Societal and Technological Aspects of Digital Rights Management

Brian McGuire David Coleman

1. Introduction

Digital content has a wide variety of applications and significant value to our society. It allows for faithful reproduction of works (i.e. DVD) and low cost or virtually free distribution (i.e. computer viruses). In most cases there is a need, usually from the content producer, to control the access to or use of this digital content. Digital Rights Management (DRM) is often defined in terms of specific applications, such as digital entertainment [47][35], and generally references electronic commerce or business models [47][35]. There is no requirement that a DRM system be a system that supports digital entertainment in an electronic commerce model. This is a bias that has been introduced by authors simply discussing these specific systems and uses instead of providing a more universal definition. In fact, one definition of a DRM system required a payment system to be a core function of a DRM system [27].

Additionally, protection of copyrights is often discussed as part of the definition or requirement for a DRM system [42]. Again this is too limiting of a definition as it restricts the functionality that might be available in the system and applied to the content as well as the domain in which it is used. There are several unique areas that DRM has been proposed for that do not involve copyrighted content.

A more general, and more useful, definition is a system that controls the uses of content. Such a system could clearly be useful for content distribution because limiting or prevent copying and preventing derivative works is well within the definition. Additionally, while payment is not clearly specified, there is nothing that prevents a content distributor using a system that falls within this definition from receiving payment in exchange for granting rights or uses of the content. Additionally, this definition opens up DRM systems to additional types of content.

There are 2 distinct domains in which the currently widely-used DRM systems fall into: consumer electronics and personal computers. As digital entertainment convergence continues to happen, with personal computers moving more and more into the realm of consumer electronics (over 40% of all computers sold with

Microsoft Windows pre-installed are Media Center Edition), the gap between these two domains narrows. In essence, even though content may be produced for CE uses, it needs to be accessible and useful in the computer domain as well. Many users today watch DVDs on their laptops and use their home computers as media servers to serve up music or movies to their conventional entertainment systems.

Most currently shipping DRM systems, and most systems that are useful, support the following requirements:

- Protecting the content from unauthorized use, generally through the use of encryption
- Different content manipulation operations such as: viewing, transferring to another device (or type of device), converting to a different format, transferring the right to use the content to another (reducing or removing the original access) .
- Validation that the content is valid via mechanisms such as digitally signing the content.
- Counters on operations above such as being able to view the content five times or copy it to a CD three times. Some of these counter properties are becoming rather elaborate and differentiating between copying an individual file to a CD vice copying a collection of files to a CD and having different counters for these two types of operations.
- Additional limits on the operations above, often allowing the content to expire after a given date or period of usage.

While the current DRM systems are primarily focused on the pay-for-content entertainment sector, there are several unique and interesting possibilities for a DRM system. Distribution and modification of sensitive, private information, such as medical records [35], is one example of a use of a DRM system to control access to content that is not entertainment related. In this case, the content is not copyrighted (although that is an interesting idea and maybe a novel method for protecting our privacy) and there's clearly no pay-for-access model that makes sense either. A system in which doctors are charged by the patient to access medical records is probably a short-lived product. Any type of sensitive information combined with some form of watermarking (often referred to as a DRM system or a component of a DRM system) would allow the owner of the information to control access as well as trace back to the source any problems of leakage. This type of system would clearly have a lot of value in today's environment of credit card fraud and identity theft.

Falling into the "traditional mold", this paper will primarily examine the current DRM systems that are primarily used for digital entertainment content distribution. We will not exclude CE DRM systems but will focus primarily on the PC systems as these have the largest interactions with privacy and cybersecurity. Additionally, copy protection of software programs definitely falls under the generalized description of a DRM system but will not be discussed. We will start with a look at the current legal environment of DRM, discuss privacy, security, and then some specific DRM technologies (including the Sony Rootkit).

2. Legal Aspects of DRM

Overview

DRM for digital entertainment distribution of content is designed around protecting the rights of the copyright holder while allowing the consumer to enjoy the content. The potential for pirating digital content is large and recent years have shown that these fears are not without merit. It is debatable how much financial impact piracy has had on the various entertainment industries that produce digital content and there really is no good way to accurately assess the impact, positive or negative, that it is had. But clearly, the copyright holders need the consumers to have the ability to consume and enjoy the content. Without a fairly reasonable user experience, the users will not pay their hard-earned dollars for it. So a balance must be struck. Some suggest that the goal is actually to reduce or remove any rights the consumer might have had so as to exploit the monopoly on content and create business models that do not exist for the purposes of exploiting the consumer [45]. While it is hard to divine the intent of the systems just from the functionality exposed (actually most DRM systems are not built by the content providers), in most cases there does seem to be a significant reduction of rights of the consumer with respect to copyrighted material.

