, provide extensibility to new language features without compromising XrML's other goals, provides an open architecture, scalability, customization, extensibility and the capacity to integrate with both existing systems and new ones as they are developed.[30]

CONCLUSION

Over all we can conclude that Digital Rights Management Techniques that are currently available have more or less achieved their objective of providing ways and means of transferring digital content from one person to another. However, there is a still lot to achieve and long way to go.
While current techniques emphasize on protecting the copyrights and rights of the content providers, the rights and concerns of the user has been invariably neglected.
Future systems and techniques have to seriously consider the users rights and requirements. While technology exists to protect digital contents from tamper, Digital Rights Management techniques shouldn't give more weightage to this aspect but rather to the aspect of managing the rights like the name suggest.
This can be having a robust standards and specifications and more emphasis should be given to license management and delivery systems.

Keywords: Digital Rights Management, DRM

[30] "Digital rights management (DRM) using XrML" - Guo H., Seminar on Network Security 2001

REFERENCES

[1] International Intellectual Property Alliance (www.iipa.com)

[2][4][22] "Digital rights management and watermarking of multimedia content for m-commerce applications" - Hartung, F. Ramme, F. Communications Magazine, IEEE Nov 2000

[3] United States Copyright Office (www.copyright.gov)

[5] "Secure spread spectrum watermarking for images, audio and video" - Cox, I.J. Kilian, J. Leighton, T. Shamoon, T. Proceedings on Image Processing, IEEE Sep 1996

[6] "Dither modulation: a new approach to digital watermarking and information embedding" - Chen, B. Wornell, G.W. Proceedings Security and Watermarking of Multimedia Contents, SPIE Apr 1999

[7] "Copy Protection for DVD Video" Bloom, J. Cox, I.J. Kalker, T. Jean-Paul, M. Linnartz, G. Miller, M.L. Brendan, C. Traw S.Proceedings of the IEEE, 1999

[8] "Digital Rights Management: Business and Technology" - Rosenblatt, B.Trippe W. Mooney S. Wiley; 1st edition (Nov, 2001)

[9] "Interoperability challenges for DRM systems" - Schmidt, A.U. Tafreschi, O. WolfIn R. International Workshop for Technology, Economy, Social and Legal Aspects of Virtual Goods, Ilmenau, Germany, 2004

[10] "Digital Rights Management (DRM) Architectures" - Iannella, R., D-Lib Magazine, Volume 7, Number 6

[11] "Digital rights management for content distribution" - Liu Q. Safavi-Naini R. Shepperd N.P., Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003

[12] Microsoft (www.microsoft.com)

[13] Real Networks (www.real.com)

[14] Real Networks (www.realnetworks.com)

[15]Europe4DRM (www.europe4drm.com)

[16] InterTrust Technologies (www.intertrust.com)

[17] Apple Computers (www.apple.com)

[18] Wikipedia - FairPlay (en.wikipedia.org/wiki/FairPlay)

[19] Real Networks' Press Release, 2004 (http://www.realnetworks.com/company/press/releases/2004/harmony.html)

[20] Adobe Systems (www.adobe.com)

[21] "How Apple, Microsoft, and Sony cash in on piracy prevention" - Adam L. Penenberg, slate.com Nov 2005

[23] Open Mobile Alliance (www.openmobilealliance.org)

[24] Wikipedia - SDMI (en.wikipedia.org/wiki/SDMI)

[25] Wikipedia - DVD CCA (en.wikipedia.org/wiki/DVD_CCA)

[26] "Open Digital Rights Management" - Iannella R., Position paper for the W3C DRM Workshop, W3C 2000

[27] VidMid (middleware.internet2.edu/video)

[28] The Video Development Initiative (http://www.vide.net)

[29] “Federated Digital Rights Management” – Martin M. Agnew G. et al, D-Lib Magazine, Volume 8, Number 7/8

[30] “Digital rights management (DRM) using XrML” - Guo H., Seminar on Network Security 2001

"Digital Rights Management: The Technology Behind the Hype" - Stamp M., Journal of Electronic Commerce Research, 2003

"Digital Rights Management in Consumer Electronics Products" - Index A. Reflections L., IEEE Signal Processing Magazine, 2004

"Fair use, DRM, and trusted computing" - Erickson J.S., Communications of the ACM, ACM, 2003

"Digital watermarking for telltale tamper proofing and authentication" - Kundur D. Hatzinakos D. Proceedings of the IEEE, 1999

"Digital watermarking of raw and compressed video" Hartung F. Girod G.Proceedings of European EOS/SPIE Symposium on Advanced Imaging

"Content-Based Digital Signature for Motion Pictures Authentication and Content-Fragile Watermarking" - Dittmann J. Steinmetz A. Steinmetz R. Proceedings of ICMCS, IEEE Volume 2, 1999

"Evaluating New Copy-Prevention Techniques for Audio CDs" Halderman J.A. Digital Rights Management: ACM CCS-9 Workshop, DRM, 2002

"Models and Languages for Digital Rights" - Gunter C.A. Weeks s. Wright A.K., Proceedings of the 34th Hawaii International Conference on System Sciences, IEEE 2001

"Digital rights management and fair use by design: Introduction" Mulligan D.K. Communications of the ACM
Volume 46, Number 4, 2003

"The Design of a DRM System Using PKI and a Licensing Agent" - Lee K.W. Park J.P. Lee K.H. Lee J.H. Kim H.S., Proceedings Network and Parallel Computing: IFIP International Conference, NPC, 2004

"LicenseScript: A novel digital rights language and its semantics" - Chong C.N. Corin R. et al, Proceedings of 3rd International Conference on Web Delivering of Music, IEEE, 2003

"Digital Rights Technology Sparks Interoperability Concerns" - Geer D., Computer, IEEE, 2004

"Privacy and Digital Rights Management" - Vora P. Reynolds D. et al Proceedings of W3C workshop on Digital Rights Management, W3C Jan 2001

"The Present and Future of Digital Rights Management - Musings on Emerging Legal Problems" - Bechtold S.

"Towards A Digital Rights Management Framework" O Pitkaenen O. Vaelimaeki M., IeC2000 Conference Proceedings, IeC, 2000

"Can digital rights management be standardized" - Rump N., Signal Processing Magazine, IEEE May 2004

"A DRM Security Architecture for Home Networks" - Crispo B. Tanenbaum A.S. et al, Proceedings of the 4th ACM workshop on Digital Rights Management, ACM, 2004

LIST OF FIGURES

REFERENCE WEBSITES

Google (www.google.com)
CiteSeer (citeseer.ist.psu.edu)
Google Scholar (scholar.google.com)
IEEE (www.ieee.org)
IEEE Xplore (ieeexplore.ieee.org)
ACM (www.acm.org)
Wikipedia (www.wikipedia.org)