Alapan Arnab and Andrew Hutchison
Data Network Architectures Group
Department of Computer Science
University of Cape Town
Rondebosch, 7701
South Africa
{aarnab, hutch}@cs.uct.ac.za

AN EVALUATION FRAMEWORK FOR DRM

Abstract: There have been numerous evaluations of DRM systems, and most of these evaluations have focused on the end user experience of DRM systems. However, some of the problems identified by these evaluations are not simply a result of business strategies by the various vendors, but caused by the underlying deficiencies in the DRM architectures themselves. For this reason, in addition to evaluating the user experience, there is a need to evaluate each DRM system as a software system.

In this paper, we present 27 requirements, divided into three categories, drawn up from a number of different sources (from consumer requirements to DRM standardisation programmes) to create an evaluation framework for DRM. We then benchmark four different DRM systems (two media systems, two enterprise systems) against this framework, and identify some of the universal problems in current DRM systems. In our analysis, we find 4 major flaws with current DRM systems: the lack of user authentication, lack of device and platform portability due to the reliance of device based authentication, poor support for revocation and modification of access rights and a poor understanding of legal and social requirements from the developers of the DRM systems.

Keywords: DRM, iTunes, Windows Media, Microsoft RMS, Adobe Document Security, DRM Requirements, DRM architectures

1. Introduction

There have been a number of articles (in academia such as [42], in the press and in blogs) evaluating different DRM systems. All these evaluations focus on the effects of the DRM system on the end user. Thus, these evaluations do not consider whether the system manages to block unauthorised uses, but rather how many devices the user can use to render protected content. As far as we know, there have been no *technical* evaluations of DRM systems.

There are two primary motivations behind technical evaluations of DRM systems. Firstly, such an evaluation can potentially reveal the architecture of the

system, and thus explain some of the user experiences associated with such a DRM system. For example, Apple Inc.'s reluctance to license their DRM standard to rival manufacturers could be explained by the integration of the DRM architecture in the complete system, and thus may not simply be a reluctance to license the file formats.

Secondly, an evaluation framework allows developers of existing and future systems to address the various gaps in existing systems. This is also a necessary step in any standardisation process. In this paper, we present an evaluation framework for DRM systems, drawing on requirements from a number of different sources (discussed in section 2). Our evaluation framework defines 27 requirements that need to be addressed by both enterprise and media DRM systems. We then use our evaluation framework to examine four different existing DRM systems.

2. Sources for Requirements

We have examined a number of different sources to draw up the requirements discussed in this paper. In [18], Bartolini et al. were one of the first to discuss requirements for content protection systems, and they were also one of the first to discus the parties involved in a DRM value chain. In [43], Park et al. discuss different taxonomies for content protection systems and a few technical requirements for DRM.

There are a number of different organisations that have released comprehensive technical requirements for DRM. The requirements by Networked Audiovisual Systems and Home Platforms (NAVSHP) [8], the Digital Media Project (DMP) [10] and the TIRAMISU project [32] are quite comprehensive, but all focus specifically on media DRM systems. The requirements documents, especially from the DMP have gone through many iterations and refinements, and differ drastically from their initial versions [49].

Unfortunately, technical requirements rarely acknowledge legal or social requirements for DRM systems; and when they do specify such requirements, they are often vague and even contradictory. For example, conflicting needs specified by the TIRAMISU project are the need for detailed tracking and monitoring of content usage information and the need for user privacy. We have drawn our requirements for social and legal requirements from two main sources: Mulligan et al.'s evaluation of media DRM systems on the infringement of "personal use" in [42] and the Center for Democracy & Technology's criteria for evaluating media DRM in [12].

There are two independent surveys that have investigated the respondents' usage patterns for physical media, their habits and attitudes concerning digital piracy as well as their attitude to DRM and other content protection

mechanisms. The INDICARE project [26] was a comprehensive survey on European users, while Arnab and Hutchison's survey in [16] investigated the relationships between the physical and digital media usage patterns. Some of our requirements are motivated by the results of these surveys.

An additional source for requirements can be found in feature descriptions of enterprise DRM systems, particularly when they describe certain use cases. In most cases, these features are already covered in the other sources mentioned above, but the use cases often bring a unique perspective on the requirements. These documents include systems from Adobe [9], Authentica [17] and Microsoft [38].

3. Requirements

We have categorised the requirements for DRM systems into three categories: core requirements for access control, usability requirements and legal and social requirements.

3.1 Core Requirements for Access Control

DRM is a form of access control, and thus every DRM system need to implement features that allow for access control. For any protected resource, access should only be granted if the consumer fulfils all the defined requirements associated with that resource. Should the resource be moved to a device which cannot interpret and enforce the access control policies, no access should be given.

> **Requirement 1: Provide Persistent Protection:** Access to the resource should only be granted when the consumer fulfils all the requirements set out by the access control policies. Furthermore, the resource should not be accessible if the device cannot interpret or enforce the access control policies.

Access control is inherently a two part process – there is an authentication process, and once the parties have been authenticated, there is an authorisation process – i.e. is the person who they claim to be, and is that person allowed access to that resource. The user in a DRM system is not necessarily the end user, but includes any person (natural or legal) involved in a DRM system, such as the rights holder or a third party processing payment.

> **Requirement 2: Represent User Identity:** Before a user can be authenticated, the user must be identified. The user identity has to be globally unique, since DRM protection has to be applied globally. User identity is often closely associated with authentication protocols, and thus;

Requirement 3: Support multiple User Authentication Protocols: Authentication proves the validity of a claimed identity. Since there are already a number of existing secure authentication protocols, it is easier to accommodate these protocols than to create new authentication protocols.

The user is not the only party in a DRM transaction. Because DRM aims to control the use of content, there is a need to identify and authenticate data content as well as the devices which wish to render the content.