Copyright Law

The Copyright Act of 1976 reserves the following rights for the copyright holders:

(1) to reproduce the copyrighted work in copies or phonorecords;
(2) to prepare derivative works based upon the copyrighted work;
(3) to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending;
(4) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly; and
(5) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display the copyrighted work publicly. [1]

Most DRM systems only address and attempt to protect rights 1-3 listed above. They usually effectively control how copies are made by encrypting the original content and either explicitly preventing copying altogether or limiting the types or number of copies that can be made. Preparing derivative works is almost always completely restricted as is distribution. The copyright holders and content distributors tend to reserve those functions exclusively for themselves. Generally, rights 4 & 5 above, which govern the public performance or display of the copyrighted work, are covered by the Terms of Use agreement(s) between the distributor and consumer and the consumer is prevented from performing these operations as well. Most of the popular DRM systems do a very good job of enforcing these rights. In the Windows Media DRM system, the ability to reproduce content is up to the producer and can be limited by a counter of operations allowed.

A conflict arises when DRM systems do such a good job of enforcing these rights that they conflict with the Fair Use provisions of the Copyright Act. This section defines certain actions that are considered to be non-infringing and depend heavily upon the context and intent in which the actions are performed. The operations allowed under Fair Use and the determining factors of Fair Use are:

> .. including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include--
> (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
> (2) the nature of the copyrighted work;
> (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
> (4) the effect of the use upon the potential market for or value of the copyrighted work. [2]

So there is an inherent conflict in copyright law between the rights of the copyright holders and the actions reserved by Congress for the consumers. Unfortunately, the consumer has very limited ability to challenge the DRM system(s) that might prevent their ability to effect the actions allowed under Fair Use. The most significant tool the consumer has is not a legal one but a financial one; they can vote with their pocketbook for the DRM system that most closely preserves they have come to enjoy with conventional copyrighted material.

Digital Millennium Copyright Act

The Digital Millennium Copyright Act (DMCA) was passed by Congress in 1998 for the purposes of further protecting copyright holders' rights [58]. There are several aspects to the DMCA, including implementing the World Intellectual Property Organization (WIPO) Copyright Treaty, protecting service providers against liability

for monetary damages or injunctive relief due to copyrighted material being distributed on their service (as long as they follow certain guidelines), exempting computer repair services, and protecting hull designs of boats. However, the largest impact relating to DRM system is contained in the anti-circumvention provisions [3]. These provisions outlaw producing a system that has the primary purpose of defeating a system that controls access to a protected work and only limited additional commercial value [4]. The DMCA leaves both the definitions of "primary purpose" and "limited commercial value" open to interpretation. These definitions seem to mirror the Sony Betamax decision where the court found that significant non-infringing uses existed for the technology, thus Sony would not be held liable for any actual infringing uses [52]. However, in MGM v. Grokster, the Supreme Court disagreed with 9th District Court and the Court of Appeals and found that whether or not a system has significant non-infringing commercial value doesn't necessarily eliminate the liability for infringement in all cases [37]. The court found that in this case the systems were in fact being intentionally produced, and used by users, for the purpose of infringing on copyrights. The systems were being used this way with the company's knowledge and blessing and marketing. In the Sony decision, one of the significant factors was the fact that the uses being advertised (recording content for time-shifting – watching it later) was argued by the studios to be an infringing use but was actually found to be a non-infringing use and protected by the Fair Use provisions. In the Grokster case, the systems were essentially being advertised to steal copyrighted material. The lower courts had applied the Sony decision because there are significant non-infringing commercial uses of the peer-to-peer technology. But because of the company's focus on using the system for distributing infringing material, even without their direct control, they were found liable for the infringements being perpetrated using their system. Thus, relying on the definition of primary purpose and additional commercial value is a dubious strategy and might not be strong enough to prevent liability under the DMCA.

DRM systems typically impose restrictions that prevent uses that would normally be classified as Fair Use, such as making backup copies of works, making copies of works for educational purposes, and others. In order for a user to perform those operations that are explicitly defined as non-infringing, the DRM system would have to be defeated. Even though there is text in the law about not conflicting with or preventing Fair Use [5], the courts have repeatedly ruled against circumventing DRM systems for the exercise of Fair Use [56][57]. Because of this, and the burden implied by the Grokster decision, many companies are wary of getting too close to the line of content manipulation tools that might allow users to infringe upon copyright holders' rights. Given that one of the largest

growing software markets is digital content manipulation tools, this is a delicate balance and a challenging one for companies to strike.

