REQUIREMENT ANALYSIS OF ENTERPRISE DRM SYSTEMS

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 or DRM has been mainly used to provide access control protection for multimedia products marketed to consumers, like music and movies. There are also a number of DRM products, like Authentica and Microsoft's RMS, that aim to protect documents for enterprises. However, none of these products provide for all the needs of an enterprise, and furthermore these products do not offer all the benefits that DRM potentially offers to an enterprise.

In this paper we discuss what DRM offers to enterprises, examine the base requirements for an enterprise DRM system and then analyse how well three existing enterprise DRM products satisfy the requirements of an enterprise DRM system. We have found that enterprise DRM systems have yet to mature with many requirements not satisfied.

KEYWORDS
DRM, Digital Rights Management, ERM, Enterprise Rights Management, Access Control, Rights Management

REQUIREMENT ANALYSIS OF ENTERPRISE DRM SYSTEMS

1 INTRODUCTION

Recently, Apple Computers took three online publications, Powerpage, Apple Insider and Think Secret, to court for publishing detailed details on new unannounced products [10]. The aim was to force the publishers to reveal their sources on who leaked the information (and thus violated Apple's non-disclosure agreements). While this case was more interesting for the legal arguments on whether the publications had to give up the identities of their sources, our focus is on the fact that Apple Computers, one of the major companies in the computer industry could not protect their trade secrets from being distributed freely to unauthorised persons. Apple is not the only company with this problem – a lot of confidential information leave the control of their owners on a regular basis, both willingly and unwillingly, and there have been many estimates on the cost of intellectual property losses.

Traditionally, data has been encrypted and together with a limited release of keys, has been all that companies have done (and have been able to do) to protect their confidential data. Traditional file system protection (like restrictions of certain users to access certain files and directories) have been used to complement the encrypted files. However, encryption is not really a complete solution. Using the example of Apple Computers above, let us call the malicious employee Bill. From the information in the press covering the court case [10], Bill is most likely to be a trusted employee who had complete access to the confidential documents. Traditional encryption and access control mechanisms will not prevent Bill from distributing the confidential documents – he needs only to decrypt the document and then he can distribute it in any form he wants.

For these reasons, what is required is a mechanism that would allow the owner of the data to prescribe the access control rules which will either work as prescribed, or not allow access at all. And while access control rules are useful, it would be even better if the rules were more substantial than read, modify and execute in addition to who gets these rules. More complex control rules like restrictions on printing and excerption could be more useful.

Enterprise Digital Rights Management (E-DRM) products aim to provide such solutions. In this paper, we discuss what are the requirements for an E-DRM system, which we have discussed with a IT security manager of a South African subsidiary of a major international communication company. We then review three major E-DRM products that available on the market, and analyse how well they meet the requirements we discussed as well as what we consider the future for enterprise DRM systems.

2 REQUIREMENTS

DRM has mainly been used by record companies to protect music sold on the Internet. Other applications of DRM such as securing e-books, have been less successful. The general requirements for DRM in the enterprise are almost the same as the DRM employed in the consumer space, except for the fact that enterprises do not need to cater for the flexibility required by consumers because enterprises operate in a more closed environment.

Enterprises have the sole control on their intellectual property (which can range from patents to office memos about Christmas parties), and can dictate the full range of rights they would like to prescribe on their intellectual property (IP). Enterprises can also extend DRM to track and monitor the usage of protected data without violating privacy laws. In this section, we present a set of requirements for DRM in the enterprise, and give our motivation for these requirements.

Some of the requirements we present below have been presented before by Bartolini et al. [7], Park et al. [12], Mulligan et al. [11] and Arnab et al. [6].

1. **Persistent protection:** A DRM system must guarantee the persistent protection of secured objects. This means that regardless of the location of the digital data [1], the access controls that are imposed by the rights holder must either be enforced or the device should not be able to read the file at all. If persistent failure is not achieved, the system can be considered a failure.

2. **Intercompany Transactions:** Other than trading between themselves, modern companies also outsource and enter into partnerships to create new products and services. These transactions often involve confidentiality clauses, but as seen with the Apple case, it is very difficult to enforce these clauses. An enterprise DRM system must be able to allow for different companies to interact with each other without compromising security.

