DIGITAL RIGHTS MANAGEMENT - AN OVERVIEW OF CURRENT CHALLENGES AND SOLUTIONS

Alapan Arnab and Andrew Hutchison

{aarnab, hutch}@cs.uct.ac.za
Data Networks Architectures Group
Department of Computer Science
University of Cape Town
Rondebosch
7701

ABSTRACT

Digital Rights Management (DRM) systems aim to create a secure framework to control access and actions that can be performed by users (both human and machine). DRM technologies have become very important in an increasingly networked world because it promises the owner of the file persistent control over the file even when the file leaves the owner's machine. It is not only useful in combating piracy (which is currently the main use of DRM systems) but also for protecting sensitive documents in enterprises.

DRM systems can be seen to fit at various levels on a computer system - at an application layer, which is currently seen in applications like Apple iTunes; at an operating system level like Microsoft's Rights Management System (RMS) in Windows Server 2003 or at a hardware level like Content Scramble System (CSS) in DVD players. However, current DRM systems are mostly not interoperable and in most cases either do not provide the all requirements expected by the customer or do not provide a totally secure framework.

DRM systems that are used for copyright enforcement give rise to many legal questions mostly revolving on the amount of control the copyright holder has over their creations once they have been distributed. Many of the legal questions do not affect DRM systems for enterprises, but most of the technical requirements are the same.

This paper gives a broad overview of the current state of DRM systems and their strengths and weaknesses. It starts by examining the legal requirements of the system to satisfy both the right holders and the end consumers. We then discuss the structure of DRM systems, their characteristics and how well they satisfy the legal requirements. Finally we review three DRM systems and look at how well they satisfy the requirements desired in a DRM system.

KEYWORDS
DRM, Digital Rights Management, REL, Rights Management

DIGITAL RIGHTS MANAGEMENT - AN OVERVIEW OF CURRENT CHALLENGES AND SOLUTIONS

1 INTRODUCTION

With the proliferation of the Internet, the speed and ease of digital data exchange has increased, together with the number of potential parties that can exchange data. This has also meant that digital data security is no longer confined to the computer that holds the original data, or even behind corporate firewalls. Furthermore, data security no longer applies only to the access to data, but also to what the user can do with the data [4]. Encryption is no longer enough, for a user can easily willingly or unwillingly pass on the unencrypted data to unauthorised users. Thus, there is a growing need for data to not only have access control mechanisms but also to define mechanisms to control the actions of how users use the data.

There are no widely accepted definitions for Digital Rights Management (DRM). Rosenblatt et al. [24] provide two definitions for DRM. In the narrower definition, DRM focuses on *persistent protection of digital data*. This definition refers to technology that protects digital content via encryption and the access control mechanisms that allow a user to view the digital content. In the broader definition, DRM is *everything that can be done to define, manage, and track rights to digital content* [24]. Under this definition, DRM technology also includes technology that manages and tracks digital content on the Internet. DRM is also known by other names, such as Content Management Systems (CMS) [8], Enterprise Right Management Systems (ERMS) [4] etc.

With the rise of music and movie piracy on the Internet, DRM systems have taken the spotlight in the media industry's fight against Internet piracy. However, multimedia is not the only use of DRM systems, and the same techniques can be used to protect documents in enterprises. The main difference lies in the legal framework in which a DRM system is implemented, since the users of media products are customers while in enterprises it is usually meant for employees.

This paper takes a broad overview on:

1. Legal issues regarding DRM systems
2. Distribution architectures of DRM systems
3. How DRM systems work
4. Rights Expression Languages (REL) and XrML
5. Some of the current DRM products and their effectiveness

2 LEGAL BACKGROUND

DRM technologies aim to enforce the legal rights of the owners of the digital media; and thus a discussion on the legal background is necessary to understand some of the problems with current DRM systems. In this discussion, *work* will be used to refer to the digital data that is meant to be protected using DRM.

2.1 The Players in a DRM System

Bartolini et al. [8] mapped out a set of requirements for content management systems to a set of players. Each of these players have different roles within a DRM system and as such, each of these roles have different legal specifications. The roles described by Bartolini et al. were:

1. The author or the creator responsible for creating the work. The author does not necessarily have to be human.

2. The right holder (or copyright owner) of the work. The author is not necessarily the copyright holder and usually the right holder is also referred to as the *owner* of the work.

3. The service producer is the entity that is responsible for the implementation of DRM on the work.

4. The media distributor is the entity that is responsible for distributing the work and usually collecting revenue from the users. In many cases, the media distributor is also the service producer (e.g. Apple iTunes music store).

5. IPR register / database is a server that maps the rights associated with the work to the user. It is also referred to as the license server [23].

6. Unique Number Issuer is responsible for issuing a unique identifier to each creation.

7. The controller is a Trusted Third Party (TTP) that is responsible for ensuring that all the transactions have been carried out legally.