Other Legal Challenges

There are additional legal obstacles for users who attempt to exercise Fair Use or personal use [39]. The Computer Fraud and Abuse Act (CFAA) [6] and state theft of services also might apply to certain situations. However, these laws are beyond the scope of this paper because they either cover an intent to defraud with fairly extreme dollar damage minimums or are state-specific. The European Union also defined their own version of the DMCA, the EU Copyright Directive (EUCD), which again is beyond the scope of this paper. Because it is conceivable that users attempting to exercise their "rights" could run afoul of these laws they did warrant mentioning.

There currently are competing bills being considered (repeatedly) in Congress, one of which further restrict users' rights and another which attempts to more strongly codify users' rights. These are the "Super DMCA" and the Digital Media Consumer Rights Act respectively. They will be discussed further in the Future of DRM section.

Conclusion

There is an inherent conflict in copyright law between the rights of the copyright holders and the actions reserved by Congress for the consumers. The DMCA, instead of clarifying or mitigating this conflict, simply added to the tools the copyright holders have. Unfortunately, the consumer has a very limited ability to challenge the DRM system(s) that might prevent their ability to effect the actions allowed under Fair Use without incurring substantial legal liability, both civil and criminal. The most significant tool the consumer has is not a legal one but a financial one; they can vote with their pocketbook for the DRM system that most closely preserves the rights they have come to enjoy with conventional copyrighted material. Content with fewer restrictions attached should have a larger value to the consumer than a more limited version of the identical content and thus would have a higher price, rewarding the copyright holders and distributors appropriately while allowing the consumer the freedoms they are used to.

3. DRM & Privacy

Introduction

Ecommerce and the information collection ability of companies selling rights to access digital media on the internet has made it easier than ever for retailers to collect very detailed records not just about every transaction but also what happens with the media after it is purchased by the consumer. This additional capability can be viewed as a direct reduction in the privacy that consumers were used to when purchasing no-DRM enabled media off-line [59].

The intersection of Digital Rights Management and privacy occurs in two distinct manners. The first is a loss of privacy that the user is aware of and can decide is acceptable before making a purchase or accessing digital content. The second is when the software used to enforce the DRM solution collects information from the user's device that the user is not made readily aware of. In this section we will discuss the motives of the companies, both types of privacy loss and discuss possible solutions.

Privacy

The definition of privacy and what it means to consumers is not easily defined. Different societies have different definitions of personal space, personal information and what is considered to be surveillance. One definition offered is that privacy is violated any time an individual is made more accessible to the rest of the world in any way while others might include an act of monitoring or surveillance as a loss of privacy [14].

In the past years there have been an umber of class action lawsuits against companies for including software, hardware or firmware that allows the company to individually identify the product sold. This happened with Real Media Jukebox in 1999 and Intel in 2000 [59].

The traditional definitions of privacy may need to be modified to fit in the information age and the extension of consumer protection laws to include privacy may be necessary to protect consumers from the type of surveillance implemented in DRM products [14].

Motivations for Collecting Media Usage Information

There are two types of data collected during the use of DRM protected digital media. The first is the information that must be stored to the financial transaction to complete and second is the additional information may be collected to limit personal use or monitor user activity. The information collected may be used to legally enforce the content owner's rights [31] or to be used to increase revenue by targeting adds or reselling the data. In this

section we will discuss these two types of data collection and the motivations for each because they directly impact the privacy of the consumer.

There is a very legitimate need for the holder of a copyright to know when a piece of media is used if the copyright holder is paid on a per use or download basis. This information is necessary for the necessary financial transaction to be completed and while there might be technologies in the future that allow for the anonymous purchase of DRM protected media most consumers are not actively worried about this.

Beyond the collection of this information, off-line retailers often adhere to requirements to destroy records after a certain amount of time. For instance video rental stores are required to destroy rental records as soon as is practicable by the Federal Video Privacy Protection act [39]. Such laws have not been passed for on-line retailers and often, because the records are related to company financials, companies may be required to store them for a significant duration.

Companies always have an incentive to collect information about who is making a purchase as well as the details of the purchase. This information allows them to manage inventories, determine marketing strategies, pay royalties, provide statistics to advertising partners and also later sell the information to other companies interested in a similar type of consumer [39]. In short information about a consumer making a purchase has value to the not just the company distributing the media but also their partners who are involved in advertising, cross-selling and providing the original media.