3. **Portability:** Portability can have a number of different meanings, and not all aspects of portability are equally important. We have divided portability into four categories, and discuss them in increasing importance:

   (a) **Time Shifting:** Time shifting refers to the ability of the user to access the work when he or she wants to. While the freedom is critical in the consumer space, this is not the same in an enterprise. In fact, it could be the case that access to protected data in “odd” hours is indicative of misuse. Thus, the ability to thwart time shifting is crucial in enterprises, and time shifting is not that important.

   (b) **Space Shifting:** Space shifting refers to the ability of the user to freely access the work in whichever device he or she wants. In most cases, enterprises would like to restrict the number of devices that can access protected data, and thus space shifting is not that important.

   (c) **Format Shifting:** Referring to online music and video stores, Mulligan et al. argued that format shifting is also an important portability issue [11]. Format shifting allows the user to change the format of the data file (without necessarily affecting the access control rules). Format shifting could be important in an enterprise for a variety of 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.

   (d) **Platform Shifting:** Platform shifting refers to the ability of the user to use different operating systems and devices to access the protected data. In an enterprise, this is probably the most important requirement. Even small businesses are likely to make use of a multitude of different devices – PDA’s, desktop computers, laptops and servers. Even if an enterprise decides to make use of one vendor for all

[1] This only applies to the digital format of the data. For example, for an electronic text file, the controls must apply to the text and not to the paper copy if the text can be printed. This is an important distinction, as there will always be analogue bypasses to DRM – for example taking photos with a camera when a screenshot is not allowed.

their devices (e.g. Linux or Microsoft), the devices are likely to run different versions of the operating system and applications and thus portability is extremely important.

4. **Excerpting:** Excerption allows a user to take a certain segment of data from one source for inclusion in another data file. Excerption is important in enterprises – not only to allow for re-use of enterprise's own IP, but also for assembling complex documents. For example, financial statements of a company comprise of amongst other things, income statements, director's reports and auditor's reports. Each of these documents are of different types and have different authors and access control requirements. However the financial statements are a complete package, and the different components must be put together, usually by someone who is not an author of any of those documents. Thus DRM for enterprises need to cater for excerption.

5. **Integration with existing applications:** Many enterprises use software developed for their specific needs, and confidential documents and data are not necessarily generated by popular office applications such as Microsoft Office or Adobe Acrobat. Thus, integration with existing applications would be a crucial deciding factor for selecting a particular DRM solution.

6. **Transfer of Rights:** Employees in a company leave projects, move to different departments, different branches and even leave the company. Similarly, IP of an enterprise also has changes in control and could even be traded to other enterprises. For this reason there is a need for DRM to allow for the transfer of rights between two parties. However, companies also need to control the trade of their IP – employees should not be allowed to reveal trade secrets to journalists for example as in the case cited in the introduction. Thus, together with a mechanism to transfer rights, there must be mechanisms to control of who can effect a transfer of rights. Thus, the use of an authorised entity, or maybe a trusted third party, is required to ensure that the transfer of rights is done legally and correctly.

   Furthermore, because of the ease of replication of digital data, transfer of rights also means that the protected data should not be accessible after the right has been transfered. Thus if an employee leaves the company, he or she should not be able to access any IP owned by the company without permission.

7. **Allow for changes to access and usage rights after distribution:** The initial rights assigned to an employee might not be enough (because they are too restrictive for example) or maybe more than necessary (because the employee was re-assigned to a different department, for example). For this reason, DRM systems in an enterprise need to allow for changes to access and usage rights after distribution of protected data.

8. **Track usage of DRM works:** Although not a feature of DRM itself, monitoring the access and usage patterns of users can be easily achieved. The enterprise would of course like to monitor the usage of confidential data, 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 a contentious issue. This issue becomes further clouded when considering the rights the employer has in monitoring employees of company property.

9. **Offline Usage:** Communication networks are not perfect, and there are many situations where an employee may not have access to the Internet (for example on a aeroplane). Thus offline usage is desirable; but does have its drawbacks – offline usage reduces monitoring and tracking capabilities; and also limits the control an enterprise has over its data. For example, 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.

10. **Easy identification:** In [7], the authors identified the identification of digital works as a crucial component of a DRM system. A DRM system must be able to uniquely identify digital works on the Internet, and have a mechanism to correctly associate the users that have rights to use/access the work as well as mechanisms to associate the right holders of the work.

11. **Easy Verification:** Another criteria given by Bartolini et al. is to allow honest users to easily prove that they have legitimate access to the protected work [7]. This extends in general to all objects and transactions in a DRM system; integrity and verification should be easy to prove.

In the next section we discuss three enterprise DRM systems, and then analyse how well they satisfy the requirements we have just discussed.