8. The certificate authority is another TTP that is responsible for authenticating all parties in the DRM transaction

However Bartolini et al. does not take into consideration the end user of the work as a player. A DRM enforced work is essentially subject to a contract between the user and the right holder [9] and thus, requires the user to be involved in the transaction. This is further complicated by rights that the user can expect to have in the contract [21].

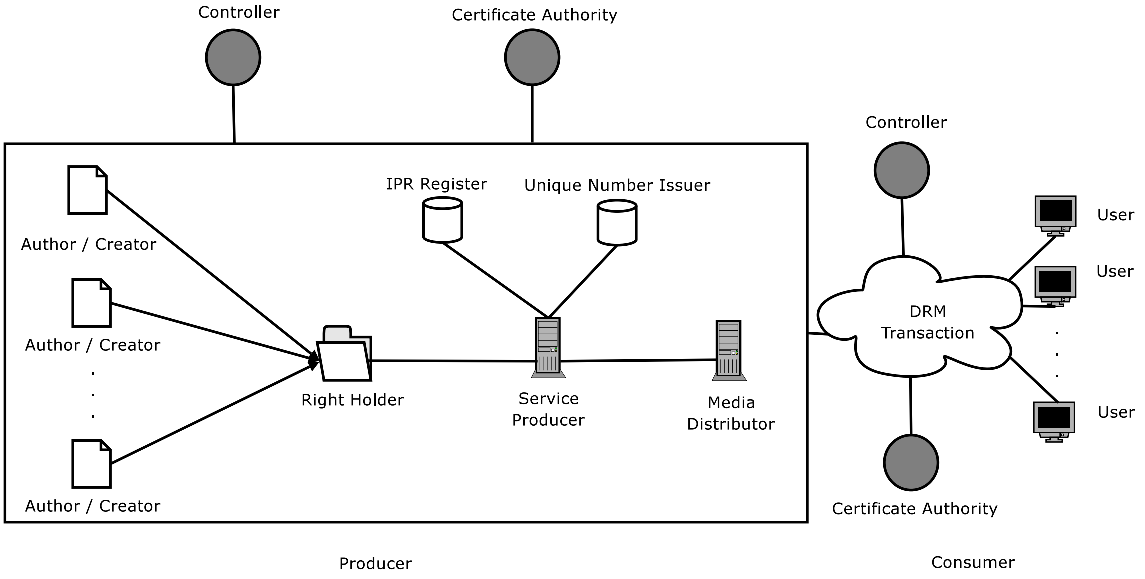

Figure 1: Players in a DRM System

Currently, most DRM systems do not employ any TTPs [23, 21]. The license server is usually deployed by the distributors and identifiers to digital works are managed by the respective distributors. Thus, a DRM transaction currently involves only the end user and the distributor. Figure 1 proposes a DRM system with all the players considered by Bartolini et al. as well as the end users. The transactions between the end users (the consumers of the work) and the producers of the work should also involve a controller to monitor the transactions for correctness and legality. A certificate authority should also be involved to authenticate the users.

2.2 Legal Perspective: The Owner

Both DRM technologies and new legislations in the U.S. and Europe are aiming to help owners to receive their dues [17]. Currently, the majority of DRM systems focus on multimedia, especially music and movies, and the owners (in this case the record and movie companies like AOL Time Warner) would like to use DRM enabled media to combat Internet piracy.

By their very nature, digital works are very easy to replicate. With Peer-to-Peer (p2p) networks and the availability of high speed Internet connections, digital works are also very easy to distribute. This makes it very easy to illegally copy digital works and distribute them, thus udercutting the right holders. The media industry would like to use DRM to enforce copyright on their works and thus receive payment when the user listens to a song, reads a book or watches a movie.

2.3 Legal Perspective: The User

Many end users are very hostile to DRM protected media [3, 5]. Many of their concerns are legitimate and this section looks at some of those concerns, namely fair use, privacy and right holder control. For DRM to be successful in the market place, DRM vendors must address these issues first. However, it must be noted that the concepts of fair use and right holder control only apply in a case where the user purchases or rents a digital work protected by DRM. In the enterprise, the large majority of the fair use and right holder control issues are non-existent.

2.3.1 Fair Use

In the famous *Sony-Betamax* or *Universal City Studios v. Sony Corporation of America*, 446 U.S. 417 case, the U.S. Supreme Court ruled that Sony could not be held liable for illegal copying of copyright works made using their Sony-Betamax video recorder [11]. The case also highlighted the idea of *fair use*[1], some of which is regulated in many countries' copyright laws (e.g. Section 107 in U.S. Copyright Act) [21].

Fair use (also referred to as personal use), usually allows for the reproduction of a copyrighted work for a variety of reasons [21, 27, 1]. Sections 12–19 of South Africa's Copyright Act 98 of 1978 gives the exceptions to copyright which allow users to reproduce (in any form) and excerpt copyrighted works for certain purposes like research or private study, reporting in the media, reviews and criticism, teaching and for backup purposes. There are also cases where there is no current legislation on how copyright regulates the use of a work [21]. These *unregulated* uses include how often, where and when a copyrighted work is used, who uses the copyrighted work or the ability to transfer the ownership of the copyrighted work to another party. Some of these uses are currently regulated by license agreements (esp. on software), but there are usually no mechanisms to enforce these regulations.

