Digital Rights (Mis) Management

Mukul Pahwa
CompSci. 725, University of Auckland
mpah004@ec.auckland.ac.nz

Abstract

Digital Rights Management Systems are being used extensively by enterprises selling intellectual property digitally to harness the full potential of the global market with the advent of the internet. While increased digital sales are indicative of success in deploying such systems, piracy still remains rampant. This paper presents a review of the current DRM systems with an aim to provide better understanding of their limitations, especially with respect to a different cultural, economic and legal background such as in India.

1. Introduction

Piracy has forever been a major concern for the entertainment industry. The availability of intellectual property on the internet has fuelled illegitimate copying, usage and even sales. Even though there has been recent success in hindering piracy, it is still rampant in countries such as India, Pakistan, China and Russia.

Unlike in the US, where a decline of CD/DVD sales can be rightfully attributed to online file sharing, revenue losses to the industry are not directly due to sharing of files by millions of users on p2p networks in India, but more from sales of illegitimate CDs and DVDs. Only a very small population can afford to pay $20 a month for a no-limit 256K broadband connection on top of a $1000 priced computer to use such services online. Instead, it is fairly easy to find CDs containing at least 150 mp3 tracks and DVDs with 3 to 5 films priced at the

equivalent of $1 and $3 respectively. $15-$20 for a CD and even more for a DVD are very high prices in a country where 25% of the population is below the poverty line, and per capita income compared to the western countries is much lower [10] add to the cause of piracy as well.

It is apparent that the way films and music are sold and consumed are different, but with increasing bandwidths, better compression and larger storage capacities, movies are following the trail of music. The industry is working extensively to improve DRM systems and business models to provide users more incentive to turn legitimate (online). DRM systems might prove successful in countries such as the US, UK, Japan to convert p2p file sharers into legitimate buyers but they aren't tackling the kind of piracy in the "top problem" [2] countries where file sharing does not play as big a role and affects the industry's revenues far more. A lot of focus has been on banning services such as Napster, Grokster and the like, while a lot more needs to be done to stop physical piracy. Technological advancements for content protection, global legal implications and probably a less capitalistic approach to creative artworks might prevent billion dollar losses from a trillion dollar industry.

The aim of this paper is to review the limitations of DRM systems and technology in use nowadays. While DRM systems serve to protect intellectual property in any digital format, most of the focus has been on safeguarding material on the internet presumably due to its global reach. While the Internet can only support digital content, digital content is not solely dependent on the internet. I hope to highlight the difference in piracy on the internet and piracy through physical copies. Section 2 introduces DRM systems and discusses issues such as flexibility, legal dependence and privacy that are contingent to the success of these systems. Section 3 gives a brief overview of the technologies that DRM systems use, such as watermarking and cryptography with an aim to present their limitations. Finally in section 4, a conclusion and some recommendations that might lead to an overall success in eradicating piracy are given.

2. Digital Rights Management

It is important to understand what current DRM systems do and what they overlook. DRM refers to technical methods to control or restrict the use of intellectual property on electronic devices [4]. Any successful DRM system while ensuring persistent protection of digital information must be flexible enough to not conflict with the user's perceived rights. The DRM systems have undergone a lot of improvement in order to get accepted. According to Goedvolk et al. in [3] DRM systems impose several limitations and drawbacks with respect to the ease of the end-user in their perceived rights of portability and sharing. Initially DRM systems such as Pressplay, Rhapsody etc. were restrictive [1] and therefore rejected. iTunes by Apple has been quite a success for its "rip, mix and burn" flexibility it provides to its customers. DRM systems also have several privacy issues in that a consumer's anonymity is compromised. In this section I review the design of DRM systems, successes and drawbacks and how the issue of physical piracy is still ignored.

2. 1 Flexible DRM Systems – a bane or a boon?

Portability issues with DRM are linked to license keys (Pressplay) where users need to profile all computers they may subsequently use content on in order to get authenticated. License expiration used in other Microsoft DRM applications limits the use of content for a contracted period [1]. Another restriction is the lack of conversion into different types of media formats. Most DRM systems use their own proprietary approach and offer little interoperability between applications [4]. The lack of interoperability is due to reluctance by vendors to share secret keys and algorithms due to an obvious capitalistic approach to this business. Since the use of content is tethered down to proprietary players, the user suffers in complying with new requirements in order to gain portability. It is quite normal to purchase a cassette or CD and listen to the tracks at home, in the car, or at any other location, DRM systems that restrict these flexibilities will not be acceptable to the user.