3 ENTERPRISE DRM SYSTEMS

Unlike DRM systems for music and other multimedia, enterprise DRM systems are less publicized and have lower media coverage. Despite this, there are a number of enterprise DRM systems in the market most offering data protection targeted mostly for Microsoft Windows XP and 2000 operating systems. In this section we discuss a few enterprise DRM system and how well they satisfy the requirements we have just discussed. In each of the subsections, we give a small description of the system and then examine how well each of the requirements are satisfied against a 3 point scale developed by us:

0 : This requirement is not available at all.

1 : This requirement is technically met, but compromises security, or not a complete.

2 : This requirement is met, but can be improved upon.

3 : This requirement is completely supported.

A comparison between all the various systems is shown in table 1 in section 3.4.

3.1 Microsoft Rights Management Services (RMS)

Microsoft's Rights Management Services (RMS) is promoted as a complete DRM system for enterprise deployment. RMS consists of server side Windows components for Windows Server 2003, as well as client side components for Windows XP [1]. The client side component is a kernel module that helps in enforcement of RMS usage rules but RMS does not offer complete operating system enforcement, and requires applications to use RMS libraries to make use of RMS on the client side.

1. **Persistent protection:** When an RMS enabled document is created, the data is put in a cryptographic envelope together with the use license [1]. As long as the cryptographic envelope is not broken, the document is protected; and with the use of strong encryption, persistent protection is achieved. As far as we are aware, there has also been no successful attacks on RMS protection.
   Rating: **3**

2. **Inter-company Transactions:** All things considered, this is probably RMS's biggest weakness. By its design, RMS has two constraints for enabling inter-company transactions – firstly, all machines that can handle RMS enabled documents first require to be a "trusted entity" [1], a trusted machine part of the trusted network. Secondly, the default authentication mechanism for RMS is the company's Microsoft Active Directory service. While Microsoft Passport is also offered as an authentication mechanism, the company would require to integrate the Microsoft Passport system with its own, and with Passport's history of security failures, very few companies are willing to take this step [8].

   Thus to enable inter-company transactions between two companies, the machines of both companies need to be part of the same trusted network and the users of both companies either need to have accounts in each other's active directories or integrate Passport. Thus inter-company transactions, though technically possible are very difficult to achieve and insecure.
   Rating: **1**

3. **Portability:** As stated in the requirements, we shall examine each aspect of portability in turn:
   (a) **Time Shifting:** RMS allows for the restrictions of when the user can access the document and for how long.
   Rating: **3**
   (b) **Space Shifting:** As discussed earlier, space shifting is limited by the insistence of using trusted machines. In an intra-enterprise scenario this is perfect.
   Rating: **2**
   (c) **Format Shifting:** RMS requires applications to be RMS enabled before RMS can be used. With Microsoft Office 2003 being the only major application that is RMS enabled, format shifting is really not available.
   Rating: **2**
   item
   Platform Shifting: In the client side, RMS is only available in full for Windows XP. However many enterprises are still using older versions of Windows and many also use other operating systems such as Linux and Mac OS. With RMS unavailable for other operating systems and non Intel-X86 architectures, platform shifting is impossible.
   Rating: **0**

4. **Excerpting:** Excerption is allowed as one of the use conditions.
   Rating: **3**

5. **Integration with existing applications:** Microsoft provides a development kit that allows for applications to make use of RMS protection. This means that existing applications need to be modified before they can have protection.
   Rating: **2**

6. **Transfer of Rights:** In RMS, "super users" are allowed to change the ownership of any RMS enabled document. Super users are also allowed to add and remove other super users. While not a perfect solution (a rogue super user could remove other super users and then leave without a trace), it is a workable solution for most enterprises (for example, the CEO or the major shareholder could be the super user).
   Rating: **2**

7. **Allow for changes to access and usage rights after distribution:** Its not possible in RMS, and in fact the user scenarios in RMS explicitly shows that this is not possible [1].
   Rating: **0**

8. **Track usage of DRM works:** RMS allows for detailed logging of access and usage patterns.
   Rating: **3**

9. **Offline Usage:** As long as the machine is a trusted entity, and the use license does not require online connectivity, RMS allows for offline usage.
   Rating: **3**

10. **Easy identification:** Identification of users is done using email addresses which are globally unique. However, RMS enabled data itself does not have versioning control by default, and thus there is no way to distinguish different versions of a document without opening the document. This has potential for problems if an 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.
    Rating: **2**

11. **Easy Verification:** Integrity and verification is easily provable in RMS.
    Rating: **3**

3.2 Authentica Enterprise Digital Rights Management Solutions

Authentica markets itself as the "leader in enterprise rights management (ERM) solutions" [4]. Their two major products, Authentica Secure Office and PageRecall, are essentially patches for Microsoft Office and Adobe PDF file format. Authentica's enforcement level is at the application layer and tightly integrated to the specific applications they support [9].