There are fears that DRM will allow media companies to protect copyright in the form of license agreements that prevent fair uses [14]. In [14], Dusollier counters that fair use clauses in the European Copyright Directive of 2001 is a legislative way of countering such moves, although the legislation itself does not address all cases of fair use.

Felten argues that the concept of fair use is too broad and not defined well enough to be ever implemented correctly [16]. Fair use is often based on the circumstances of use, thus the fair use of

[1] The concept of fair use itself is not new – it was initially proposed in the early 1800's to allow book buyers leeway in how they used books. Fair use allowances has changed over the years to cater for newer technologies

a copyrighted work will depend on each individual user. Furthermore, implementing fair use will require highly sophisticated AI, and many of the fair use tests are already hard AI problems. Felten believes that these factors make it very difficult for DRM systems to implement fair use.

On the other hand, Bechtold [9] argues that at least DRM vendors should allow for the possibility of enabling fair use. Many of the current DRM products do not allow for fair use [21] even though current right expression languages have the capability to express most of the requirements on an individual basis [9].

2.3.2 Privacy

DRM systems have often been accused of violating user privacy [21] and next to fair use, end user privacy violation (or the potential to) is seen as one of the major problems with many DRM systems [21, 13, 25]. The ability of DRM systems to track the usage of DRM protected media is seen as one of the major violations of privacy. However, Bartolini et al. [8] and Park et al. [22] all put the ability of DRM to track usage as one of the most important in meeting all the objectives. The problem with tracking user usage boils down to how much monitoring is done. In the past, user tracking has been used to look at browsing habits [21] and tracking can be potentially used to track habits of users even when they are not using DRM enabled works.

2.3.3 Right Holder Control

Right holder control is essentially how much the DRM enabled work determines what the user does with the work. In an enterprise scenario, right holder control could be absolutely critical – the enterprise would like to define exactly the boundaries for using the DRM protected work. Consumers however, would like as little control as possible on DRM protected works [21]. This is shown especially with the popularity of Apple iTunes Music Store compared to other music offerings, with the Apple iTunes offering DRM enabled works with the least control and out-selling virtually all other offerings combined. Section 4 takes a more detailed look at the DRM systems used in current music stores.

2.4 Legal Perspective: The Distributer

The distributor is responsible for providing DRM enabled data to the user and at the same time allow the right holders mechanisms to track the illegal use of the data [8]. In many current media distributions, the distributor also plays the role of the license server.

From the user’s perspective, the distributor needs to keep user data confidential and not reveal the data to third parties. Whether the right holders are a third party, however, will usually depend on the license agreements with the end user. Most of the legal concerns of the user (like privacy) are controlled by the distributor and thus it falls on the distributors to solve them.

From the right holders perspective, the distributor must be able to distribute data without compromising the security of the data. If a security compromise does take place, then the distributor must be able to track down the offender [8]. Others have suggested that pirated DRM data must at least be identifiable [12, 26].

2.5 Legal Requirements

For DRM to be effective, the legal concerns of the users and the right holders need to be taken into account. It is very likely that all the fair uses that are expected by users cannot be accounted for in an automatic system and there might be a need for a user to ”apply” to a license server/distributor for a fair use to be enabled (e.g. a magazine writer asking for the right to excerpt from a document). Such a system will however require a third party to authenticate and accredit the users (e.g. the user is a accredited journalist), which is not used in the current implementations of DRM systems. Because DRM has the capability of imposing very tight right holder control, legislation might be required to counteract such a move.

In summary, users would like a DRM system that:

1. can handle most fair use scenarios
2. keeps data collected from users confidential and does not monitor the usage of DRM data[2]
3. allows for the transfer of rights, and
4. is flexible depending on the media/situation

while right holders would like DRM systems that:

1. can keep track of illegal use of DRM enabled media
2. can correctly collect revenue from the usage of their works
3. can create a secure distribution channel, and
4. prevents the illegal use of their works

3 STRUCTURE OF DRM SYSTEMS

In 1999, Bartolini et al. [8] looked at the requirements and the players involved in a possible DRM system. In 2000, Park et al. [22] looked at all the different possible distribution architectures that could be implemented for securing content distribution. This section looks at the different distribution architectures, how all the players fit together to access a DRM enabled work, the types of DRM controllers and gives an overview of right expression languages.

3.1 Distribution Taxonomy

Park et al. gave three factors that distinguish the different security architectures involved in distributing secure content: the presence of a virtual machine (VM), the type control sets and the distribution style. Figure 2 shows the different distribution architectures with the notation used by Park et al. to distinguish between them.