Requirement 4: Represent and Authenticate Resource Identity: To control access to a resource, the resource first needs to be identified in a globally unique scheme. Once a resource can be identified, there is also a need to verify the correctness of the association between the resource and its identity.

Requirement 5: Represent and Authenticate Device Identity: To confine access to a resource to a particular device, there needs to be a mechanism to define the identity of the device. Once a device has been identified, there is a need to verify the correctness of the association between the device and its identity.

While access control can be defined for an individual user, resource and device, it is also useful to control access through defined groups of users, resources and devices. For example, it could be useful to define location domain, such as a department in an enterprise, where data can be accessed. Furthermore, access control can also be defined though the function of the user in an organisation [27](or society) and this functionality should also be catered for in DRM.

Requirement 6: Represent and Authenticate User Groups: There is a need to control access to data to a defined group of users, and there should be a mechanism to define and authenticate such a grouping.

Requirement 7: Represent and Authenticate User Roles: There is a need to control access to data through a definition of the functionality/role played by the user in an organisation. There should be a mechanism to define and authenticate that the user belongs to the defined role.

Requirement 8: Represent and Authenticate Resource Groups: There is a need to control access to data to a defined group of resources, and there should be a mechanism to define and authenticate such a grouping.

Requirement 9: Represent and Authenticate Device Groups: There is a need to control access to data to a defined group of devices, and there should be a mechanism to define and authenticate such a grouping.

The above requirements are all involved in authenticating the parties involved in a DRM transaction. Once the parties are authenticated, authorisation for the parties is required.

Requirement 10: Represent the Authorisation (Use License): There is a need to define the authorisation for an individual person, group or role

to access one or more resources on one or a group of devices. The data unit that provides such an authorisation is hereby referred to as a ***use license***

Requirement 11: Authenticate the Use License: There is also a need to ensure that the authorisation is created by the appropriate party (the rights holders or one of their representative), as well as the integrity and correctness of the use license.

Requirement 12: Support User Duties: Consumers may be required to perform certain actions before they are authorised access. For example, in a media DRM setting; the resource may have a limited free evaluation stage (e.g. shareware) and then the consumer is required to pay for further usage. Thus, the consumer would need to show proof of payment before getting authorisation for use. This scenario is not restricted to the media DRM scenario, and may also be required in an enterprise scenario; for example, a consumer may only be granted access to an application, once (s)he has passed the training for that application.

Requirement 13: Revocation of Rights: Access control rights may need to be revoked for a number of reasons such as the consumer violating the terms of the agreement or the consumer getting a different use license for the same work. Thus, there needs to be an efficient mechanism to revoke access control rights; but at the same time revocation has to be controlled in a fair manner.

Requirement 14: Update of Rights: Access control rights may need to be changed for a number of reasons such as the consumer acquiring an extension of the agreement beyond the stated period. Thus, there needs to be an efficient mechanism to update access control rights; but at the same time updates have to be controlled in a fair manner.

We contend that the requirements discussed above constitute the core requirements for any DRM system, and define the minimum requirements for persistent access control. However, there are other requirements for general DRM systems which we are going to discuss in the remainder of this section.

3.2 Usability Requirements

There are a group of requirements that, though not strictly required to provide access control, are very desirable for a DRM system. These requirements, such as portability, are demanded from the users (producers and consumers) of the system and can be termed essential features required for a DRM system, and systems that have these features are likely to have more success and attract less criticism.

Chief amongst this group of requirements is portability, and the lack of support for portability in DRM systems has attracted the most criticism in DRM

systems in academia [42], consumer groups [12][26], public comment [3] and the media [20, 11]. Mulligan et al. defined portability as:

> *the ability to use acquired content on any suitable device, regardless of ownership in the device or its physical surroundings. Portability also refers to the ability to shift the format of a copy. [42]*

We believe that portability can be distinguished into four different categories, and each category can be seen as an individual requirement for any DRM system; although the importance of the requirements can vary between different applications of DRM.

Requirement 15: Time Shifting: Time shifting refers to the ability of the DRM systems to regulate when the consumer accesses a protected work. In the media DRM space, time shifting could be used to rent works to consumers for limited time periods (similar to a movie rental or library). In the enterprise, access of corporate infrastructure at "odd hours" is already used in intrusion detection and other security infrastructure and time shifting restrictions in DRM could be used in a similar vein.

Requirement 16: Format Shifting: Format shifting refers to the ability of the DRM systems to regulate the consumer's ability to change the format of the data file (without affecting the access control rules), and Mulligan et al. argued that it is an important portability issue in media DRM systems [42]. Format shifting could be important in an enterprise for similar reasons – for example, the enterprise could keep internal data stored in a certain format and in a different format when released to other companies or even to the public (in the case of financial statements for example). Format shifting should also allow for easier integration between different applications across different platforms.

Requirement 17: Space Shifting: Space shifting refers to the ability of the DRM systems to regulate which devices the consumer can use to access the protected resource. Space shifting operates within the same type of device and operating system.

Requirement 18: Platform Shifting: Platform shifting refers to the availability of a DRM system across multiple devices and operating systems. In a world with multiple types of convergent devices, users can expect to access protected resources on mobile phones, portable computers, desktop computers and hand-held computers to name a few. Each of these devices also supports a number of different operating systems, sometimes from the same vendor. Thus, platform shifting refers to the DRM systems ability to support multiple operating systems and devices.

For portability, DRM systems need to be able to support the regulation of time shifting, format shifting and space shifting while implementations of DRM systems need to support the implementation of platform shifting. There are

requirements other than portability which can be grouped under usability requirements, and we discuss them next.

Requirement 19: Integration with Existing Applications: Current DRM systems introduce their own applications in order to enforce the access control policies. This strategy is however not feasible in the long term: in the media DRM space, consumers want the choice for which applications they want to use, because of familiarity or features provided by these applications. Similarly, enterprises often use software developed for their specific needs and resources that need to be protected are not necessarily generated by applications supplied by current vendors of DRM systems.

