Digital Rights Management for Content Distribution

Qiong Liu*, Reihaneh Safavi-Naini and Nicholas Paul Sheppard

School of Informatics Technology and Computer Science
University of Wollongong
Northfields Ave, Wollongong, NSW 2522, Australia

quong@uow.edu.au, rei@uow.edu.au, nps@uow.edu.au

Abstract

Transferring the traditional business model for selling digital goods linked to physical media to the online world leads to the need for a system to protect digital intellectual property. Digital Rights Management (DRM) is a system to protect high-value digital assets and control the distribution and usage of those digital assets. This paper presents a review of the current state of DRM, focusing on security technologies, underlying legal implications and main obstacles to DRM deployment with the aim of providing a better understanding of what is currently happening to content management on a legal and technological basis and well prepared for grasping future prospects.

Keywords: DRM, digital content

1 Introduction

With widespread use of the Internet and improvements in streaming media and compression technology, digital music, images, video, books and games can be distributed instantaneously across the Internet to end-users. Many digital service providers sell their digital content not only through CDs but also over computer networks. However, without protection and management of digital rights, digital content can be easily copied, altered, and distributed to a large number of recipients, which could cause revenue loss to media companies. Sony, the world's second-largest consumer electronics maker, has blamed digital piracy for eroding profit at its music business, which posted a loss of 10.3 billion yen ($160 million) in the three months to June 30, 2002 (Suzuki 2002). To protect commercial digital intellectual property and avoid digital piracy, we need a system that prevents unauthorized access to digital content and manages content usage rights.

Digital Rights Management systems can be used to protect high-value digital assets and control their distribution and usage. A DRM system should offer a persistent content protection against unauthorized access to the digital content, limiting access to only those with the proper authorization. It should be flexible to manage usage rights for different kinds of digital content (e.g. music files, video streams, digital books, images) across different platforms (e.g. PCs, laptops, PDAs[1], mobile phones) and control access to content delivered on physical media or any other distribution method (e.g., CD-ROMs, DVDs, flash memory).

This paper presents an overview of the current state in DRM. Section 2 describes DRM systems in general and explains how a typical DRM model used by current DRM implementations works. Existing commercial systems in the domain of digital rights protection are presented in Section 3. Section 4 analyzes the security measures to face the new challenge. We will look at underlying legal implications of DRM in section 5. In section 6, the major concerns raised by consumers about current DRM implementations are presented. Section 7 focuses on the working status towards standardization of DRM. Finally, a discussion about key factors that will lead to the success of DRM is given in Section 8.

2 System Overview

The core concept in DRM is the use of digital licenses. Instead of buying the digital content, the consumer purchases a license granting certain rights to him. A license is a digital data file that specifies certain usage rules for the digital content. Usage rules can be defined by a range of criteria, such as frequency of access, expiration date, restriction of transfer to other devices, copy permission etc. These rules can be combined to enforce certain business models, such as rental or subscription, try-before-buy, pay-per-use and a lot more.

Protected content can be distributed though a client/server system, super-distribution[2], digital audio/video broadcasting, or CDs. Without possessing digital license to the content, digital content is a sequence of scrambled bits. Often digital content and licenses are stored separately, which makes the system more flexible in a way that protected content can be freely distributed amongst users and license requests can take place later.

Through digital licensing, content providers can gain much more control over what the consumer can do with the content. The following subsections describe the common components in DRM systems, the working

*: This work is funded by Cooperative Research Centres - Smart Internet Technology, Australia.

[1] PDA: Personal Digital Assistant, a term for any small mobile hand-held device.

[2] Super-distribution: An approach to encourage users to pass along digital content to other users. However, the distributed content is in a cryptographically protected form.

process of DRM models and the role taken by client-side applications in DRM.

2.1.1 A Typical DRM Model

Different DRM vendors have different DRM implementations, names and ways to specify the content usage rules. However, the basic DRM process is the same, which usually involves four parties: the content provider, the distributor, the clearinghouse and the consumer. Usually a DRM system is integrated with an e-commerce system that handles financial payments and triggers the function of the clearinghouse, but due to space considerations we will not describe the details here. Figure 2.1 displays the common components of a DRM system based on most existing commercial systems. Following the explanation of these common elements, a typical model used by current DRM implementations is presented.

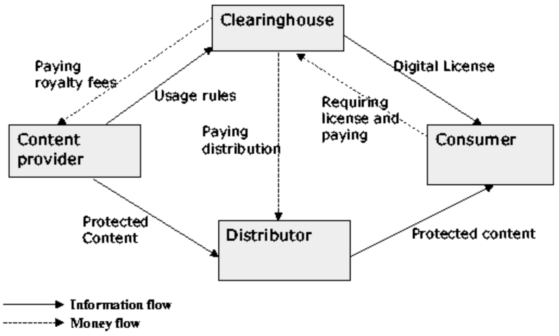

Figure 2.1: The common components in DRM system

- ***The content provider*** such as a music record label or a movie studio holds the digital rights of the content and wants to protect these rights.

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

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

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

A typical DRM model used by current DRM implementations works as follows:

Firstly, the content provider encodes the digital content into the format supported by the DRM system. Different DRM systems provided by different DRM vendors may support different content formats. The digital content is then encrypted and packaged for the preparation of distribution. The content provider may use watermarking technology to embed digital codes into the digital content that can identify the ownership of the content and the usage rules.