3.1.1 Presence of a virtual machine

The first level of distinction is the presence of a virtual machine (VM). The VM is described by Park et al. as "*software that runs on top of vulnerable computing environment and employs control functions to provide the means to protect and manage access and usage of digital information*" [22]. A VM can be in the form of a plugin that controls access to DRM enabled data or embedded in the application itself. Systems that do not have a VM cannot manage and control access and usage of secure data that the recipient receives, making it unsuitable for use as a DRM solution.

[2] Monitoring of usage will depend on the usage of the data. An enterprise will probably not be willing to take the risk of an employee leaking secrets and thus will monitor all uses of data. Entertainment companies however have not monitored how the content is used by a consumer; and thus the consumers would expect such in DRM enabled media.

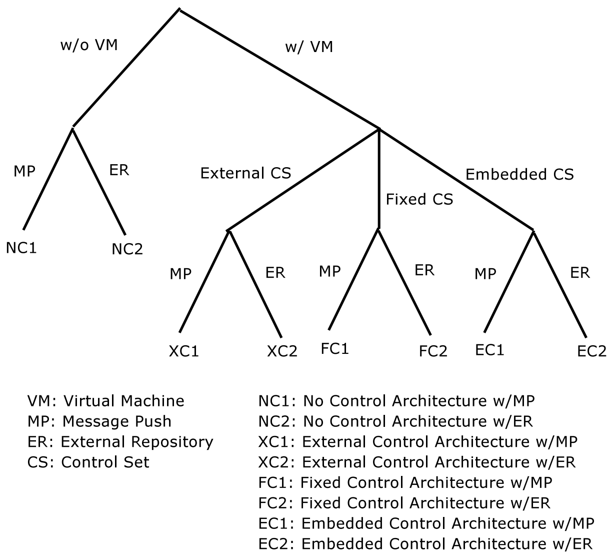
w/o VM
w/ VM
MP
ER
External CS
Fixed CS
Embedded CS
NC1
NC2
MP
ER
MP
ER
MP
ER
XC1
XC2
FC1
FC2
EC1
EC2
VM: Virtual Machine
MP: Message Push
ER: External Repository
CS: Control Set
NC1: No Control Architecture w/MP
NC2: No Control Architecture w/ER
XC1: External Control Architecture w/MP
XC2: External Control Architecture w/ER
FC1: Fixed Control Architecture w/MP
FC2: Fixed Control Architecture w/ER
EC1: Embedded Control Architecture w/MP
EC2: Embedded Control Architecture w/ER

Figure 2: DRM Distribution Architectures [22]

3.1.2 Types of control sets

The second level of distinction is in the type of control set used. Control sets are the rules governing the use of a DRM enabled work, and this has given rise to Right Expression Languages (REL) that allow for the description and specification of the control sets. Park et al. categorised control sets into three types: fixed control sets, embedded control sets and external control sets [22].

In fixed control sets, the virtual machine comes with a predefined control set which is enforced for all DRM enabled data. Fixed control sets are easy to implement, but offer very little flexibility. The encryption system for DVDs (DVD-CSS) is a good example of a fixed control set mechanism and the possible problems with such a mechanism. The DVD-CSS algorithm was flawed and was compromised within a few months of availability of DVD systems. Because of the wide installation base, and the fact that DVD systems could not undergo firmware upgrades, DVD encryption system was as good as not being present at all [21, 9]. While fixed control sets are not suitable for general application in DRM systems, they have been used successfully in other right management systems. For example, the Linux kernel has a system to track whether independently loadable modules (like device drivers) are GPL compatible or not [10].

Embedded and external control sets are more adaptive to the needs of the user. In an embedded control set, the DRM enabled work comes with the control set embedded into the work. This can be done by encapsulating the control set and the work in a security envelope [22]. In an external control set, the DRM enabled work and the control sets arrive separately. The obvious advantage of a system of this nature is that a single control set can be used to define rights for multiple works of the same type. On the other hand, external control sets are usually held on a network server and are required to be accessed each time a DRM work is accessed [23], allowing for strong right holder control. Both of these systems can be further combined with a fixed control set. Many of the current DRM systems use one of these two systems; the Apple iTunes Music Store for example uses an embedded control set (Apple Fairplay) on the music combined with a basic fixed control set in the iTunes music player. On the other hand, Microsoft recommends the use of a combination of embedded and external control set system for distributing music and movies with the DRM enabled Windows Media Player 9 and WMA and WMV media formats [19].

3.1.3 Distribution process

The third and final level of distinction is in the distribution process. Park et al. differentiated between *message push* and *external repository* [22]. In a message push system, the data is transfered between the sender and recipient by a direct communication channel such as e-mail. In an external repository, the recipient fetches the data from a central repository and there is no need for the recipient to store the data locally. Both systems have their uses in DRM systems, and the choice of distribution system does not necessarily impact on the security of the data. Message push systems are useful in enterprises where the data is only meant to be available to specific employees. Message push also has a greater flexibility in managing individual right permissions. External repositories are useful for a wider range of deployment, where the prospective user is unknown, and can also be used in systems where the user cannot store the data permanently onto their own systems. This type of DRM allows the right holder a high degree of control in how the user accesses and uses the data.