1. **Persistent protection:** As with RMS and other DRM products, when the protected document is created, the data is put in a cryptographic envelope. As long as the cryptographic envelope is not broken, the document is protected; and with the use of strong encryption, persistent protection is achieved. As far as we are aware, there has also been no successful attacks on Authentica's products.
   Rating: **3**

2. **Inter-company Transactions:** Unlike RMS, Authentica supports a wider range of authentication protocols, and also has a simpler and more effective way of allowing external users access. External users are still required to authenticate themselves to the creator of the protected document, but this authentication does not have to be tightly integrated with the company's own user management systems.
   Rating: **2**

3. **Portability:** As stated in the requirements, we shall examine each aspect of portability in turn:
    (a) **Time Shifting:** Authentica allows for the restrictions of when the user can access the document and for how long.
    Rating: **3**
    (b) **Space Shifting:** Unlike RMS, Authentica does not insist on the use of "trusted entities", and thus space shifting is easier to achieve.
    Rating: **3**
    (c) **Format Shifting:** Like RMS, documents protected by Authentica can only be opened and used by applications that are supported by Authentica. With Microsoft Office and Adobe PDF being the only applications supported, there is very limited scope for format shifting.
    Rating: **1**
    (d) **Platform Shifting:** Similar to RMS, Authentica only supports Windows 2000 and XP as the client operating system. However many enterprises are still using older versions of Windows and many also use other operating systems such as Linux, Mac OS and even embedded operating systems such as Palm OS and Windows CE on PDAs. With Authentica's DRM solutions unavailable for other operating systems and non Intel-X86 architectures, platform shifting is impossible.
    Rating: **0**

4. **Excerpting:** Excerption is allowed as one of the use conditions.
    Rating: **3**

5. **Integration with existing applications:** Authentica's system is only for specific applications and not customizable.
    Rating: **0**

6. **Transfer of Rights:** As part of rights changes after distribution, Authentica allows for the transfer of rights. However the mechanism is not detailed.
    Rating: **3**

7. **Allow for changes to access and usage rights after distribution:** Changes in rights are allowed after distribution.
    Rating: **3**

8. **Track usage of DRM works:** Like RMS, Authentica's E-DRM solutions offer very good usage tracking.
    Rating: **3**

9. **Offline Usage:** It is not clear if Authentica's E-DRM solution requires authentication every time the user accesses the document [9].
    Rating: **n/a**

10. **Easy identification:** Like RMS, versioning support is not available by default, and thus there is no way to distinguish different versions of a document without opening the document. This has potential for problems if an 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.
    Rating: **2**

11. **Easy Verification:** Integrity and verification are easily provable.
    Rating: **3**

3.3 Adobe LiveCycle & Adobe DRM

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. However, unlike Authentica and Microsoft RMS, the main aim of Adobe's DRM system is to protect documents that are published in the PDF format instead of protecting the original format. Adobe's LiveCycle suite is a collection of programs that allow for the creation and management of protected PDF files. The *Adobe LiveCycle Document Security* system is essentially a webservice that takes a PDF file and encapsulates it in a cryptographic envelope designed for a specific recipient. The system can also handle PDF forms [2]. The *Adobe LiveCycle Policy Server* allows for finer management of the protected PDF files by adding functionality like document expiry dates and changing user rights after distribution [5]. Protected PDF files can only be read by some versions of the Adobe Acrobat Reader like versions 6.0 and later for Microsoft Windows XP and 2000. [3].