Next, the protected content is transferred to the appropriate content distribution server, e.g. web server or steaming server, for on-line distribution. The digital license containing content decryption keys and usage rules is sent to the clearinghouse. The usage rules specify how the content should be used, such as copy permit, pay-per-view, a one-week rental, etc.

At the other end of the process, the consumer downloads the digital content from the web server or requests streaming content from the streaming server. To be able to consume the protected content, the user has to request a valid license from the clearinghouse. After receiving the license request, the clearinghouse verifies the user's identity for example by having the user present a valid digital certificate, charges his account based on the content usage rules, and generates transaction reports to the content provider. Finally, the license is delivered to the consumer's device after the consumer has paid through the e-commerce system, and the protected content can be decrypted and used according to the usage rights in the license.

In this model, consumers can pass along received digital content to other people through super-distribution, which lets vendors market their digital content to a vast amount of potential customers without direct involvement. Although digital content can be freely distributed, to utilize the content, the recipient has to contact the clearinghouse and provide whatever information or payment required for the license.

2.1.2 Other Variants

Sometimes, the license can be delivered to the requesting application prior to or at the same time as the transfer of digital content. This usually applies to temporary licensing for promotional purposes. For example, a temporary license specifying a three-time access for a piece of digital music could be pre-delivered with the media, allowing the consumer to listen to the music three times and then making decision to request and paying for a permanent license allowing unlimited accesses. Some companies offer 'try-before-buy' business model that directs the consumer to the clearinghouse where a permanent license can be purchased after the temporary license expires.

2.1.3 Plug-ins

Client-side applications, such as content viewers, players or readers, play a very important role in the DRM implementations, because they have to be able to enforce protection of digital content on the basis of licenses. Most DRM providers extend existing viewers without DRM functionalities through the use of plug-ins, which essentially makes those applications become integral components of DRM systems. In this approach, the content provider usually uses a special file extension to identify digital content protected by a specific DRM system. Through a particular plug-in, the content viewer opens and decrypts the digital content based on the usage rules in the license. However, each DRM system uses its own proprietary approach and there is no interoperability between application extensions and plug-ins at this stage. Digital content protected by one DRM system cannot be accessed by the client-side application in another DRM system. To access various digital content provided by multiple DRM systems, the consumer has to install different plug-ins and vendor-specific applications. We will look at how this problem affects user experience over the impact of DRM and possible solutions in sections 6 and 7.

3 Markets for DRM

Having understood the main components and the common process of DRM systems, it is also important to get a market overview for the current deployment of DRM in order to understand the impact of DRM on the content industry.

3.1 Existing Commercial Systems

Deployment of DRM is still at an early stage. There are a number of DRM solutions on the market. Generally speaking, we can obtain only limited information from various white papers on their web sites. Among these solutions, Microsoft's Windows Media Rights Manager (WMRM), IBM's Electronic Media Management System (EMMS), InterTrust's Rights|System, and RealNetworks's RealSystems Media Commerce Suite (RMCS) are the most promising ones at the time of writing.

3.1.1 Microsoft WMRM

WMRM (Microsoft 2002a) is an end-to-end DRM system for the secure distribution of multimedia files. It is an SDMI[3]-compliant solution based on Windows Media Player and Server. The system only supports Microsoft's proprietary WMA (Windows Media Audio) and WMV (Windows Media Video) formats. Both server and client Software Development Kits (SDKs) are available to develop customised DRM solutions. The supported business models can be subscription, sales, counted operations and secure transfer of protected digital media files to SDMI portable devices or media.

The main advantage of WMRM is that the Windows media format is widely used on the Internet and the Windows media player has already incorporated DRM support. PressPlay, a large online music service company, uses WMRM technology (Microsoft 2001) to offer digital music from Sony, Universal, EMI and many independent labels. The main difference from other music service providers is that PressPlay allows the consumer to burn the music onto CDs (CNET 2002).

3.1.2 InterTrust Rights|System

Rights|System (InterTrust 2002) offers a solution for content packaging, distribution and rights management based on a packager program and rights server technology. This system supports pay-per-use, rentals, sales, and try-before-buy business models.

System clients are not only for desktop PCs, but also for mobile phones, set-top boxes, and music players. Examples of supported applications are Adobe Acrobat for documents, MusicMatch for music, and MPEG-4 players for video. There are toolkits for independent software vendors and media player developers to integrate InterTrust's DRM technology into their products.

Nokia has selected InterTrust as its preferred DRM technology for the mobile content distribution (Nokia 2001). InterTrust has recently gone through a downsizing, reducing its staff by 70 percent and removing its products from the market. A new license agreement with Sony (Duhl 2002) has been made so InterTrust may survive on licensing fees and ongoing royalties from sales of Sony's products that incorporate its DRM technology.

3.1.3 IBM EMMS

EMMS (IBM 2002a) was developed for the preparation and secure distribution of all forms of digital content. It supports the goal of SDMI. The supported business models can be pay-per-use, pay-per-time, subscription, controlled printing, and protected transfer to portable devices and portable media.

Currently EMMS only supports Windows platforms. An EMMS-enabled player called "Madison Player 1.0" has been distributed since the beginning of August 2001 and an SDK for the player is available.

EMMS is mainly used in Japan for online music distribution. There are a number of web sites (IBM 2002b) selling digital music using the EMMS in Japan. IBM has strong ties with Sony for mobile content distribution. EMMS has been used in one of the most famous mobile distribution services – DoCoMo's M-stage music service in Japan.