3.1.4 Characteristics of the Security Architectures

Park et al. also looked at some of the characteristics of the security architectures described above. In these characteristics, they did not take into account any restrictions imposed by other elements in a DRM system such as the REL. Table 1 looks at some of the characteristics of the different distribution systems. These characteristics are a combination of features and characteristics proposed by Park et al. [22] and Mulligan et al. [21]. Some of the suggestions need to be finely balanced in a DRM system, for example the ability to track usage and access is liked by right holders but invades user privacy. Architectures not utilising a VM (NC1 and NC2) are not considered as they are not suitable for DRM systems.

Characteristics	**FC1**	**FC2**	**EC1**	**EC2**	**XC1**	**XC2**
Right Holder can control access and usage	Y	Y	Y	Y	Y	Y
Right Holder can change the access rights after distribution	N	N	N	Y	Y	Y
Right Holder can change the usage rights after distribution	N	N	N	N	Y	Y
Provides persistent protection	Y	Y	Y	Y	Y	Y
Virtual Machine is vulnerable to attack	Y	Y	Y	Y	Y	Y
Allows right holder to track usage and access	N	Y	N	Y	Y	Y
Allows for re-use of the digital container[3]	N	N	N	N	Y	Y
Users are allowed to access DRM protected data offline	Y	N	Y	N	N	N
Users can access data from any location or machine (without carrying the data themselves)	N	Y	N	Y	N	Y
Architecture allows for transfer of rights without third parties	N	N	N	N	Y	Y
Architecture allows for transfer of rights through a trusted third party	N	N	Y	Y	Y	Y

Table 1: Characteristics of DRM Distribution Architectures

[3] The user is allowed to distribute the DRM protected data him/her-self and the other users are allowed to access the data after getting their own licenses

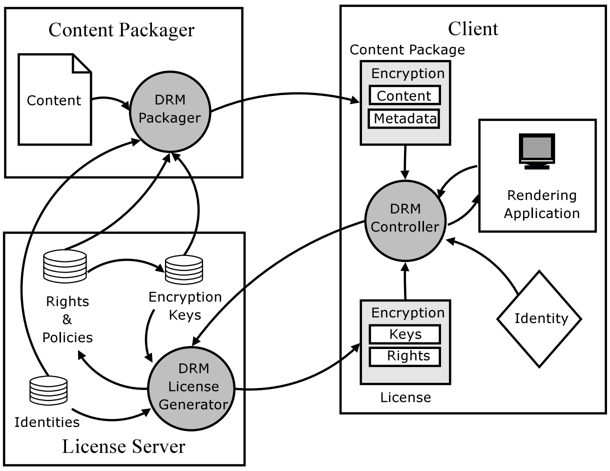

Figure 3: Using DRM enabled works [23]

3.2 Using DRM Enabled Works

In section 2.1, we described the different players in a DRM system as discussed by Bartolini et al. The players described could fall into three categories - the right holders and authors, the distributors and trusted third parties. We also suggested the addition of a new player - the user, which was left out by Bartolini et al. The DRM security architectures (figure 2) describe how the content can be communicated from the right holder (and/or authors) to the user.

Figure 3 shows how Rosenblatt [23] and Erickson [15] describe the usage of DRM enabled works in most of the current systems. Current systems usually use a combination of embedded and external rights control (i.e. the XC1, XC2, EC1 and EC2 distribution architectures described by Park et al.) and make use of a license server that creates a license to access the work based on the rights. First the content is packaged with a set of rights and distributed to the user. When the user requests the use of the protected work, the DRM controller validates the rights and issues a license to use the work depending on the rights. The application is then able to access the DRM protected work in accordance to the rules set out by the license. Identity control is achieved by using an identity register that can uniquely identify the client and different DRM solutions use different techniques to achieve this.

3.3 Types of DRM Controllers

The DRM controller in Rosenblatt and Erickson's models are equivalent to the VM proposed by Park et al, with a subtle difference. Park et al. defined the virtual machine as "software that runs on top of vulnerable computing environment" [22]. Rosenblatt however argues that DRM controllers can be placed at the hardware level (e.g. enhancing the BIOS of a desktop PC) or as an operating system module in addition to being a VM for a specific application [23].

Most current DRM systems, like Apple iTunes, use software virtual machines for DRM controllers. Application level DRM controllers have the advantage of having the capability of tailoring the DRM to suit the needs of the application. However there are two key disadvantages to application level DRM controls. Firstly, application level DRM control is hard to generalise, and this has led to the development of multiple incompatible solutions for the same application [23]. Furthermore, the development of DRM control becomes harder as each application has different designs and frameworks which need to be controlled. The second disadvantage is that application level DRM cannot guarantee right control of the protected work from operating system commands like "Print Screen" or the copy shortcut "Control C".