1. **Persistent protection:** Persistent protection is achieved, but as shown a few years ago, Adobe DRM can be broken. However, Adobe has subsequently fixed the flaw and no further attacks have taken place.
   ***Rating:* 3**

2. **Inter-company Transactions:** Adobe's system has a very fine control of users who can view the protected documents. Thus not only are inter-company transactions enabled, but transactions between the enterprise and any individual is also possible. [2]
   ***Rating:* 3**

3. **Portability:** As stated in the requirements, we shall examine each aspect of portability in turn:
   (a) **Time Shifting:** Adobe does support documents that expire after a limited time. [5]
   ***Rating:* 3**
   (b) **Space Shifting:** Space shifting is regulated by how the enterprise protects the documents. If the protection is done through the use of passwords, space shifting is possible. However, if asymmetric encryption is used, space shifting does not seem to be possible.
   ***Rating:* 2**
   (c) **Format Shifting:** Adobe's DRM solution only works with Adobe PDF. [5]
   ***Rating:* 0**
   (d) **Platform Shifting:** Adobe's PDF reader is available on a number of different operating systems including various versions of Windows, Linux, OS X and Palm OS. Other operating systems are also supported but its unclear if these readers support DRM enabled PDFs [3].
   ***Rating:* 3**

4. **Excerpting:** Excerption is allowed as one of the conditions.
   ***Rating:* 3**

5. **Integration with existing applications:** Adobe's system allows for any data type to be converted into protected PDF. However, the native data formats are not protected. This type of protection does have value if it can be ensured that the native data files themselves are not distributed.
   ***Rating:* 1**

6. **Transfer of Rights:** LiveCycle creates documents on a per user basis [2], and thus transfer of rights is not possible. However revocation is still possible [5].
   ***Rating:* 1**

7. **Allow for changes to access and usage rights after distribution:** Changes in rights are allowed after distribution.
   ***Rating:* 3**

8. **Track usage of DRM works:** Tracking is supported, but the extent is not publicised as in the case of RMS and Authentica.
   ***Rating:* 2**

9. **Offline Usage:** Offline usage is supported in both protection modes.
   ***Rating:* 3**

10. **Easy identification:** Versioning support is included and different versions will have different identification mechanisms. We assume that the identifiers used are globally unique.
    ***Rating:* 3**

11. **Easy Verification:** Integrity and verification are easily provable.
    ***Rating:* 3**

3.4 Summary

A summary of the rating is given below:

	Requirement	**RMS**	**Authentica**	**Adobe**
01	Persistent Protections	3	3	3
02	Inter-company transactions	1	2	3
03	Portability: Time Shifting	3	3	3
04	Portability: Space Shifting	2	3	2
05	Portability: Format Shifting	2	1	0
06	Portability: Platform Shifting	0	0	3
07	Excerpting	3	3	3
08	Integration with existing applications	2	0	1
09	Transfer of Rights	2	3	1
10	Allow for changes to access and usage rights after distribution	0	3	3
11	Track usage of DRM works	3	3	2
12	Offline Usage	3	-	3
13	Easy identification	2	2	3
14	Easy Verification	3	3	3
	Total (out of 42 assuming equal weighting)	29	29	33

Table 1: Requirement Analysis Scores of three enterprise DRM systems with equal weighting

3.5 Interpretation

Although we have measured each rating equally, most enterprises would value some requirements more than others. Enterprises that run a single operating system for example (highly unlikely with the spread of PDA's) are going to value platform shifting less than other requirements. Thus the overall score achieved by the three systems discussed will change dramatically when taking this into account.

In our opinion, we think the following requirements would be more valued by enterprises:

- Inter-company transactions
- Portability: Format Shifting
- Portability: Platform Shifting
- Integration with existing applications
- Transfer of rights
- Allow for changes to access and usage rights after distribution
- Offline usage

If we give the above requirements higher weighting, the results are more interesting as can be seen in table 2. Authentica is no longer tied with RMS (and in fact falls behind), and Adobe retains its lead.

	W	**Requirement**	**RMS**	**Authentica**	**Adobe**
01	1	Persistent Protections	3	3	3
02	2	Inter-company transactions	2	4	6
03	1	Portability: Time Shifting	3	3	3
04	1	Portability: Space Shifting	2	3	2
05	2	Portability: Format Shifting	4	2	0
06	2	Portability: Platform Shifting	0	0	6
07	1	Excerpting	3	3	3
08	2	Integration with existing applications	4	0	2
09	2	Transfer of Rights	4	6	2
10	2	Allow for changes to access and usage rights after distribution	0	6	6
11	1	Track usage of DRM works	3	3	2
12	2	Offline Usage	6	-	6
13	1	Easy identification	2	2	3
14	1	Easy Verification	3	3	3
		Total (out of 63)	39	38	47

Table 2: Requirement Analysis Scores of three enterprise DRM systems with weighting

4 DISCUSSION

We have only reviewed three enterprise DRM systems, and while there are others, most of the other systems offer similar functions as Authentica and are also essentially application patches like Authentica. Thus, we expect their rating to be similar to Authentica's rating.