3.1.4 RealNetworks RMCS

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

RMCS is currently utilized by MusicNet (MusicNet 2001), a joint venture of RealNetworks, AOL Time Warner, Bertelsmann AG, EMI Group and Zomba. MusicNet is offering digital licenses for a music subscription service for the four record labels and its music format is bound to the Real format. Both AOL and RealNetworks (RealOne) have launched a MusicNet - based service (Hansen and Hu 2001).

[3] SDMI: Secure Digital Music Initiative is a forum to bring music and technology companies together to develop voluntary standards for digital security and interoperability. http://www.sdmi.org/.

3.1.5 Other DRM Providers

Apart from the above major DRM providers, there are many other companies delivering DRM solutions including Adobe (www.adobe.com), IPR Systems (iprsystems.com), Liquid Audio (liquidaudio.com), Alchemedia (alchemedia.com), Digital World Services (dwsco.com), ContentGuard (contentguard.com), SealedMedia (sealedmedia.com) and many more.

3.2 Potential Markets

Current DRM solutions are mainly used for the online music services and eBook[4] publishing on PC-based platforms, but we should also realize that the potential future markets for DRM are varied.

- DRM systems can be used for e-health to protect patient's privacy. To securely store and transfer personal medical information over open networks, a DRM system for rights access control is necessary. For example, it may be the case that doctors, pharmacists and nurses are required to have different rights to access and modify information.
- In an online learning and information environment, DRM can facilitate trade and exchange of learning objects between institutions such as universities and colleges on a free or fee basis. Universities and other tertiary institutions have held hundreds of thousands of learning objects, many of which are useful to other teaching institutions as well. Promoting the exchange and re-use of quality learning objects, while respecting and rewarding the intellectual property of the various contributors, are the two key issues which have to be solved before online learning can become cost effective (IPR and Macquarie 2002). A flexible and effective DRM solution can manage the creation, retrieval, trading and distribution of online learning objects and support collaborative development.
- Similar to a document management system on the corporate intranet, a DRM system could be used within a corporation to guarantee that only authorized people can access certain information and prevent employees from disclosing critical and proprietary information to the company's competitors, e.g. Alchemedia's Mirage System (Alchemedia 2002).

4 Security in DRM

This section focuses on the security measures deployed in current DRM implementations. General requirements for security in DRM systems are explained first. Next an analysis of the security model in DRM is given. Then we take a look at various security technologies and solutions used for DRM.

4.1 General Requirements

A DRM system requires persistent content protection, meaning that protection has to stay with the content. For example, a digital movie can be delivered securely over the Internet using standard cryptographic mechanisms. But if the recipient can save and copy the content in an unrestricted form and put the digital copy onto the Internet, many people in the world can download the movie without reduction in quality. Therefore, the required security level in DRM systems goes beyond simply granting digital licenses to authorized users. More importantly, restrictions of the content usage rights have to be maintained after the content is delivered to the end user.

Essential security requirements in DRM systems include data protection to protect against unauthorized interception and modification, unique identification of recipients to enable access control for the digital content, and effective tamper-resistant mechanism to process protected data and enforce content usage rights.

4.2 Trust Model

The DRM trust model is different from the simple cryptographic model where two trusted parties who own a shared secret key are exchanging encrypted information and an attacker sitting in between tries to intercept and recover the data. In DRM, one communication party (the end users) cannot be trusted with a shared secret key or even unencrypted data. Internet provides an open distribution channel for consumers who wish to share their digital content with their friends. In the DRM trust model, it is not possible to separate honest and dishonest users.

Malicious users (crackers) may break the security system to make a profit through selling cracked software and digital assets. Once the protected content is delivered to the user's device, an attacker has a chance to break the system with unlimited time and resource. Although average users normally do not have the interest or skill to attack the system, one hostile user/hacker with enough motivation and hacking skills is sufficient to drastically affect effectiveness of the system. If the attacker can encode his break into software and publish his attack on the Internet, anyone can get access to the tool, download it and defeat the protection scheme.

4.3 Cryptographic Mechanisms

Many DRM systems are built on various cryptographic solutions that have been studied and developed for many years. To summarize, the following subsections present some of the cryptographic primitives that are commonly used in DRM systems.

4.3.1 Symmetric and Asymmetric Encryption

To prevent illegal copying of digital content, the content is generally encrypted using a symmetric key algorithm. Most DRM providers keep their encryption process and algorithm details confidential. This is "security through obscurity" which is contrary to the basic Kerkhoff's

[4] eBook: a book that is published or transcribed into digital form. eBooks are downloadable and readable versions of books.

Principle (Internet Solutions 2001). However, a number of companies have announced that they employ well-known cryptographic algorithms for content encryption, such as InterTrust and MediaSnap (mediasnap.com) who say they use the Advanced Encryption Standard in their DRM solutions. Compared with standard implementations of cryptographic algorithms, non-standard implementations of such algorithms are not as trustworthy, and probably, not as efficient (Stamp 2002).

Asymmetric encryption is based on the usage of key pairs – public key and private key that are mathematically related so that data encrypted with one key can only be decrypted with the other key. The digital license containing the content decryption key must be encrypted using the public key of the receiver. Therefore, only the party holding the correct private key can decrypt the content key and get access to the content.