Microsoft Right Management Services (RMS) is the best example of an operating systems level DRM system. A RMS system comprises of three parts: the client side DRM controller, the software development kit to develop DRM enabled applications and a server module (for Windows 2003 Server) for administering DRM enabled works. The RMS client module enforces rights requested by RMS enabled applications and is available for all Microsoft Windows 98SE and later versions of Microsoft's operating systems. Applications are developed using the RMS SDK which allows the developers to handle rights associated with the works. Because RMS is an operating systems based module, the right management is more wholistic and can prevent system commands like "print screen" from executing. However RMS is not yet a complete solution, and is targeted only as an intra-enterprise solution.

Rosenblatt believes that hardware level DRM controllers are the long term solution [23]. However hardware level DRM controllers do not have a good reputation and the copy control mechanism in DVD is the prime example. However the main failure of DVD-CSS was the use of a flawed encryption algorithm and that the hardware control could not be upgraded by using a firmware [21]. Rosenblatt believes that overcoming these problems is easy and once the full specifications of a hardware DRM control mechanism is standardised, it will be only a matter of time before it is implemented.

3.4 Right Expression Languages

Right expression languages (RELs) are used to define the rights and conditions for a DRM enabled work that the right holder gives to the user. RELs are usually modelled on access control languages [20], and usually take the form of:

```
              has the                          to do
USER -----------------> RIGHT  -----------------> ACTION
```

on the object being protected. This can be further enhanced by including parameters that restrict (or maybe enhance) the right. The most common parameter is "time" which can be used to make the right expire automatically. In the XrML 2.0 specifications [2] the requirements for a REL are given as:

- *Comprehensive*: A language that shall be capable of expressing simple and complex rights in any stage in a workflow, lifecycle or business model.
- *Generic*: A language shall be capable of describing rights for any type of digital content or service (an ebook, a file system, a video or a piece of software)
- *Precise*: a language shall communicate precise meaning to all players in the system.

One of the most common RELs is eXtended Rights Markup Language (XrML). which was developed originally at Xerox Parc labs and is now developed jointly by Microsoft and Xerox. XrML is an XML based REL, and its syntax is specified by XML while its grammar is defined by XML schema definitions [2]. The XrML 2.0 specifications are split into three parts: a core schema, a standard extension schema to handle definitions that are broadly applicable but not a core feature, and a content specific extension schema to handle concepts specific to the type of digital content.

In an XrML license, the issuer grants a set of principals a set of rights, under certain conditions, over a set of resources. While the resources are usually digital files, XrML not only provides mechanisms to include non digital objects such as a "a computer terminal" but also services and transactions.

XrML is used in all Microsoft DRM solutions including RMS as well as being the base of other RELs. However, there have been many critisicms of current REL implementations for not being able to handle all the legal requirements when enforcing copyright [20, 16]. Mulligan et al. argues that RELs like XrML cannot be considered comprehensive until users are able to request additional rights [20]. They argue that this ability is crucial for the enabling of fair use. Bechtold however argues that many of the XrML rules and definitions like rights transfers are not implemented in current DRM systems [9] and thus the failure of DRM systems to have fair use is not hampered by the language. Bechtold maintains that a suite of programs that can implement all the rules and definitions available in XrML will be able to achieve most of the requirements of DRM systems with less compromise from right holders [9]. This would require users to communicate with the right holder to request additional rights or changes in rights, as argued by Mulligan et al.

3.5 Protection, Management and Tracking

The broader definition of DRM systems include tools that enable the right holder to manage and track the protected work. Protection itself can come in various forms. Most DRM enabled media come in a secure envelope consisting of the encrypted work and its signature. Multimedia vendors are also looking at embedding watermarks to identify the right holders of the digital work [12]. New techniques in fingerprinting enable identification for text and even database tables [26, 18].

Uzuner et al. proposes the usage of tracking mechanisms to completely replace DRM systems that exist solely to enforce copyright (like online music distributions) [26]. In such a system, every time a copy of the copyrighted work is distributed, an Internet Service Provider (ISP) can keep record of the transaction and then the users can be charged at the end of the month. However, such a system has three key flaws. Firstly, this system will create a logistical nightmare for ISPs and it will also require every ISP to implement such a tracking system. Secondly, users sitting behind firewalls and proxies will only get a consolidated bill and additional detectors will be required to detect the actual users of the work. And finally, if the users distribute works via secure encrypted channels, it is highly unlikely that the content of the channel will be divulged and analysed.

4 CURRENT DRM SYSTEMS

In this section we compare 3 types of popular DRM systems. The first system is the 99 cent music store as characterised by Apple iTunes. Of all the DRM systems, the Apple iTunes Music Store has been the most successful commercially and is currently the dominant player in the online music stores. The second system is the DRM system of the subscription music stores like Real’s Rhapsody, while the third system is Microsoft’s Rights Management Service. For a technical report providing further elaboration on these systems, the reader is referred to [7].

In section 2.5 we looked at the legal requirements for DRM systems, while in section 3.1.4 we looked at the characteristics of the distribution architectures. In table 2 R01 – R04 are the legal rights that users are granted by current fair law standards, while R05 – R08 represents the legal rights for the right holders. C01 – C11 represents the characteristics of the DRM systems and are the same characteristics discussed in section 3.1.4.