Requirement 20: Delegation of Rights: At least one user has to have the right to delegate rights to other users (e.g. an author has to be able to delegate the right to view to a reader); but there is a need to control delegation of rights. We are however interested in delegation of rights after the initial delegation, and if possible, all aspects of delegation must be possible. Delegation of rights could also include the transfer of rights (either temporary or permanent) between consumers of a work. A permanent transfer of rights can effectively be seen as a revocation followed by a granting of rights, without the rights holder exerting additional payment (or other duties).

Requirement 21: Fine Grained and Flexible Access Control Specification: The use cases for DRM systems in general demand fine grained access control – not just control on the traditional read, write and execute but also application specific controls. Furthermore, restrictions on specific controls would also be preferred. Because of the variety of use cases for DRM, there is also a need to create flexible access control specification, with the definition of the controls differing according to the use cases.

Requirement 22: Tracking and Monitoring: Although not a feature of DRM itself, monitoring the access and usage patterns of users (both consumers and producers) can be easily achieved. In an enterprise, monitoring the usage of confidential data is crucial, and should compromises to security take place, access logs and usage patterns would be very useful in tracking down the source of the compromise.

However, with the ability to track and monitor usage, privacy does become a concern. Monitoring employee activity in the workplace is already a contentious issue, while monitoring consumers in media DRM systems could be illegal in some countries, and already attracts criticism in academia [42] and the public [3]. Thus, the ability to track and monitor usage is only desired in certain applications of DRM, and care needs to be taken to stay within the boundaries of appropriate monitoring.

Requirement 23: Offline Usage: Communication networks are not perfect, and there are many situations where consumers (or even producers) may not have access to the Internet (for example on an aeroplane), or may need to access resources on devices which have no connectivity (such as the current generation of Apple iPods). Thus offline usage is desirable; but does have its drawbacks – offline usage reduces monitoring and tracking capabilities; and may also limit the control desired. For example in an enterprise, if an employee is fired and the employee has protected data that can be accessed offline, the employee could still retain access to the protected data. Generally, online usage could be required periodically but not necessarily all the time for operation

3.3 Legal and Social Requirements

Ultimately, transactions regulated in a DRM system are governed by applicable laws. When disputes do occur, the only fair solution to the disputes can be found through arbitration or the courts. However, current DRM systems (and arguably most computer systems) do not consider the legal implications of the services they provide; nor do they have clearly identifiable legal frameworks under which they operate.

Requirement 24: A Legal Framework for DRM: There is a need to identify and position DRM systems, and the transactions in a DRM system, in a comprehensive legal framework. The legal framework should address concerns relating to copyright law and fair use and personal uses such as portability and archiving.

Consumer organisations have also commented on some of the requirements for media DRM systems with respect to features consumers expect from DRM systems. Some of these requirements can be addressed as part of a legal framework, while other requirements do not necessarily have any legal backing. These requirements also apply (although at times, to a lesser degree) to enterprise DRM systems.

Requirement 25: Transparency: DRM systems should clearly disclose the restrictions imposed. The restrictions should be available to the user before the resource is acquired, and the user should also have the means to view the restrictions during use. Furthermore, the restrictions should be clearly stated and documented, and not hidden away in complex agreements and user agreements.

Requirement 26: Privacy and Anonymity: The requirement for privacy and anonymity, goes against a previously stated requirement for monitoring and tracking. While both can co-exist in the same system, a system that provides tracking and monitoring cannot claim to provide complete user privacy and vice versa. However, some parts of both are

required for generalised DRM systems, and the range of the features implemented will depend on the exact application.

If monitoring and tracking are implemented, the user must be informed of what data is being collected, how the collected data is going to be used, who will have access to the collected data and how long the collected data will be stored.

Requirement 27: Do Not Alter Platform Functionality and Performance: Implementation of a DRM system should not drastically alter the functionality or performance of the whole system for non-protected works. This includes the introduction of security loopholes through the DRM system, or the need for additional software or hardware to regain functionality or performance.

4. Evaluation of Existing Systems

In this section we evaluate 4 existing DRM systems against the requirements we discussed in the earlier section. For each system, we give an overview of the players involved in the system, how protected files are assembled and how access controls are enforced. For the requirement analysis, we use a simple 3 point rating system for each requirement, defined below. The ratings are then used to compare different systems, and identify which requirements are least satisfied by current DRM systems.

0 : The requirement is not supported at all.
1 : There is limited support for the requirement.
2 : The requirement is supported in full.

The requirement analysis is done with respect to the DRM system itself and what is possible with the DRM system, and not what is expected by consumers or consumer organisations. Certain requirements could be considered fully met in design but have no support in implementations. In these cases, we often score the systems as limited support, especially if the decisions behind non-implementation are driven by the vendor's business model and practices; and not because of adequate market demand. Due to space constraints, we present only one consolidated table with our ratings in section 4.5.

4.1 Apple iTunes Music Store

In March 2003, Apple Computers debuted the Apple iTunes Music Store1 which allowed customers to download individual music tracks for 99 US cents, and whole albums for US $9.99. Within one year, iTunes Music Store had become the dominant online music store, selling over 50 million songs [23] and it currently commands the majority of legal online music downloads [28]. With

over 2 billion downloaded songs, 50 million TV episodes and 1.3 Million movie downloads, it can be considered to be the most successful DRM system [15].

Apple's iTunes Music Service is a proprietary system, and the details we present below are compiled from the user documentation provided by Apple [13], and from some well known compromises of the system – Playfair (subsequently renamed Hymn) [1][4][5] and PyMusique [51][47] and its successor SharpMusique [29].