4.3.2 Digital Signatures and One-way Hash Functions

In DRM systems, digital signatures are usually used for non-repudiable rights issuing. The clearinghouse should digitally sign licenses of the digital content. Therefore, the player application on the consumer's device can verify the correctness of the usage rights and keep the signature as a proof of rights purchase.

One-way hash functions combined with digital signatures are used for integrity checking. For example, the clearinghouse uses its private key to sign the hash value of the encrypted content rights. Integrity verification of the license is through decrypting the signature using the public key of the clearinghouse and then comparing the hash value with a re-computed hash value.

4.3.3 Digital Certificates

Digital certificates are used to authenticate or verify the identity of the parties involved in the system. In DRM systems, it is essential to use this mechanism to ensure that the packaged digital content is from the genuine authorized content distributor. The certificates of fake packaging applications should be revoked to limit the damage they can cause.

4.4 Individualization

Most current DRM solutions rely on unique identification of user devices. Each license is bound to a unique playback device, so the license stored in one device cannot be transferred or used by another device. To illustrate how this works, we use the example of the individualization process in Microsoft WMRM:

An individualized Windows Media Player is one whose DRM component has been individualized, which is like receiving a security upgrade (Microsoft 2002b). Content providers may require their digital content to be played only on the player that has been individualized. During individualization process, Microsoft Individualization Service generates a unique DLL[5] that is bound to the client computer using its hardware ID[6]. Once the player has been individualized, a public/private key pair is generated. The private key is stored in the DLL file that is generated in the individualization process. The corresponding public key is used as the player's identifier when requesting a license and the clearinghouse will encrypt the license using this key. If the player is moved to another host, it will require another individualization, because there is no corresponding DLL file binding to the new host. The license granted by the clearinghouse is not transferable or usable on another computer.

In the context of DRM, individualization can reduce the damage caused by system cracking, because if the DRM module on a user's computer is compromised, only that terminal is affected. However, it introduces another problem concerning the portability of rights: When the user wants to watch the movie at his friend's place or listen to the music on his portable devices (PDAs, mobile phones, portable players, etc.), he has to acquire new licenses for every device to enable content consumption. To reduce the impact of digital licensing process on the user experience, some DRM solutions allow users to back up their licenses and restore to another computer. To prevent abuse, users can only do this a fixed number of times.

4.5 Digital Watermarking

A digital watermark is an imperceptible signal that can be inserted into digital content for a variety of purposes, including captioning and copyright control. An important property of watermarks is robustness to common signal transformations such as file filtering and compression, and resistance to tampering (Cox and Miller 1997).

In DRM systems, watermarks can be used for binding information to digital content, such as content owners, the buyer of the content and payment information. They should be recoverable by special watermark-reading software to check content copyright and determine royalty payments. Watermarks can also be used forensically to trace digital pirates. Many companies provide a web spider service that routinely searches the web and tests for digital files that have been watermarked. The purpose of this service is to detect violations of copyright for registered content owners. Once the copyright violation is detected, content owners will be notified and the infringer will be likely taken to court.

Moreover, watermarks can be used for data annotation and access control. These watermarks are called annotation watermarks (Dittmann, Wohlmacher and Ackermann 2001). For example, the usage rule defining the allowable number of secondary copies and playbacks

[5] DLL: a Dynamic Link Library (DLL) is a collection of small programs that can be called by a larger program running in the computer.

[6] Hardware ID: a unique identifier of a computer, a kind of serial number.

can be embedded as annotation watermarks in every copy of the content. The control of content usage is enabled through the user's player application. When the digital content is accessed in a compliant user device, the user's player application counts annotation watermarks, checks the usage restrictions and updates watermarks as required. If the amount of annotation watermarks does not comply with the counting usage, the user's device will not perform the request. The major advantage of using annotation watermarks is that it binds usage rights with digital content no matter where the content travels.

Another application of watermarking is in the 'try-before-buy' business model, which allows the user to access watermarked digital content in inferior quality for evaluation and then make a decision to buy the content. The digital content will not be rendered in the original quality until the payment is done.

Current watermarking technology is imperfect. There is no standard watermarking solution in real applications. The robustness of many watermarking systems is not very satisfactory. The majority of copyrights marking schemes in the literature are vulnerable to attacks (Petitcolas, Anderson, and Kuhn 1998). The current state of watermarking technology is such that if an attacker knows the watermarking technique, he can almost certainly mangle the watermark beyond recognition (Stamp 2002). It is possible for a hacker to remove the content usage restrictions and add additional usage rights for himself. Therefore, merely applying watermarking technologies to the DRM solution may not be secure enough to meet the commercial requirements.

4.6 Tamper Resistance

Tamper resistance systems protect trusted software running on a malicious host. In DRM, content providers must deliver digital content across hostile networks to host platforms where end users cannot be assumed to be trusted. Rights enforcement software executes in a hostile environment, taking control of how the content is used, by whom and under which conditions. To prevent malicious users from tampering with rights entitlement functions of the DRM-enabled applications, it is essential to employ tamper resistance technology to make hacking extremely difficult and ensure that the DRM client can be trusted to perform as designed. The following subsections present both software based and hardware based tamper resistant approaches for DRM systems.