The following points discuss some of the characteristics of the systems in more detail:

- R01: Except for allowing for excerption from the audio files and the ability to transfer ownership, the music stores allow for almost all other fair uses. RMS allows for the same range of freedoms but subscription music stores are currently unable to offer most fair use scenarios.
- R02: RMS logs all user activity and currently there is no mechanism to stop monitoring of user activity. Similarly, subscription music stores monitor usage, and Mulligan et al. contends that

	Characteristics / Requirements	**99c Stores**	**Subscription Stores**	**RMS**
R01	Can handle most fair use scenarios	Y	N	Y
R02	Promotes user privacy, and does not monitor usage of DRM data	Y	N	N
R03	Allows for the transfer of rights	N	N	N
R04	Allows for flexibility in rights implementations	N	N	Y
R05	Can keep track of / detect illegal use of DRM enabled media	N	Y	Y
R06	Can correctly collect revenue from the usage of works	Y	Y	n/a
R07	Creates a secure distribution channel	Y	Y	Y
R08	Prevents the illegal use of protected works	Y	Y	Y
C01	Right holders control access and usage	Y	Y	Y
C02	Right holders can change the access rights after distribution	N	Y	Y
C03	Right holders can change the usage rights after distribution	N	N	N
C04	Provides persistent protection	Y	Y	Y
C05	Virtual machine is vulnerable to attack	Y	Y	Y
C06	Allows right holder to track usage and access	N	Y	Y
C07	Allows for re-use of the digital container	N	N	N
C08	Users are allowed to access DRM protected data offline	Y	N	limited
C09	Users can access data from any location or machine (without carrying the data themselves)	N	Y	Y
C10	DRM system allows for the transfer of rights	N	N	N
C11	DRM system allows for the transfer of rights through a trusted third party	possible	N	possible

Table 2: Comparisons of different DRM systems

some go further and actually have the ability to monitor other user activities like web browsing habits [21].

- R04: Although none of the systems have feedback mechanisms, RMS is the only system that allows a wide variety in rights configurations.
- R05: Because the 99c music stores have no tracking mechanisms, they cannot detect the illegal usage of their media.
- C02: In RMS, the right holder can invalidate the user's license and thus can change the access rights after distribution. Similarly subscription music stores can deregister a user and the user will no longer be able to listen to the music he/she downloaded.
- C03: RMS does allow the invalidation of use licenses, but cannot remotely change the license conditions.
- C05: There is no known VM vulnerability in any of the DRM systems discussed, but there is no guarantee that they are invulnerable.

- C06: The 99c Music stores do not use any logging or tracking mechanisms.
- C07: Because of this characteristic, none of the systems allow for transfer of ownership.
- C08: RMS needs at least one connection to get a use license. Subscription music stores do not allow offline access.
- C09: Assumes that the machine itself is a trusted entity, or that the user can register the machine as a trusted entity.
- C11: PlayFair[4] allows the DRM to be stripped away from an iTunes Store file. Therefore it can be employed in reverse to re-encrypt the file with the key for a different user, thus creating a rights transfer. In RMS, the administrator can invalidate the user's license, and can change the rights of the file.

5 CONCLUSIONS

This paper gave a broad overview on what constitutes a DRM system, looking at both the legal and technical requirements. Technically, it is very difficult to implement fair use as required by copyright legislation and none of the current DRM systems implement all the fair use requirements. However, systems such as Fairplay used in Apple's iTunes Music Store, have managed to strike quite a good balance between users' expectations and providing sufficient protection to right holders.

Microsoft's RMS has the potential to become the standard for enforcing rights management; it provides flexibility in allowing for both weak DRM control as needed for consumer services and for strong DRM control as required for protecting enterprise documents. RMS also has the potential for use in enforcing shrink-wrap licenses and a general mechanism in enforcing digital contracts. However, much of these applications cannot be enforced unless RMS creates a new mechanism for user authentication, since the current mechanisms are either too restrictive or have too many security problems.

One of the key challenges in rights management remains the ability to transfer rights between two parties. Although XrML supports the right to transfer, there are no mechanisms to do so. XrML also lacks the ability to allow for bi-directional communication where the user asks the right holder for a right. This ability is required if fair use is to be properly implemented.

Rights management technologies are here to stay and future systems will need to include DRM systems to either meet legislative requirements or to satisfy publishers' and consumers' demands. The RMS platform is the first step in such a direction but open standards are required to enable protection seamlessly across different operating systems and devices.

6 ACKNOWLEDEGEMENTS

This work is supported through grants from the UCT Council and the KW Johnstone scholarships. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not neccessasrily reflect the views of UCT or the trustees of the UCT Council and KW Johnstone scholarships.

[4] For more information on PlayFair the reader is directed to the discussions on Slashdot [6].

REFERENCES

[1] Copyright act 98 of 1978. 2000 ed., vol. 2 of *Statutes of South Africa*. Juta, 2001, pp. 2–214–2–234.