People who buy music online expect the usual capabilities that offline purchased CDs offer, such as portability. According to Julie E. Cohen in [7], “DRM Systems impose direct restrictions on what individuals can do in the privacy of their own homes with copies of work they’ve paid for”. Rhapsody, Pressplay and MusicNet restricted users from CD burning, or transferring content when they were initially launched in 2001 [1]. Such systems were obviously rejected as the consumer was paying a similar price to obtain content that lacked the flexibility that is otherwise a norm. As a result by 2003, these systems incorporated burning and device transfer to enhance usability. The success of iPod along with iTunes is highlighted by the fact that it is not restricted to playing tracks bought from iTunes, it plays almost all music files (mp3 etc) whether purchased or shared (p2p networks). iTunes lets registered users buy a track at 99c and do what they like with it. Such systems have been embraced by a market where the consumers have enough money to buy music online and respect copyright (due to laws or other reasons) to not want to infringe upon it.

A 744% increase in paid-for-music downloads in the UK for the second quarter of 2005, compared to 2004 [9] and the fact that the digital music revenues worldwide have tripled in the first half of 2005 compared with 2004 [6] indicate success of DRM systems. This suggests acceptance of DRM systems and shows that the incentives offered by online services in the form of try-before-you-buy, portability and better pricing are successful in the online market.

However a completely different set of figures show the still unconquered growth of piracy that is not directly enabled through the use of internet. In 2005, the estimated loss of DVD piracy alone has been worth USD 3bn in the US, and about 1bn in the UK [8: Online News]. In 2003, according to [2], the global pirate music market from sales of pirate CDs was worth USD 4.6bn. Perhaps offering consumers permissions through flexible DRM is impeding a decrease in piracy. Flexibility is a great tool in one country to generate revenues from the online market. At the same time though, flexibility may kindle piracy even more in

another country where only a few people can afford to buy online, and then mass replicate the content to make profits through illegitimate selling.

2.2 DRM and Law

In the US, The Digital Millennium Copyright Act (DMCA) was passed in 1998. According to the DMCA, any "attempt for the creating and distribution of DRM circumvention tools even for legal reasons may violate federal law under DMCA" [4]. The European Union Copyright Directive (EUCD) and the Copyright Amendment Act 2000 (DACA) in Australia are similar measures to make copyright infringement using technology illegal.

There has been a lot of news recently about arrests in the UK and the US of illegal DVD manufacturers. The Federation Against Copyright Theft (FACT) seized 386,569 UK made DVD's from January to June this year [8]. In the US, legal action until now has been taken against 14,800 people for using file-sharing networks to illegally share music online [9]. On the contrary, more recently, a ruling by the High Court in Australia that chipping the console of PlayStation so that it can play imported games is not a breach of copyright law came as a big surprise to corporations, especially Sony.

The Legal systems play a very important role in the success of DRM. Unfortunately, in countries such as India, China, Ukraine etc. there are essentially no Intellectual Property (IP) protection laws [2] and DRM systems seem to be based on such legal bastions. Moreover, the limitations in the global implications of these laws where they do exist, are highlighted by the existence of websites such as Jon Johansen's, gloating of the 'hacks' and circumventions he has created for a number of protected technologies.

2.3 Privacy Issues

R. Mori in 1983, coining the concept of 'Superdistribution' [11], laid out nine provisions that an online economic model must ensure. One of them was anonymity of the people engaging in these transactions. More than two decades later, anonymity still remains an issue. The current DRM applications and the payment models such as credit card, digital cash etc. depend on knowing who the customer is. They depend on authentication of the user in order to allow access to protected content. Authentication is based on private details that are usually circumvented in purchasing such content physically.

Contrary to Ms Cohen's remark in [7] that copyright owners gain information on the activities of the individual users, it is the distributors that benefit from such information. Mulligan et al. in [1] conducted a study to analyze the DRM systems in 2003 and found that MusicNet and Rhapsody, both online film services read from the user's index.dat file and periodically contact their servers. They found that these services accessed these files for the cookies, history and temporary internet files folders. The information gained from such access is very valuable to the services in learning the user's interests for marketing and also very intrusive to the user's privacy. Given the technology available today, it seems unlikely that an end user can be trusted without registration. However, it is important to inform the consumers that such surveillance will take place during the use of services. Gathering interest and preference information of users is a new technology in itself, Case Based Reasoning Systems boast of being able to suggest to users what they might like.

Although the success of DRM systems is highly dependant on adherence to legal compliance, they appear to be violation of certain privacy laws. For example, in the US, The Video Privacy Protection Act mandates rental outlets (films) to destroy rental records "as soon as practicable" [1]. These outlets are barred from sharing records of customers with anyone other than government officials with a warrant. Online, the user's information can be shared among distributors or other

copyright owners for monetary or other gains and there seem to be no legal technicalities of such (mis) use.