DRM opens up an avenue where the companies can collect significantly more information about media usage than with traditional non-DRM media. For instance they may collect information about the number of times a track was listened to, whether a portion of a movie was replayed more than once, whether a track is skipped etc. All of this information potentially has value to the company collecting the data and is often collected without the knowledge of the end user [39]. In effect it is in the best interest of companies to provide the consumer with as little privacy as possible. In terms of reducing consumer privacy, DRM technologies and the license agreements that consumers are required to agree to grant copyright holders rights and access to personal information that they would not be granted only under copyright law [13].

All of this is not to say that there aren't benefits to users who companies may be better able to serve is the have more information about the consumer's likes or dislikes. Advertisements and 'recommendations' made by content providers made by mind user data may lead the consumer to content they are grateful for learning about –

this can be seen in the effectiveness of targeted advertising based on user interests as carried out companies like Amazon and Google.

Some companies have drafted privacy policies meant to assure users that the information they collect is 'anonymous' or not tied to the individual's exact identity. However even in situations like this the possibility of information leakage is possible where anonymous information can be correlated with information that isn't anonymous such as records from an internet service provider to make it clear which consumer was carrying out the anonymous activity.

Dissemination of Private Information

The information that DRM enabled players can collect does not only end up in the hands of the company that sells the digital content or device on which the media is played. The information about the users activities often has to be sent from the content provider to the copyright holder so that royalty payments can be determined. In addition on-line retailers often sell information about their customers to other companies. Finally there is always the possibility that a database of user activity information could be hacked into and stolen for other nefarious uses, such as reselling, spamming or phishing, extortion of the customer or company.

Knowingly Surrendered Privacy

The first manner of loss of privacy is that which the consumer knowingly surrenders as long as they have a basic understanding of how online shopping occurs versus making off-line purchases. This section will compare the two types of purchases to demonstrate the loss of privacy inherent in online purchases.

Traditional Purchases

With traditional means of purchasing media a consumer has the ability to decide the manner of purchase such that they can remain relatively anonymous to the company selling the media. For instance, a consumer can pay cash at an electronics store for a CD or DVD and the store would not be able to collect any information about the consumer other than the time and location of purchase [39].

Additional information about the purchase has significant value to the seller of the product and they often attempt to collect additional information about the consumer, but always with the consumer's knowledge. One example of this voluntary loss of privacy includes the sales person asking for additional information such as zip code or phone number, or complete address at the point of sale. A second example

is the use of ‘loyalty cards’ where a consumer is encouraged to present a card that will connect their purchase to their personal account in exchange for some benefit such as discounts or other rewards. In both situations the user must purposely decide to present additional information about themselves for the retailer to collect.

DRM Enabled Content Purchases

Consumers purchasing digital media online are often required as part of the purchase process to register with the web site before procuring the items. This process offer puts the consumer in a situation where they must provide additional information which is unnecessary when making a traditional purchase, including mailing address, name, and credit card information [13].

Then the digital media includes the use of a DRM technology the user is often prompted to acknowledge license agreements for installed software or must seek out and read the privacy policies of the content provider in order to determine what type of loss of privacy they are giving up. These license agreements are often complex and may not be clear to the average consumer [14]. This loss of privacy is significantly different than the manner in which privacy is surrendered off line since the consumer has to take responsibility to read and understand detailed documents which are often dense and difficult for a consumer to understand. Once the policy or license agreement is acknowledged the consumer’s information can be used as the online retailer or content provider wishes without the active agreement of the consumer for each type of information collected.

DRM Related Loss of Privacy

Unlike traditional media purchases, the current crop of digital rights management technologies require that the device used by the user for viewing or listening to the digital media include software that validated the digital media and it’s validity to be used by the device. This additional step requires the DRM software to often have to intrude on the user’s privacy in order to guarantee that the rights of the media holder are being protected. This section will describe the problem and provide specific examples of how DRM solutiosn have encroached on the consumer’s privacy often without the user’s knowledge.

Some DRM products have been programmed to check for non DRM enabled media on consumer’s computer for the purpose of monitoring the users’ interest in related products [14]. Specific products like MusicNet

and Rhapsody which provide DRM enables music were found to routinely monitor and report back on the web sites visited by users who had installed the related DRM client software on their computers [39].