[2] *eXtensible rights Markup Language (XrML) 2.0 Specification*, 2001.

[3] DRM from the viewpoint of the electronic industry. *Slashdot* (2003).
URL: http://slashdot.org/article.pl?sid=03/11/25/1821218&mode=thread&tid=126&tid=141&tid=188.

[4] Windows rights management services: Protecting electronic content in financial, healthcare, government and legal organizations, 2003.
URL: http://www.microsoft.com/windowsserver2003/techinfo/overview/rmsverticals.mspx.

[5] Linux and DRM? *Slashdot* (2004).
URL: http://ask.slashdot.org/article.pl?sid=04/02/10/2329229&mode=thread.

[6] Playfair relocates to india. *Slashdot* (2004).
URL: http://slashdot.org/article.pl?sid=04/04/13/1156258.

[7] ARNAB, A., AND HUTCHISON, A. Digital rights management — a current review. Departmental technical report, no. cs04-04-00, University of Cape Town, 2004.
URL: http://pubs.cs.uct.ac.za/archive/00000114/.

[8] BARTOLINI, F., CAPPELLINI, PIVA, A., FRINGUELLI, A., AND M, B. Electronic copyright management systems: Requirements, players and technologies. In *Proceedings of the Tenth International Workshop on Database and Expert Systems Applications* (1999), IEEE, pp. 896–899.

[9] BECHTOLD, S. Digital rights management in the united states and europe. IVir, Buma/Stemra - Copyright and the Music Industry: Digital Dilemmas.

[10] BECHTOLD, S. Reconciling DRM technology with copyright limitations. IVir, Buma/Stemra - Copyright and the Music Industry: Digital Dilemmas.

[11] BRIDGES, A. Contributory infringement liability in recent us peer-to-peer copyright cases. IVir, Buma/Stemra - Copyright and the Music Industry: Digital Dilemmas.

[12] BYERS, S., CRANOR, L., KORMAN, D., MCDANIEL, P., AND CRONIN, E. Analysy if security vulnerabilities in the movie production and distribution process. In *Proceedings of the 2003 ACM Workshop on Digital Rights Management* (2003), ACM, pp. 1–12.
URL: http://doi.acm.org/10.1145/947380.947383.

[13] COHEN, J. DRM and privacy. *Communications of the ACM 46*, 4 (2003), 47–49.

[14] DUSOLLIER, S. Fair use by design in the european copyright directive of 2001. *Communications of the ACM 46*, 4 (2003), 51–55.

[15] ERICKSON, J. Fair use, DRM and trusted computing. *Communications of the ACM 46*, 4 (2003), 34–39.

[16] FELTEN, E. Skeptical view of DRM and fair use. *Communications of the ACM 46*, 4 (2003), 57–59.

[17] GROVE, J. Legal and technological efforts to lock up contenet threaten innovation. *Communications of the ACM 46*, 4 (2003), 21–22.

[18] LI, Y., SWARUP, V., AND JAJODIA, S. Constructing a virtual primary key for fingerprinting relational data. In *Proceedings of the 2003 ACM Workshop on Digital Rights Management* (2003), ACM, pp. 133–141.
URL: http://doi.acm.org/10.1145/947380.947398.

[19] MICROSOFT. Microsoft windows media data session toolkit, 2003.

[20] MULLIGAN, D., AND BURSTEIN, A. Implementing copyright limitations in right expression languages. In *Proceedings of the 2002 ACM workshop on Digital Rights Management* (2002), ACM.

[21] MULLIGAN, D., HAN, J., AND BURSTEIN, A. How DRM based content delivery systems disrupt expectations of ”personal use”. In *Proceedings of the 2003 ACM workshop on Digital Rights Management* (2003), ACM, pp. 77–89.
URL: http://doi.acm.org/10.1145/947380.947391.

[22] PARK, J., SANDHU, R., AND SCHIFALACQUA, J. Security architectures for controlled digital information dissemination. In *Proceedings of the 16th Annual Computer Security Applications Conference* (2000).

[23] ROSENBLATT, B. DRM for the enterprise, 2004.

[24] ROSENBLATT, B., AND DYKSTRA, G. Integrating content management with digital rights management - imperatives and opportunities for digital content lifecycles. White paper, Giantsteps Media Technology Strategies, 2003.
URL: http://www.giantstepsmts.com/drm-cm_white_paper.htm.

[25] SAMUELSON, P. DRM {AND, OR, VS.} the law. *Communications of the ACM 46*, 4 (2003), 41–45.

[26] UZUNER, O., AND DAVIES, R. Content and expression-based copy recognition for intellectual property protection. In *Proceedings of the 2003 ACM Workshop on Digital Rights Management* (2003), ACM, pp. 103–110.
URL: http://doi.acm.org/10.1145/947380.947393.

[27] WIPO. Berne convention for the protection of literary and artistic works.
URL: http://www.wipo.int/clea/docs/en/wo/wo001en.htm.