Regardless of the shortcomings, consumers have come to accept such invasion of privacy due to lack of options. In a different culture, or country however, once people do begin to use credit cards and can afford to buy online, treading upon personal information may be completely unacceptable. This may add to resentment towards DRM systems, further contributing to their ineffectiveness.

3. Security Technologies for DRM

This section reviews the technologies used by DRM applications to safeguard digital content against malicious use. It is important to understand the limitations of technology, especially when it is built around business models instead of the other way around. Most technologies for content protection are based on watermarking and/or cryptography designed to protect content during and after online distribution.

Even though the internet provides an opportunity for an average user to indulge in illicit trade of copyright material [2], more sophisticated manufacturing plants and factories that require a sufficient investment are still responsible for the large scale production of pirated material. Huge revenue losses to the music and film industries, and never ending raids to seize fake [8] DVDs highlight the limitations of the present technology for securing content. The source for these factories is not limited to the internet. As Byers et al. in [5] point out there are a lot of loop holes within the film distribution process that enable access to such content.

3.1 Digital Watermarking

Digital watermarking is the technique of inserting an undetectable piece of data (unobtrusive) into the audio or video content. The watermark can contain information about the content owner, usage terms and conditions etc.

Watermarks do not stop a user from accessing the watermarked content unless the content is bound to an application that detects the watermark first. Since binding content to such applications would be restrictive to the end-user and may require new legislation to force manufacturers into installing such detection capability in their devices, watermarking is intended more to monitor the usage of content and enable the owners of the content to assert their rights. There are several kinds of digital watermarks, such as robust, fragile and annotation which are prone to subtractive, additive, distortive and collusive attacks [12].

A robust watermark is intended to stay intact after compression and decompression of the digital content. A fragile watermark on the other hand is one that is easily lost. Annotation watermarks contain information about the number of copies and playback permitted [4]. Even though annotation watermarks bind usage rights of the content permanently, regardless of where the content might be used, its success depends heavily on the playback device. Watermarks are also used for traitor tracing where any modifications to the watermark can be used to trace the consumer responsible. Again, this mechanism also depends on the playback device. Fingerprinting is a type of watermarking in that a distinct watermark is used on every single copy of the content [12].

The authors in [5] see watermarking as “short term mitigation” for addressing the vulnerabilities in the film distribution process. Even though pirated copies of films contain obtrusive watermarks that disrupt the experience while warning the viewers, consumers take it as part of the package for paying a relatively smaller price. Watermarking is a technology still under development and it seems that whenever watermarking can successfully trace traitors to thereby hinder piracy, it would need the backing of the legal system.

3.2 Cryptography

Cryptography is the exchange of information in a way that an unauthorized party cannot access it. A cryptography based technology protects content by licensing which enables the consumer to have access to keys [3]. Symmetric and Asymmetric Encryption, Digital Signatures and One-way hash functions and digital certificates are all cryptographic means of securing content. Symmetric encryption encrypts the content using a key which can then be decrypted with the same key. Asymmetric encryption differs in that there is a pair of keys, public and private (mathematically related) such that data encrypted with one key can only be decrypted using the other. Digital Signatures and One-way Hash Functions are used for rights issuing and integrity checking [4]. Digital Certificates allow authentication of the parties involved in the DRM system.

Even though encryption requires more computational power on the receiving devices, it is a widely used technique for securing content. However, encryption depends on the availability of the decryption keys on the playback device. The Content-Scrambling System (CSS) that was used on some DVDs is one of the biggest failures of encryption highlighting the limitation of such dependence. Jon Johansen along with two other European developers reverse engineered the CSS algorithm and through the internet distributed the DeCSS software. His trials and subsequent acquittal show the need of legal backing for any such content protection technology (it is legal under Norwegian law to make copies of films for personal use). Another example of how a relaxed legal system promotes piracy is the availability of “Open” DVD players in India. The significant advantage of these locally made, reasonably priced DVD players is that they can play any type of protected DVDs and are not restricted to regional settings. The choice made by consumers seems rather obvious when an original branded DVD player costs at least twice as much as its local counterpart.

Lastly, although encryption provides sophisticated protection for the delivery of content, the analogue hole is yet to be circumvented. The analogue hole is a

major vulnerability in copy prevention schemes. If music can be heard or a film be seen, it can be recorded. The quality of such analogized then digitalized copies is usually compromised but offer consolation to the end customer with a lower price.