As shown in tables 1 and 2, enterprise DRM systems have not fully matured yet. No DRM system can offer both portability and support for a wide range of applications, and while Adobe's system comes close for providing great support, the system is only useful for protecting "published" documents and not for documents that need to be edited frequently. For example if two companies wish to jointly bid for a tender, employees of the respective companies need to collaborate to produce the bid document. Adobe's system is not going to be useful for this function and if the document needs to be produced using applications other than Microsoft Office, RMS and Authentica would not work either.

As shown in tables 1 and 2, some requirements are not handled well in more than one DRM systems, especially format and platform shifting. The list below looks at these requirements and some of the reasons for this:

1. **Inter-company Transactions:** The main problem with Authentica and RMS is in the manner they conduct user authentication. With RMS, enabling inter-company transactions leads to possible general security issues with Microsoft Passport or requires integration with the originating enterprise's servers. Similarly, even though Authentica allows for a wider range of authentication mechanisms, the end authentication is still controlled by the originating enterprise. Thus a problem in the originating enterprise (power failure, Internet disconnection) would hamper the recipient.

2. **Space Shifting:** Space shifting is hampered by authentication mechanisms used by the DRM system; and on an enterprise level, we do not consider space shifting to be a very important requirement.

3. **Format Shifting:** In the case of RMS, it is currently a lack of applications using RMS (and Microsoft Office not supporting different formats) that hampers format shifting. Authentica only caters for Microsoft Office, and thus does not support format shifting while Adobe's DRM system is tied in with the Adobe PDF format. We do not see this situation changing in the near future.

4. **Platform Shifting:** Microsoft RMS and Authentica are centered around Microsoft Windows XP only and thus do not lend itself for platform shifting.

5. **Integration with existing applications:** RMS and Authentica essentially require modification of the existing applications to work while Adobe will work with any PDF file, but only PDF files.

6. **Easy Identification:** We were surprised at the lack of version control in the systems. Identification also has implications for portability and inter-company transactions.

In our opinion, Enterprise DRM systems must address all the requirements we have outlined before being considered for mass roll out. Part of the problem in this regard is the lack of standards regarding DRM package formats and protocols. We also support the view that application level DRM enforcement (such as Authentica and Adobe) is only a temporary solution [13], and operating system and ultimately hardware level enforcement are the only full solutions. In our current project, "Distributed Componentised DRM System", we aim to create a framework that caters for the requirements we have outlined. The framework aims to separate the various players and functions of a DRM system and then build up a system using the components (most of them being web services). We also have a sub project that is investigating the effectiveness of kernel level DRM enforcement.

5 CONCLUSION

In this paper we presented a set of requirements for enterprise DRM systems. We then analysed three existing enterprise DRM systems on how well they satisfy these requirements. Unfortunately, even though there is a clear need for enterprise DRM systems, none of the products examined are suitable for mass deployment and use as standard security tools in enterprises.

6 ACKNOWLEDGMENTS

This work is partially supported through grants from the UCT Council and the National Research Foundation (NRF) of South Africa. Any opinions, findings, and conclusions or recommendations expressed in this paper/report are those of the author(s) and do not necessarily reflect the views of UCT, the NRF or the trustees of the UCT Council.

REFERENCES

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

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

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

[4] Authentica delivers next-generation enterprise rights management platform. Press release, Authentica, 2005.
URL: http://www.authentica.com/news/pr2005/02-14-2005-ARM.aspx?pf=1.

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

[6] ARNAB, A., AND HUTCHISON, A. Digital Rights Management - An overview of Current Challenges and Solutions. In *Proceedings of Information Security South Africa (ISSA) Conference 2004* (2004).

[7] 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.

[8] BECKER, D. Passport to nowhere? *C-Net News.com*.
URL: http://news.com.com/2100-7345_3-5177192.html.

[9] DEMARINES, V. Authentica's enterprise-drm suite for document protection. White paper, Authentica, 2004.
URL: http://www.authentica.com/request/downloadwp.aspx?fileId=ERM_doc_protect.pdf.

[10] FRIED, I. Apple goes to court to smoke out product leaker. *C-Net News.com* (21 December 2004).
URL: http://news.com.com/2102-1047_3-5499814.html.

[11] 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.

[12] 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).

[13] ROSENBLATT, B. DRM for the Enterprise, 2004.