4.1.1 Brief Overview

iTunes DRM system can be considered as a set of two services. Initially, iTunes started as a music player system for Apple Macintosh, and later became the interface between the Apple Macintosh and their portable music player, the iPod. iTunes (the software) has evolved to become a comprehensive media player, and is available on Microsoft Windows and Apple Mac OS operating systems. The second part of the system is the iTunes Music store, which sells music, audio books, movies and TV episodes. All media sold on the music store is protected by the Apple DRM system known as FairPlay, which is the focus of our discussion.

When a user first registers in the iTunes Music Store, a digital certificate, including a key, is generated for that machine. We believe that this certificate is signed by the iTunes Music Store. Currently, the user can register five machines in total, which would all carry the same digital certificate. It is possible to deregister the machine (thereby removing the key from the key store), but it is not possible to register beyond the maximum – even if those machines are no longer registered.

When protected data (currently music and video) is transferred to a portable device (currently only the Apple iPod is supported), the digital certificate associated with the data is also transferred. It is therefore possible to utilise data from different users on the portable device.

There are no other keys or digital certificates involved in the iTunes Music Service, and thus Apple manages to keep a very tight control over the chain of trust. However, the short chain (only two types of keys) introduces its own problems, primarily with regards to portability. Using the primary key (on the iTunes service) provides no user authentication; and thus any data that is protected with the key is accessible to every registered user. Thus, the iTunes service utilises the user key to protect content, requiring user authentication to access data. This means that portability between different users is not possible; a limitation which will affect every user who reaches their maximum limit on registered computers.

A flaw in the system, uncovered by PyMusique, is that the protection of content does not occur on the iTunes server; presumably because it would

require the iTunes service to keep track of all the keys. Instead, the protection is only applied once the data is downloaded to the registered computer. PyMusique and SharpMusique took advantage of this flaw, and interacted with the iTunes music server directly, but did not protect the data once it was downloaded.

In late 2006, the protocol used by iTunes to interact with iTunes Music Store changed, and SharpMusique no longer works [29]. Hymn (also known as PlayFair) is a more direct attack on the service, where the user's key is recovered from the portable device and used to decrypt the protected content. Once the data is decrypted, the user can do what they wish with the content.

4.1.2 Core Requirement Analysis

FairPlay cannot be considered a complete DRM system. Its primary protection relies on secure distribution, which has already been compromised. Furthermore, the user identity system is basic, and two different users cannot be accommodated on the same iTunes system directly (it is possible to cater for two different users if they use different user profiles on the consuming computer's operating system). Furthermore, even though Apple is introducing iTunes enabled media into other areas of the home through products such as Apple TV2, mechanisms to manage device or user groups do not exist. And even though music is sold as albums, songs are effectively treated as individual and not as a group of resources. This could be due to the fact that the system does not make use of any licensing structure. Revocation of rights is also poorly supported, and only allows the complete revocation of user's rights and not selective revocation. The rights profile can be updated (and have changed since the inception of the store), but requires an update to the iTunes software, and users who do not update their software do not get the updated rights profile.

4.1.3 Usability Requirement Analysis

Portability is often seen as a major consumer problem with DRM and FairPlay scores interesting ratings with respects to portability. FairPlay currently does not have any time shifting restrictions imposed on the user – once the user downloads a song or video clip, they can render it however often they wish. The subscription model, which requires time shifting is not supported in FairPlay, although rumours of such as a service have been reported by the media [22][31]. Since we do not have access to any internal documentation on FairPlay, we assume that Time Shifting is simply not supported, and future support will require an update of the iTunes service.

FairPlay is openly acknowledged as a DRM wrapper, thus there is no reason why multiple format types cannot be accommodated, or why format conversion

cannot be performed between these different formats. However, only two formats are currently implemented: AAC for audio and Quicktime Video for video. Likewise, limited platform portability is supported through the evidence of support for different operating systems and the iPod, but the support remains tightly controlled. Space shifting however is well supported.

Apart from Offline Usage, where FairPlay does not require any Internet connection other than for initial acquisition of media, other usability requirements are not catered for by FairPlay. iTunes does not support delegation of rights, and the lack of licensing structure means that there are no fine grained access controls. With the tight integration of iTunes software, other applications are ignored and the iTunes music store claims that it does not track or monitor usage of protected works.

4.1.4 Legal and Social Requirement Analysis

While it is well known that the iTunes Music store sells media to the general public, the exact legal position of the store is, at best unknown, and has attracted legal attacks in some countries like Norway [46], which would like to force portability of FairPlay beyond the iPod. If iTunes sells media under copyright law, then a number of functions allowed under copyright are not permitted and that means it can be considered as illegal. If it is under a licensing system, then do they fulfil the requirements necessary for concluding valid contracts? Thus, with an unclear and unknown legal position, it scores a 0 rating for the legal framework rating.

iTunes Music store is very transparent in identifying all the restrictions placed by iTunes, but does not provide much detail on how much personal data is collected (sales records etc) or if data is correlated to keep track of general trends. Apple does have a comprehensive privacy policy, and is easily available to all users [14], and thus our higher score. Finally, studies have shown that battery life of portable media players diminishes faster when playing DRM enabled media when compared to non DRM enabled media [30], but that is understandable considering the extra CPU operations required to render the media. Apple iPod had one of the lowest reported degradation in performance, and hence the full rating.

4.2 Microsoft Windows Media (WM)

Recent versions of Microsoft's Windows Media (WM) Audio and Windows Media Video were designed to compete with iTunes Music Store and thus feature DRM protection. Unlike Apple, Microsoft's initial strategy was to support multiple online music stores and multiple portable media players. But, even though the formats are supported by one vendor; different versions support different features and are often incompatible. Microsoft's first release, Windows

Media 9, did not support automatic time shifting expiry and was confined to online connectivity only [33]. This was solved in a subsequent release, “Play For Sure”. This is possibly the most widely used version, and is supported by many device manufacturers and online music stores. More recently, Microsoft released yet another specification, which is incompatible with “Play For Sure”, and geared towards its own portable device player, Zune [2][50]. With this strategy, it seems that Microsoft is trying to emulate Apple’s tight integration strategy.