4.6.1 Software Based Technologies

Software based technologies rely only on software mechanisms to defend against tampering. Some common software based approaches include code obfuscation (Chang and Atallah 2001) in which the software is transformed into a functionally equivalent form which is difficult to understand and analyze, code encryption (Sander and Tschudin 1998) that prevents hackers from seeing and accessing the software, and self-modifying code that generates other code at run time. Cloakware for example, a non-DRM company focusing on tamper resistant software technologies, claims that it has developed a highly reliable new code transformation technology that can be embedded into DRM systems (Cloakware 2002). This technology uses a one-way program translation tool to transform each program into a unique tamper resistant instance of the program. This feature is especially important for DRM systems, because if each instance of a particular DRM application is unique from the other, it will be very hard for an attack to succeed against all instances of the software.

Another possible approach to ensure tamper resistance is for the software to require taking control at the operating system (OS) level. For example, to prevent a screen capture program from capturing unencrypted data on the screen, DRM systems can employ anti-screen capture method that operate at the OS level to disable unauthorized attempts (Alchemedia 2002).

4.6.2 Hardware Based Technologies

Hardware based technologies rely on secured hardware devices for protection. The hardware-based DRM approach is to provide a hardware trusted space, the execution space protected from external software attacks, for hosting protected content and in which only approved applications can execute. DRM services such as content decryption, authentication and rights rendering take place only in this trusted space.

For example, Microsoft is currently developing the "Palladium" architecture for trusted computing in future versions of Windows (Microsoft 2002c). While Microsoft says that DRM is not Palladium's stated purpose, the "Palladium" architecture provides a trusted environment upon which a DRM system could be implemented. In this proposed architecture, the nexus, a component of the Windows kernel running in trusted space, is in charge of booting and maintaining trusted space and authenticating user applications that need to run in trusted space. Every machine has a unique embedded private key in hardware and never exposed. This secret hardware key will be used to encrypt data within the trusted space. "Palladium" will offer a way to protect DRM applications against snooping and modification by other software and ensure that only software trusted by the person granting access to the content or service has access to the enabling secrets (Microsoft 2002d). However, some people fear that they will completely lose control of their computers and are concerned that Microsoft could use Palladium to exert monopoly control over the desktop and the IT industry. Whether "Palladium" itself is secure and whether Microsoft will eventually succeed is a very complicated economic issue. Microsoft recognizes that industry support will play a big role if Palladium is to ever succeed and plans to develop "Palladium" as a collaborative consumer and industry initiative (Manferdelli 2002).

4.7 Self-protecting Container

Another security mechanism used by DRM systems is Self-protecting Container technology. A self-protecting container is a cryptographic carrier of the electronic information or content that uses encryption, digital signature and digital certificates to ensure data confidentiality and integrity. Both IBM and InterTrust use this technology as the key element in their DRM systems to prevent unauthorized access to the protected digital content. The secured container DigiBox in the InterTrust DRM system associates rights management components with digital content via cryptographic means. To make the protected content available according to its associated access control rules, the DigiBox needs to be manipulated by a trusted rights protection application. The Cryptolope technology that IBM research team developed in 1996~1998 provides similar functionality (Kaplan 1996). Self-protecting Container technology can support almost any network topology and any number of system participants and offers flexible rights control, so it is considered as a true super-distribution means (Yan 2001). To enable deployment of this technology, it is required to have a secure environment for the container processing. Therefore, pervasive deployment of tamper-resistant technologies is necessary.

5 Legal Issues

This part will describe the current legal situation in the domain of DRM, focussing on the US Digital Millennium Copyright Act (DMCA), the US Security Systems Standards and Certification Act (SSSCA), the European Union Copyright Directive (EUCD) and the Australian Copyright Amendment (Digital Agenda) Act 2000.

5.1 Digital Millenium Copyright Act (DMCA)

The Digital Millennium Copyright Act (DMCA), passed in 1998, is an American law implementing the World Intellectual Property Organization (WIPO) Copyright Treaty and Performances and Phonograms Treaty (WIPO Treaties) (Harvard 2000). DRM is backed by the DMCA. Any attempt for the creation and distribution of DRM circumvention tools even for legal reasons may violate federal law under DMCA. Several legal cases attracting a much attention were:

- The arrest of Dmitry Sklyarov, a Moscow graduate student, for defeating a DRM system used in Adobe's eBook Reader (EFF 2001).
- The lawsuit threatened against a research team led by Professor Ed Felten for breaking a DRM system developed by the Secure Digital Media Initiative (SDMI) (Greene 2001a).
- The court case against 2600.org, an open source software forum, for posting a program 'DeCSS' to decrypt the content of DVDs (Stevenson 1999).

Many people claim that DMCA stifles innovation and academic freedom (ACM 2001) and is a threat to open source software development. A lot of disputes are going on whether the DMCA should be altered to guarantee free speech.

5.2 Security Systems Standards and Certification Act (SSSCA)

The Security Systems Standards and Certification Act (SSSCA) is a draft bill for a US law, being developed by Senators Fritz Hollings and Ted Stevens with the assistance of the Walt Disney Company. The bill would require hardware manufactures of any digital data processing devices such as PCs, portable music players, mobile phones, digital cameras and a lot more with a microprocessor to build in DRM functionality, including copy protection, into their products. Anyone in U.S. who produces, imports or provides digital devices without built-in DRM would be breaking the law.

If the bill passes, it would not only influence hardware manufacture but also concern software applications and operating systems in America. The user is no longer allowed to modify the software running on his computer or capture the digital content on the path from storage to the screen or speakers. Moreover, it would impose a heavy burden on the manufacturers as a consequence of the additional requirement of the system. Many vendors are worried that the increased prices and the complexity of the system will drive people away from new equipments with copy protection built in.