4. Conclusion and Recommendations

This issue of piracy has two critical aspects to it. Firstly, illegal sharing of content through file-sharing on the internet continues while consumption of digitally available or physical content has dropped. And secondly, the people who could not afford to buy over priced music CDs and DVDs are now purchasing cheap, illegal bootleg versions of the same. DRM Systems focus on protecting content on the Internet whereas most people in economically lesser developed countries do not even use the internet to access music and films but buy bootlegs instead, still as easy or hard to create as they have always been.

In countries where there are Intellectual Property laws, they are not sufficient deterrents to hardened pirates of digital content. Some improvements as discussed in section 2.1 result more from better pricing and flexibility than from better legal support. There is a much needed improvement in business models, legal systems and of course, the technology to protect such valuable content.

The business models that use DRM systems seem to assume that every pirate is a potential buyer. Piracy has increased the consumption of intellectual property though profits have declined. Big labels have reduced marketing costs in countries such as China because it only brings about awareness of music and films which then lead to piracy [2]. This might only end up increasing the novelty of pirated content.

Since DRM systems depend on technology as much as legislation, technology improvements are very important. Digital watermarking and cryptography, probably since they are developed around the business models have several

shortcomings as discussed earlier. Although many corporations and universities ban the use of file sharing software, this restriction is easily circumvented with increasing email account and attachment sizes.

Perhaps, better pricing of legitimate copies of music and films will help defer piracy and convert the major revenue losses into smaller gains. Promotions such as added value need to be very region specific in order to entice consumers into buying legitimate copies. People in countries where piracy is most rampant need to be educated and informed of its implications. This step should be taken by the suffering industry instead of leaving it to other authorities. There need to be stringent laws that do not leave piracy to be an insidious crime. Maybe someday, piracy of digital content will cease to exist, and the trillion dollar industries can make trillion dollar profits.

.

5. References

[1] Deirdre K. Mulligan, John Han, Aaron J. Burstein, "How DRM-Based Content Delivery Systems Disrupt Expectations of "Personal Use"", in Proc. 2003 ACM workshop on Digital rights management, ACM Press, 77 - 89, 2003.
[2] Tsvi Gal, Howard M. Singer, Laird Popkin, "The IP War - Apocalypse or Revolution?", in Proc. 2003 ACM workshop on Digital rights management, ACM Press, 39-46, 2003.
[3] Ernst-Jan Goedvolk, Edward Faber, René W. Wagenaar, "Towards a framework for understanding the effectiveness of digital content exploitation strategies", in Proc. 6th ACM International Conference on Electronic commerce, 239 - 244, 2004.
[4] Qiong Liu, Reihaneh Safavi-Naini, Nicholas Paul Sheppard, "Digital Rights Management for Content Distribution", in Proc. Australasian information security workshop conference on ACSW frontiers Volume 21, Conferences in Research and Practice in Information Technology Series, Volume 34, 49 - 58, 2003.

[5] S. Byers, L. Cranor, D. Korman, P. McDaniel, and E. Cronin, "Analysis of security vulnerabilities in the movie production and distribution process", in Proc. 2003 ACM Workshop on Digital Rights Management, ACP Press, 1-12, 2003.
[6] BBC News - Entertainment (3rd October, 2005) [article online], "Digital Music Revenue 'triples'", available at http://news.bbc.co.uk/2/hi/entertainment/4304466.stm
[7] Julie E. Cohen, "Digital rights management and fair use by design", Communications of the ACM archive, Volume 46, Issue 4, ACM Press, 46 - 49, 2003.
[8] BBC News - Entertainment Film (12th September, 2005) [article online], "Fake UK DVD seizures up by 133%", available at http://news.bbc.co.uk/1/hi/entertainment/film/4237008.stm
[9] BBC News - Entertainment Music (30th September, 2005) [article online], "Legal action for 757 file sharers", available at http://news.bbc.co.uk/1/hi/entertainment/music/4298430.stm
[10] Nationmaster - India Profile (19th October, 2005) [online reference], "Economic Profile of India", available at http://www.nationmaster.com/country/in/Economy
[11] Ryoichi Mori, Masaji Kawahara, "Superdistribution: An Electronic Infrastructure for the Economy of the Future", Transactions of Information Processing Society of Japan Volume 38, Issue 7, 1465-1472, July 1997.
[12] Christian S. Collberg and Clark Thomborson, "Watermarking, Tamper-Proofing, and Obfuscation - Tools for Software Protection," IEEE Transactions on Software Engineering, Volume 28, Number 6, 1-13, June 2002.