In this section, we primarily discuss “Play For Sure”, although all three versions use a similar architecture. Like iTunes, Windows Media is a proprietary solution, although there is a lot more documentation available on its operation than iTunes’ operation. We use documentation released by Microsoft [37][41][34][35][45][36][44] and reports on the breaking of the protection (through a tool FairUse4WM) in [21] and the original details posted in [25] and an earlier attack using a tool DrmDbg [24].

4.2.1 Brief Overview

Unlike Apple, Microsoft has chosen not to control the distribution and licensing components of the DRM system. Furthermore, because the playback libraries can be licensed, theoretically, playback is possible in a wide range of platforms and devices.

One of the key features of the Microsoft approach is the default support for super distribution – it does not matter how the consumer acquires the media, but to access the media, the consumer will require a license. However, the licenses are non transferable, and usually tied to the device. This approach severely limits portability, as consumers cannot use multiple devices even if the consumer owns these devices.

Unlike iTunes, DRM protected media files are encrypted before distribution. The key to access these files are distributed through the use license. Licenses also carry a revocation list of consuming devices that should be refused access to the protected media. Because the licenses are locked to the consuming device, there is no need for user authentication. Unfortunately, neither the public documentation nor the break indicate conclusively whether the use license itself is encrypted.

The documentation does confirm that the use licenses are signed by the licensors. The licensors’ root certificates in turn have to be signed by Microsoft directly. This means, that while, Microsoft may not control the entire DRM value chain, they still control the chain of trust. This also means that Microsoft ultimately can decide which licensors to trust, and can refuse licensors a signed certificate, thereby refusing them access to utilise the Windows Media DRM system.

Like Hymn, FairUse4WM (based on an earlier attack DrmDbg) is a direct attack, extracting the key(s) from the licenses and then extracting the content from the protected package.

4.2.2 Core Requirement Analysis

Since protection offered by WM is not distribution dependent, it offers a more persistent access control protection. However, like iTunes FairPlay, there is no provision for individual user identity, and instead user identity is replaced by device identity. Also, like iTunes FairPlay, there is no provision to identify groups of devices, resources or users; and revocation of rights is tied to the device, and not individual rights or resources. Unlike iTunes FairPlay, WM does make use of use licenses and these use licenses are authenticated through the digital signature of the issuer. However, there does not seem to be any mechanism to verify the authenticity of the issuer (whether it is still trusted for example) or whether the license issuer can differ from the actual packager of the media (i.e. can an artist package the media him(her)self and then use music stores to market and sell licenses?). Rights can be updated through the issuing of a new license, but we are not aware of any media store that supports such a practice. Since current revocations are based on device rather than license, we are not sure if license revocation is possible.

4.2.3 Usability Requirement Analysis

Initially, WM was used exclusive in subscription business models, and thus time shifting was a key feature, although this initially required online connectivity. Like iTunes FairPlay, WMuses a wrapper and thus it potentially can support other media formats. However, no other implementations exist, and thus cannot be verified any further. Unlike Apple, Microsoft has been more liberal in allowing WM to be incorporated into other devices and platforms. However, the recent change with Zune, and because of the fact that Microsoft can still refuse to license to any vendor they wish, we have lowered the platform shifting scores. Since WM is based on a set of libraries, it is possible to render media on compatible software that makes use of the libraries, although not all applications may work. Because media licenses are device specific, space shifting is not possible under most schemes.

Even though WM does feature a licensing mechanism, the lack of individual users make fine grained access control difficult, and this difficulty is compounded by a relatively small set of access control primitives. Without user identification, delegation is also not possible. WM does support tracking and monitoring support, but the extent is not documented; and both “Play For Sure” and Zune versions support offline usage.

4.2.4 Legal and Social Requirement Analysis

As with Apple iTunes FairPlay, there is no legal certainty to the legal position of online media stores using WM. Furthermore, because individual media stores set their own privacy policies, and their own disclosure rules, we cannot rate these factors. With regard to performance and battery life, the reviews mentioned earlier found that WM enabled devices fared the worst, losing battery life up to 25% faster [30]. This is significantly higher than the iPod and thus our lower rating.

4.3 Microsoft Rights Management Services (RMS)

Microsoft's Rights Management Services (RMS) is a DRM system geared for the enterprise, and is the only DRM system we are aware of that has access control support in the operating system kernel. In this section, we examine the effectiveness of RMS as a general DRM system. RMS is also a proprietary solution, but like for Windows Media, there is a lot documentation released by Microsoft that can be used to examine the system [39][38][40]. We have also used Rosenblatt's comparative analysis of RMS and Authentica ARM [48] to confirm our own analysis. However, unlike WM and iTunes FairPlay, we do not know of any compromises that can reveal any additional information on RMS' operations.

4.3.1 Brief Overview

RMS can be used to protect any type of data, although its user authentication design has meant that it is used primarily for intra-enterprise use. Like Windows Media, RMS does not have any restrictions on distribution, but cannot really be super distributed. Although the use license is distributed separately, the restrictions on which user(s) (or user groups) can access the data is linked to the data itself. Thus, it is not possible for a user to acquire a license for the data, if they do not have preallocated access.

To use RMS in an enterprise, the enterprise must first set up an infrastructure of trusted entities. At the core of this set-up is a local certification authority that can create other trusted entities. For this purpose, RMS requires a server (running Windows Server 2003) to be enrolled as a trusted server. Like with Windows Media DRM, this server requires its public/private key pair to be signed by Microsoft directly, through its RMS Server Enrolment Server. Once this is done, the server can act as a certificate authority for the enterprise, and enrol other servers (license servers, active directory for authentication and other certificate authorities), client machines and users as certified entities. The local trust server does not need to be connected to the machines once they have been enrolled as trusted entities.