5.3 European Union Copyright Directive (EUCD)

The European Union Copyright Directive (EUCD) is a directive for implementing the WIPO treaties in the European Union member states into national law. If the current directive were passed without modification, it would be a criminal offence to break or attempt to break the copy protection or DRM systems on digital content. The main concerns raised by the EUCD is that it could prevent teachers copying materials for their students and prohibit academic research on security issues of an operating system or a protection mechanism. In order to develop playback tools, developers would be forced to sign licenses with the creators of a format, because it is illegal for any circumvention of copyright protection mechanism. Critics argue that the EUCD is even more restrictive than US Digital Millennium Copyright Act (Leyden 2002).

5.4 Copyright Amendment (Digital Agenda) Act

In Australia, the Copyright Amendment (Digital Agenda) Act 2000 (DACA) is similar to the US Digital Millennium Copyright Act. The DACA introduces new criminal offences and civil remedies regarding the intentional removal and alteration of electronic rights management information, typically including details about the copyright owner, and terms and conditions of use of the copyright material. Manufacture, sales and dealing with unauthorized broadcast decoding devices will result in civil remedies and criminal sanctions unless such devices are for personal use. It is illegal to provide computer programs, or manufacture, sell, import or advertise devices designed to circumvent copyright protecting measures. The exceptions to this include the reproduction of computer programs to make interoperable products, to correct errors and for security testing, activities covered by libraries and archives exceptions, the use of copyright material for the Crown, and activities covered by the statutory licences for educational institutions and institutions assisting persons with a disability under Part VB of the Copyright Act.

6 Consumer Concerns

The following subsections present the major concerns raised by consumers about privacy, fair use rights and inconvenience of DRM.

6.1 Privacy and Anonymity

One of the major issues raised by DRM solutions concerns the protection of the user's privacy and anonymous consumption of digital content. The authentication process in the DRM system usually requires the user to reveal his identity to access protected content, which can help profiling user's preferences and monitor what content the user is consuming. DRM systems usually do this by assigning a unique identifier to the content player and attaching the user's personal information to it (EPIC 2002). For example, Microsoft Windows Media Player for Windows XP has an embedded globally unique identifier that can be used to track users. Each time the user requires access to digital content, the system captures a unique hardware identifier that directly links to the user's identity. Though authentication is necessary for current payment processes, the system should not be allowed to generate a link between the user's identity and different purchases. In the worst case, the system can even send collected user-specific information to marketing agencies without the user's permission. A good DRM solution should regard privacy protection and grant anonymous access to the digital content.

6.2 Fair Use

Fair use is the doctrine in US copyright law that exists as a defence for individuals who engage in an unauthorized use of protected content. Under the fair use doctrine, using digital content for purposes such as research, teaching with the exception of distance learning, criticism, review, or news reporting is not an infringement of copyright (Cornell 2002). Fair use allows the consumer to resell what he bought, or make a private backup copy for personal use. However, there are no clear rules defining fair use, which is usually decided by a judge on a case-by-case basis.

There is an increasing tension between DRM and proponents of fair use. Some people put forward criticism on the erosion of fair use in DRM, because DRM systems cannot incorporate fair use principles (Lohmann 2002). For instance, for digital content on the Internet such as research papers and articles, DRM may restrict the ability to save or print a copy for reference. This would be a major inconvenience for students or anyone conducting research. For those who buy DRM-protected content, some of them complain that their sense of ownership is diminished by built-in technical restrictions. For example, a consumer buys an eBook but can't read it on another computer. Another example is that a consumer buys a CD, but cannot convert it to MP3 format to listen to on his portable player. It should be the case that once the consumer owns the digital content, apart from the restrictions imposed by laws aimed at eliminating piracy, the content belongs to him and he should be able to do what he likes with it. "Beale Screamer", an anonymous hacker of Microsoft DRM version 2, was motivated by the restrictions of the traditional fair use rights in the Microsoft WMRM (Greene 2001b).

6.3 Usability

Current DRM implementations present some usability obstacles, especially platform restrictions on usage and plug-in requirements for users (Berry 2002). As explained in Section 2, existing DRM systems use their own proprietary player applications to protect digital content. If a user wishes to acquire digital content from multiple services using different DRM systems, he encounters a new set of requirements with each service and downloads various vendor-specific software in order to unlock the content protected by different DRM vendors. This inconvenience could certainly make the user annoyed.

7 Standards

As discussed in Section 6.3, the usability problem in current DRM implementations is caused by the deployment of non-standardized protection mechanisms. To guarantee wide acceptance and interoperability between different DRM systems, standard definition for different components of a DRM system is required. Using a standard DRM architecture and rights language, different DRM vendors can work together and end users will not be locked up into a particular DRM system.

Several organizations and initiatives are working towards the definition of standards, such as the Open Digital Rights Language Initiative (odrl.net), World Wide Consortium (www.w3c.org), Open eBook Forum (openebook.org), Secure Digital Music Initiative (www.sdmi.org), Internet Digital Rights Management (idrm.org), etc.

It seems that the progress by the Moving Picture Expert Group (MPEG 2001) is very promising. The MPEG term for DRM is "Intellectual Property Management and Protection" (IPMP). MPEG is currently working on an interoperable IPMP terminal architecture. The aim of this architecture is to allow multimedia content with different formats to be delivered and consumed on different vendor's terminals and protected by different vendor's IPMP tools. The fulfilment of this goal will enable more interoperability in DRM, which is crucial to an open multimedia infrastructure. At the end of 2001, MPEG issued a Call for Proposals for a Rights Expression Language[7] (REL) and Rights Data Dictionary[8] (RDD) for

[7] Rights Expression Language: a specification grammar for expressing rights and conditions associated with digital content, resources, and services.

the MPEG-21 Multimedia Framework. It was XrML (eXtensible Markup Language) from ContentGuard that was selected among the submissions. Some modifications need to be done to fully meet the MPEG-21 requirements.

8 Concluding Remarks

DRM is a multi-faceted new concept. We have described the architectures, underlying security primitives and implementations, laws and standards. Although DRM is still at an early development stage and is not widespread, it has drawn a lot of media attention and there are a lot of discussions going on whether and how it can succeed.

With well-designed system architecture and security technologies, DRM seems to be good news for content providers who want to develop digital services without fear of losing control over their valuable digital assets. However, to deploy a successful digital online service, it is not sufficient to apply cryptographic primitives and security measures to encrypt and distribute digital content online. Security technologies can certainly help raise the bar against circumvention of the system and make it more difficult to defeat the protection scheme. But the key factors that determine successful deployment of the new services do not depend on security alone. The essential question is: Will the consumer be willing to play by the rules? Criticisms about DRM's inconveniences, incompatible platforms and dilution of fair use rights raise alarm that a restrictive and complicated DRM system may not be valued by consumers. To encourage consumers to buy digital content online and accept the new services, the content industry needs to invent an attractive business model that is easy to use with fair pricing and respect for consumers' rights. Security technologies need to follow such models accordingly.

Government intervention by changing laws to back DRM is also important to prevent large-scale illegal distribution. The court ruling to shut down Napster's illegal distribution system is a good example (Lara 2000).

Through our review, we can forecast the development trend of DRM based on what is happening and analyse the criteria for success. However, only the future can tell us whether this new concept will win eventually.

9 References

ACM (The Association for Computing Machinery) (2001): Computer Professionals Concerned DMCA Stifles Academic Freedom And Speech. http://www.acm.org/usacm/copyright/DMCA-release.html.

Alchemedia (2002): Technology Benefits. http://www.alchemedia.com/benefits/technology.html.

Attorney-General's Department (2000), Copyright System: Copyright Amendment (Digital Agenda) Act 2000, Australia Law Online. http://law.gov.au/publications/copyfactsheet/copyfactsheet.html.

Berry, M. (2002): That's What I Want - Developing user-friendly DRM. CMP Media's New Architect. http://www.newarchitectmag.com/documents/s=2452/new1011653160573/.

Chang, H. and Atallah, M.G. (2001): Protecting Software Code By Guards. ACM Workshop on Security and Privacy in Digital Rights Management 2001. Pennsylvania, USA.

Cloakware Corporation (2002): Protecting digital content using cloakware code transformation technology. Cloakware Whitepapers. http://www.cloakware.com/resources/.

CNET Networks Inc. (2001): Researchers weigh publication, prosecution. http://news.com.com/2100-1023-271712. html?legacy=cnet.

CNET Networks Inc. (2002): Pressplay - Software Reviews. http://www.cnet.com/software/0-3227898-1204-8494686.html.

Cornell Law School (2002): Title 17 – Copyrights, Chapter 1 – Subject Matter And Scope of Copyright, Sec. 107 - US Code Collection. Legal Information Institute. http://www4.law.cornell.edu/uscode/17/107.html.

Cox, I.J. and Miller, M.L. (1997): A review of watermarking and the importance of perceptual modeling. Proc. of Electronic Imaging 97, February 1997. NEC Research Institute.

Dittmann, J., Wohlmacher, P. and Ackermann, R. (2001): Conditional and User Specific Access to Services and Resources using Annotation Watermarks. Communications and Multimedia Security Issues of The New Century. pp.137-142. Ralf Steinmetz, Jana Dittman and Martin Steinebach (eds). Kluwer Academic Publishers.

DRM Watch (2002): GiantSteps Media Technology Strategies. http://www.giantstepsmts.com/DRM%20Watch/sssca.htm.

Duhl, J. (2002): Content Management and Retrieval Software - Sony licenses InterTrust's DRM: What does it mean? http://www.intertrust.com/main/images/home/idc.pdf.

Duhl, J. and Kevorkian, S. (2001): Understanding DRM Systems, An IDC White Paper. http://www.intertrust.com/main/research/whitepapers/IDCUnderstandingDRMSystems.pdf.

EFF (Electronic Frontier Foundation) (2001): FBI Arrests Programmer in Las Vegas. http://www.eff.org/IP/DMCA/US_v_Elcomsoft/20010717_eff_sklyarov_pr.html.

EPIC (Electronic Privacy Information Center) (2002): Digital Rights Management and Privacy. http://www.epic.org/privacy/drm.

Greene, T.C. (2001a): SDMI crack team launches preemptive suit. The Register, UK. http://www.heregister.co.uk/content/archive/19555.html.

[8] Rights Data Dictionary: a dictionary of key terms that can be used by REL to describe rights.

Greene, T.C. (2001b): MS digital rights management scheme cracked. The Register, UK. http://www.theregister.co.uk/content/4/22354.html.