Client machines require the installation of a RMS operating system component (which enforces some of the license conditions) and RMS-aware applications which can interact with the RMS operating system component. RMS-aware applications can assemble and use protected data.

4.3.2 Core Requirement Analysis

UnlikeWindows Media, RMS does feature user identification through the use of Microsoft Active Directory or through Passport. Using Active Directory also allows the enterprise to regulate usage through the use of groups or roles. However, the use of Active Directory does mean that there is little scope for portability outside the enterprise, as any such measure would require the external systems to be within the trust realm and the user identities have to be integrated with the enterprise's Active Directory. Passport is not really a viable choice considering its poor security history [19]. More recent versions of RMS also allow for authentication through X.509 certificates, but the addition of other identification mechanisms during deployment is not possible. The trusted realms allow for device identification, but do not seem to cater for grouping devices under different security levels or categories.

RMS enabled data itself does not have versioning control by default, thus there is no way to distinguish between different versions of a document without opening the document. This has potential for problems if a user is allowed to access one version but excluded from the other version (for example the user is allowed to access version 1 but not version 2). If the use license is not forced to be renewed, then the user should be able to continue accessing both versions.

The use of dual licenses (an embedded license with the data, and an external use license), both of which are required, is puzzling; especially as it thwarts easier portability, rights revocation and renewal or extension of license terms. For example, update of rights is allowed, but requires the document to be repackaged with the new conditions and then redistributed to the recipient. Even with high speed networks, this can be impractical, especially considering the size of certain documents such as high resolution images or presentations.

4.3.3 Usability Requirement Analysis

Space shifting is easily possible, as the use licenses are not tied to specific devices, and because RMS does not specify formats, format shifting is only hindered by applications implementing RMS. Time shifting is also possible. However, platform shifting is not that easy, as it requires Microsoft to support RMS in the target platform, and requires applications in the target platform to be RMS enabled. Thus, we have to score RMS low on platform portability especially if one considers the fact that Microsoft does not support RMS on

every version of Windows (even if legacy operating systems such as Windows 98 are excluded). RMS can be integrated with any application, but every application requires be patching or upgrading to enable even the basic protections like read and write, which cannot be enforced by the operating system. However, the use of application support does allow for very fine grained and flexible access control specifications which can control any part of the application behaviour. Rights can be delegated but it requires the repackaging of the protected media, which could be expensive operation considering the size of certain documents such as presentations.

RMS has a comprehensive tracking and monitoring system, and it can be configured to handle various levels of data. Offline usage is possible, but depends on the flexibility of Active Directory or Passport to enable offline usage.

4.3.4 Legal and Social Requirement Analysis

Unlike media DRM systems, enterprise DRM systems are on a sounder legal footing, as they regulate the control of corporate data, often within a closed boundary. However, it is unknown how sound their legal footing is, especially when one considers different legislations with regards to employee privacy, monitoring of employees and employee access to information. In terms of transparency, there are no clear mechanisms on establishing the extent of the protections placed on the data without application support. There is no performance data with RMS, thus it cannot be rated.

4.4 Adobe Document Security

Adobe's DRM system was one of the earliest implementations in the consumer space. Originally (and still) used for Adobe's eBook format, Adobe's DRM system is now also available to enterprises. Unlike some of the DRM systems mentioned previously, Adobe Document Security provides protection for only one file format – PDF. But, the DRM system is the only system that can claim to support a wide range of platforms, from portable devices to different desktop architectures and operating systems. The details of the system are summarised from public documents published by Adobe [9][6][7].

4.4.1 Brief Overview

Adobe's DRM solution has two components – a server to create secure documents, and Adobe's popular PDF rendering application: Acrobat Reader. Note that, not all versions of the reader can access protected files, but Adobe does have capable readers for a number of different platforms. Documents are encrypted using symmetric keys, and these keys are protected in the license

using the user's public key. The user's private key serves as the authentication mechanism, as well as the means to extract the symmetric key to decrypt content. It is therefore possible to use super-distribution since use licenses are separated from the content.

Adobe does not retain control over the chain of trust – Acrobat Readers are capable of installing new certificate authorities, and trusted users; which means that there is no reason to enforce any restrictions for creating secure documents. Adobe's approach does have one flaw – there is no restriction on the user distributing multiple copies of his/her private keys across the Internet; thus allowing more than one person access to the protected data. To counter this, Adobe's system allows for tracking usage and access of the protected data.

4.4.2 Core Requirement Analysis

Access control is not governed by the distribution of the data, and access to protected data is not confined to a defined boundary; and thus persistent access control is achieved. The system does not regulate device management, and while digital certificates provide user identity control, this control can be replicated and does not provide any advanced identity system functionality such as groups or roles. Revocation of licenses, once issued, is virtually impossible as the licenses can easily be replicated and restored if revoked. The system does have mechanisms to update rights through issuing new licenses (which most probably invalidate existing licenses).

4.4.3 Usability Requirement Analysis

Adobe provides protection on only one document format – PDF, and thus provides no means for format shifting, without loosing the protections. However, the system scores very well on other portability factors such as time shifting, space shifting and platform shifting. Because almost any document type can be converted into PDF, the system provides for easy integration to existing systems; although the rendering is restricted to only one application. The system provides for restricting any functionality provided by Adobe Reader, and thus scores well in this respect.

4.4.4 Legal and Social Requirement Analysis

Unlike media DRM systems, enterprise DRM systems are on a sounder legal footing, as they regulate the control of corporate data, often within a closed boundary. However, how sound their legal footing is, is unknown, especially when one considers different legislations with regards to employee privacy, monitoring of employees and employee access to information.

Furthermore, Adobe Document Security can be used as a media DRM system, but then the system's legal footing needs to be examined in terms of the implementation. In terms of transparency, Adobe Reader can easily display all the restrictions placed on the data. There is no performance data therefore this cannot be rated.