Hansen, E. and Hu, J. (2001): RealNetworks plugs in MusicNet. CNET News.com. http://news.com.com/2100-1023-276549.html?legacy=cnet.

Harvard Law School (2000): Digital Millennium Copyright Act. The Berkman Center for Internet & Society. http://eon.law.harvard.edu/openlaw/DVD/dmca/.

IBM (2002a): Electronic Media Management System (EMMS). http://www.ibm.com/software/emms.

IBM (2002b): Electronic Media Management System (EMMS) - Success stories - IBM Software. http://www-3.ibm.com/software/data/emms/success/.

Internet Solutions (2001): Cryptography. http://www.tml.hut.fi/Opinnot/T-110.401/2001/Luennot/titu20011114.pdf.

InterTrust Technologies Corp. (2002): Technology - Rights|System. http://www.intertrust.com/main/technology/index.html.

IPR Systems Pty Ltd and Macquarie University (2002): Digital Rights Management in the Higher Education Sector. Evaluations of Investigations Program Higher Education Group.

Kaplan, M.A. (1996): IBM Cryptolopes, SuperDistribution and Digital Rights Management. http://www.research.ibm.com/people/k/kaplan/cryptolope-docs/crypap.html.

Lara, A. (2000): Napster Shut-Down? The File-Sharing FAQ. ZDNet Music. http://www.zdnet.com/products/stories/reviews/0,4161,2609080,00.html.

Leyden, J. (2002): Alan Cox attacks the European DMCA. The Register, UK. http://www.theregister.co.uk/content/4/25088.html.

Lohmann, F.V. (2002): Fair Use and Digital Rights Management: Preliminary Thoughts on the (Irreconcilable?) tension between them. Electronic Frontier Foundation. http://www.eff.org/IP/DRM/cfp_fair_use_and_drm.pdf.

Manferdelli, J. (2002): Q&A: Microsoft Seeks Industry-Wide Collaboration for "Palladium" Initiative. PressPass. http://www.microsoft.com/PressPass/features/2002/jul02/07-01palladium.asp.

Microsoft Corporation (2001): Microsoft and pressplay Team to Deliver Cobranded MSN Music Subscription Service. PressPass. http://www.microsoft.com/presspass/press/2001/Jul01/07-12MSpressplayPR.asp.

Microsoft Corporation (2002a): Microsoft DRM Offering. http://www.microsoft.com/windows/windowsmedia/wm7/drm/offering.asp.

Microsoft Corporation (2002b): Microsoft Media Rights Manager SDK. http://msdn.microsoft.com/library/default.asp?url=/library/enus/wmrm/htm/requiringindividualizedplayers.asp.

Microsoft Corporation (2002c): Microsoft "Palladium": A Business Overview. PressPass. http://www.microsoft.com/PressPass/features/2002/jul02/0724palladiumwp.asp#aspect.

Microsoft Corporation (2002d): Microsoft "Palladium" Initiative Technical FAQ. PressPass. http://www.microsoft.com/PressPass/features/2002/aug02/0821PalladiumFAQ.asp.

Microsoft Digital Media Division (2001): Security Overview of Windows Media Rights Manager. http://www.microsoft.com/windows/windowsmedia/wm7/WMRM_security.pdf

MPEG (Motion Picture Experts Group) (2001): MPEG-21 Working Documents (IPMP Part). http://mpeg.telecomitalialab.com/working_documents.htm

MusicNet (2001): Digital Rights Management (DRM) Software. http://www.musicnet.com/ policy10.html.

Nokia (2001): Nokia Selects InterTrust's DRM Technology And Acquires 5% Stake. Press Release. http://press.nokia.com/PR/200102/806790_5.html.

Petitcolas, F.A.P., Anderson, R.J. and Kuhn, M.G. (1998): Attacks on Copyright Marking Systems. David Aucsmith, Ed., Second workshop on information hiding, in vol. 1525 of Lecture Notes in Computer Science, Portland, Oregon, USA, pp. 218-238.

RealNetworks, Inc. (2001): RealSystem Media Commerce Suite Technical White Paper. http://www.realnetworks.com/products/commerce.

Sander, T and Tschudin, C. F. (1998): Protecting Mobile Agents Against Malicious Hosts. In G. Vigna (ed.), Mobile Agent Security, LNCS.

Sonera Plazza Ltd MediaLab (2002): Digital Rights Management White Paper. http://www.medialab.sonera.fi/workspace/DRMWhitePaper.pdf.

Stamp, M. (2002): Digital Rights Management: The Technology Behind the Hype. Cupertino, CA. http://home.earthlink.net/~mstamp1/papers/DRMpaper.pdf.

Stevenson F. (1999): Cryptanalysis of Contents Scrambling System. http://www-2.cs.cmu.edu/~dst/DeCSS/FrankStevenson/analysis.html

Suzuki, H. (2002): Sony innovation guards content. Australian IT. http://australianit.news.com.au/articles/0,7204,4874591%5E16681%5E%5Enbv %5E,00.html.

Waeber, E. (2002): Protecting digital music using DRM: example of a mobile service over WLAN (version 1.0). Swisscom CT-MMS, Switzerland.

Yan, Z. (2001): Mobile Digital Rights Management. Nokia Research Center. In Telecommunications Software and Multimedia TML-C7 ISSN 1455-9749.