4.5 Consolidated Ratings Summary

The consolidated ratings summary for the systems discussed in this paper is detailed in Table 1.

Table 1. Summary of our requirement ratings for the various DRM systems which we discussed in this paper

	Requirement	iTunes	WM	Adobe	RMS
1	Provide Persistent Protection	2	2	2	2
2	Represent User Identity	1	0	1	2
3	Support Multiple User Authentication Protocols	0	0	0	1
4	Represent and Authenticate Resource Identity	n/a	n/a	n/a	1
5	Represent and Authenticate Device Identity	2	0	0	2
6	Represent and Authenticate User Groups	0	0	0	2
7	Represent and Authenticate User Roles	0	0	0	2
8	Represent and Authenticate Resource Groups	0	0	0	0
9	Represent and Authenticate Device Groups	0	0	0	0
10	Represent the Authorisation (Use License)	0	2	2	2
11	Authenticate the Use License	0	1	2	1
12	Support User Duties	0	0	0	0
13	Revocation of Rights	1	1	0	1
14	Update of Rights	1	1	2	1
15	Time Shifting	0	2	2	2
16	Format Shifting	1	1	0	2
17	Space Shifting	2	0	2	2
18	Platform Shifting	1	1	2	1
19	Integration with Existing Applications	0	1	1	0

20	Delegation of Rights	0	0	0	1
21	Fine Grained and Flexible Access Control Specification	0	1	2	2
22	Tracking and Monitoring	0	n/a	2	2
23	Offline Usage	2	2	2	1
24	A Legal Framework for DRM	0	0	1	1
25	Transparency	2	n/a	2	1
26	Privacy and Anonymity	2	n/a	n/a	n/a
27	Do Not Alter Platform Functionality and Performance	2	1	n/a	n/a

5. Conclusions

In this paper we have discussed 27 requirements for a generalised DRM systems, which we have drawn from a broad number of different sources. These requirements are categorised into three categories: the core requirements for access control, usability requirements and the legal and social requirements. We have discussed each requirement in detail, together with our motivations regarding their importance in DRM systems. As the categories imply, not all of the requirements are necessary to achieve persistent access control, but, these additional requirements provide a greater usability of the DRM system for all the parties involved.

We also evaluated four different DRM systems, and our ratings are summarised in table 1. We focused our analysis on how easily the systems can be used as general DRM systems instead of focusing on the consumer evaluation of DRM systems, as Mulligan et al. did in [42].

Our analysis shows a few clear general issues:

1. DRM systems do not focus on users and thus have very poor user-management systems. Microsoft RMS is designed for enterprises and is the notable exception. User management is a crucial component of access control and the lack of user management shows the immaturity of most of these solutions.
2. Using device identity as the base for identity management is clearly the popular approach, despite the fact that users own and operate a number of different devices; and in fact a single device can be owned and operated by multiple users. The use of device groups have been ignored even when the vendors of the DRM systems market a number of different devices capable of rendering protected data. Furthermore, electronic devices often have short lifespans

(when compared to analogue media) but restrictions on space and platform portability severely hamper the user experience.

3. Revocation and change of access rights is also important in any access control schemes; and DRM systems have rather poor support for both of these. DRM systems currently revoke entire devices or users instead of focusing on individual resources; and in the long run this is not a sustainable strategy.
4. Vendors of DRM systems do not advertise, and possibly do not understand, the legal and social requirements for their systems. Vendors like Microsoft who want to license their systems need to set up clear guidelines on what consumers expect from DRM protected media.

We believe that a successful DRM system needs to successfully address all the requirements we have outlined. Unfortunately, as we summarised in table 1, none of these systems have satisfied more than 50% of the requirements completely. One of the major benefits of the evaluation framework we have presented, is that we can track the progress of current and emerging DRM systems as they evolve.

References

[1] PlayFair. URL: http://playfair.sourceforge.net/.

[2] Zune problems for MSN customers. *BBC News (online)* (06 Nov 2006). URL:http://news.bbc.co.uk/2/hi/technology/6120272.stm.

[3] DRM From the Viewpoint of the Electronic Industry. *Slashdot* (2003). URL:http://slashdot.org/article.pl?sid=03/11/25/1821218.

[4] New Tool Cracks Apple's Fairplay DRM. *Slashdot* (2004). URL:http://apple.slashdot.org/comments.pl?sid=102992.

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

[6] Adobe livecycle document security. Data sheet, Adobe, 2005. URL:http://www.adobe.com/products/server/securityserver/pdfs/docsecurityserverds.pdf.

[7] Adobe reader, 2005. URL:http://www.adobe.com/products/acrobat/readermain.html.

[8] NAVSHP (FP6) DRM requirement report, 2005.

[9] A primer on electronic document security. Technical white paper, Adobe, 2005. URL:http://www.adobe.com/security/pdfs/acrobat security wp.pdf.

[10]Approved document no 1, wd 3.0 – technical reference: Value chain functions and requirements, phase iii. *The Digital Media Project* (2006-11-02). URL:http://www.dmpf.org/open/dmp0861.zip.

[11] Gates: Digital locks too complex. *BBC NEWS* (2006-12-15 11:38:36 GMT). URL:http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/6182657.stm Last Accessed: 2006-12-30.

[12] Evaluating DRM: Building a marketplace for the convergent world. *Center for Democracy & Technology* (September 2006).

[13] APPLE INC. Apple iTunes – Overview. URL:http://www.apple.com/itunes/overview.html.

[14] APPLE INC. Apple customer privacy statement, 2004-12. URL:http://www.apple.com/legal/privacy/ Last Accessed: 2007-01-29.

[15] APPLE INC. iTunes Store tops two billion songs, 2007-01-09. URL:http://www.apple.com/pr/library/2007/01/09itunes.html Last Accessed: 2007-01-29.

[16] ARNAB, A., AND HUTCHISON, A. Piracy and content protection in the broadband age. In *Proceedings of the South African Telecomunication Networks and Applications (SATNAC) Conference 2006* (2006).

[17] AUTHENTICA. Enterprise rights management for document protection. White paper, Authentica, 2005.

[18] 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.

[19] BECKER, D. Passport to nowhere? *C-Net News.com*. URL:http://news.com.com/2100-7345 3-5177192.html.

[20] BERLIND, D. A load of C.R.A.P. *ZDNet.com* (2005). URL:http://news.zdnet.com/html/z/wb/6035707.html Last Accessed: 2007-01-06.

[21] BLOCK, R. Fairuse4wm strips windows media DRM! *Engadget* (2006-08-25). URL:http://www.engadget.com/2006/08/25/fairuse4wm-strips-windows-media-drm/ Last Accessed: 2006-08-26.

[22] BURROWS, P. I want my iTunes subscription service! *BusinessWeek.com* (2005-08-16). URL:http://www.businessweek.com/the thread/techbeat/archives/2005/08/ i want my itune.html Last Accessed: 2007-01-29.

[23] COHEN, P. iTunes hits the 50 million song mark. *The Industry Standard - Internet Business News* (2004).
URL:http://www.thestandard.com/article.php?story=20040315173205175.

[24] DOOM9 FORUMS. DRM 10 cracked?
URL:http://forum.doom9.org/showthread.php?t=89243 Last Accessed: 2006-08-26.

[25] DOOM9 FORUMS. FairUse4WM - a WM/DRM removal program.
URL:http://forum.doom9.org/showthread.php?t=114916 Last Accessed: 2006-08-26.

[26] DUFFT, N., STIEHLER, A., VOGELEY, D., AND WICHMANN, T. Digital music usage and DRM – results from an European Consumer Survey. Report, INDICARE Project, 2005.

[27] FERRAIOLO, D. F., AND KUHN, D. R. Role-based access control. In *Proceedings of the 15th NIST-NSA National Computer Security Conference* (1992). Available online: http://csrc.nist.gov/rbac/ferraiolo-kuhn-92.pdf.

[28] GRAHAM, J. Emusic's pitch: Download song & and own it. *USA Today* (2006-07-30). URL:http://www.usatoday.com/tech/products/services/2006-07-30-emusic x.htm Last Accessed: 2007-01-29.

[29] JOHANSEN, J. L. Sharpmusique, 2005-09-17.
URL:http://nanocrew.net/2005/09/17/sharpmusique-10/ Last Accessed: 2007-01-29.

[30] KIM, J. MP3 Insider: the truth about battery life. *CNET.com* (2006-03-13).
URL:http://reviews.cnet.com/4520-6450_7-6462771-1.html Last Accessed: 2007-01-29.

[31] KIM, J. MP3 Insider: all-you-can-eat itunes–why not? *CNET.com* (2006-05-30).
URL:http://reviews.cnet.com/4520-6450_7-6534082-1.html Last Accessed: 2007-01-29.

[32] LIFSHITZ, Z. TIRAMISU DRM requirements. *The Digital Media Project* (2004-05-10). URL: http://www.dmpf.org/open/dmp0086.doc.

[33] MAGUIRE, J. Microsoft vs. iTunes. *NewsFactor.com* (2004).

[34] MICROSOFT. Features of windows media drm.
URL:http://www.microsoft.com/windows/windowsmedia/forpros/drm/features.aspx Last Accessed: 2006-08-23.

[35] MICROSOFT. Sdks and versions of windows media drm. URL:http://www.microsoft.com/windows/windowsmedia/forpros/drm/sdkandversions.aspx Last Accessed: 2006-08-23.

[36] MICROSOFT. *Taking Advantage of Super Distribution with Windows Media Rights Manager 7*, 2000. URL:http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwmt/html/wmrm7distribution.asp.

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

[38] MICROSOFT. Technical overview of windows rights management services for windows server 2003. White paper, 2003.

[39] MICROSOFT. Windows right management services - data sheet, 2003. URL:http://www.microsoft.com/windowsserver2003/techinfo/overview/rmsdatasheet.mspx.

[40] MICROSOFT. 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.

[41] MICROSOFT. Windows media DRM FAQ, October 2005. URL:http://www.microsoft.com/windows/windowsmedia/forpros/drm/faq.aspx Last Accessed: 2006-08-23.

[42] 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.

[43] 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).

[44] PRUNEDA, A. *Security Overview of Microsoft Windows Media Rights Manager*, 2001.URL:http://msdn.microsoft.com/library/en-us/dnwmt/html/wmrm71security.asp.

[45] PRUNEDA, A. *Getting Started with Windows Media Rights Manager SDK*, June 2002. URL:http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwmt/html/wmrm7quickstart.asp.

[46] RAGAN, S. Trouble for Apple's iTunes in Norway. *Monsters and Critics* (2007-01-29).

[47] ROJAS, P. Pymusique returns. *Engadget.com* (2005-03-22). URL:http://www.engadget.com/2005/03/22/pymusique-returns/ Last Accessed: 2007-01-29.

[48] ROSENBLATT, B. Technology comparison: Authentica active rights management and microsoft windows rights management services. White paper, Giantsteps Media Technology Strategies, 2005. Document Commissioned by Authentica.

[49] SCHULTZ, C., AND MERRIL, P. Proposed requirements for interoperable DRM platforms. *The Digital Media Project* (2004-02-13). URL:http://www.dmpf.org/open/dmp0025.doc.

[50] SLATER, D. Microsoft's zune won't play protected windows media. *EFF DeepLinks* (15 Sep 2006). URL: http://www.eff.org/deeplinks/archives/004910.php.

[51] WATKINS, T., BROCIOUS, C., AND JOHANSEN, J. L. pyMusique, 2005. URL: http://drmnews.com/pymusique/ Original Website Broken, Last accessed: 2007-01-29.