The limitations in current licensing agreements that force or facilitate a loss of privacy include the one size fits all method of defining the use of the consumer's personal information. Consumers must choose to accept or decline and can't specify exactly how they would like their personal information to be used [13]. This drastically reduces the flexibility implied by laws that promote consent passed privacy, as consumers are required to forgo all privacy if they hope to view a piece of content. Companies will make the agreement such that it is as wide open as possible for the use of the user information such that they reduce risk from any possible lawsuit stemming from misuse of the user's personal information.

Possible Solutions to the DRM Privacy Problem

This section will list possible solutions to the privacy problem inherent in DRM technologies. These requirements, if implemented would help guarantee that a user's privacy with DRM enabled media and players is closer to the privacy experienced with non-DRM media.

Collection of Necessary Data Only

Rather than automatically collecting every action taken by a user, the DRM software should only be active when at the time of the content purchase and to validate the use of the media afterwards. The is no reason to report back how many times a track is played or which songs are skipped in a streaming radio station since those actions are not related to the financial transaction that the DRM software is being deployed to protect.

Destruction of Records

Once a consumer has completed a transaction and the company has received the funds from the consumer, besides recording the amount, time and other financial details of the sale, there is little need for the company to store the user's specific purchase tied to their exact identity indefinitely. Instead the non-financial detailed information could be anonymized [39] and stored for later reporting without providing the company the ability to pull up every transaction, and every action take by a user.

Consumer Opt-In

Companies would still have the ability to collect additional details about a user, but those details should require the user to knowingly opt-in on a case by case basis [39]. That was a user can decide whether the benefits of providing that additional information to the company is worth the loss of privacy that is carried with it.

Privacy Rights Management

The question of how to guarantee the protection of consumer privacy when the two parties involved (content provider and consumer) have directly opposed goals may best be solved by a trusted third party that can guarantee the exchange of information and the agreed to amount of anonymity [59].

In order to build a DRM system capable of adhering to the privacy laws in different countries a type of Privacy Rights Management system could be implemented that allow for the clearly defined collection, protection, definition and distribution of personal information [32]. A PRM system would take the data collection away from the companies that might have a financial interest in misusing the information and place it in the hands of a trusted third party. Such a system could store and model all of the rules that must be adhered to in different jurisdictions and guarantee data lifespan and that the data is anonymized on schedule and that actors only have access to the information the consumer has granted. The usage of the data would be monitored, reported on and controlled not by the content provider, but by a central source.

While a PRM system similar to that described above could guarantee the adherence of laws, there is not guarantee that companies wouldn't share the information immediately after collecting it form the PRM system and there couldn't be a guarantee that the PRM system itself would never be hacked into, revealing all personal information of the consumers. A centralized approach might ensure uniformity but might also generate a single point of failure.

The benefit to the consumer is however apparent in that the consumer could see all of the data they have allowed companies to collect about them and verify that there is no inaccuracies and that the data is only retained as long as agreed to [32].

4. DRM & Security

Computer security can be defined in terms of confidentiality, integrity, and availability. Confidentiality refers to keeping secure information and resources. Integrity is defined as the trustworthiness of data. Availability refers being able to access the data or system whenever necessary. [8] When computers are compromised by security exploits, they are usually taken control of by the attacker. Once that happens, all three parameters of security can be violated (although it isn't required). It isn't clear to what extent confidentiality and integrity are typically compromised when home computers are taken over. In many cases, these machines simply become zombies and are used in botnet attacks on other systems. In any event, DRM systems need not violate any of these principles. There are essentially two types of risks with DRM systems: the normal and expected risks posed by the necessity to communicate with other computers (usually servers) and the risks caused by attempting to "hack" the system to protect otherwise unprotected content.

In general, DRM systems need to communicate with servers to acquire licenses, authenticate users, potentially query for rights, and other valid types of communications. None of these activities directly threatens the security of the client computer. However, because of the nature of these systems and the communications that inevitably entail, there are potential security vulnerabilities. Any time a computer communicates with another, especially over the Internet, a door is opened for attack. A well designed and implemented system can, and should, protect these communications in such a way as to guard against any security issues. Traditional security enhancement techniques such as threat modeling, static code analysis, white-hat hacking, and others can mitigate these risks, but they cannot be completely removed. The number of vulnerabilities continuing to be discovered, sometimes in old and well-understand code, is evidence of the difficulty of creating a truly secure system.

The risks posed by a well designed system are not the primary vulnerability. When rights management is attempted to be applied to essentially unprotected content problems can arise. Conventional audio Compact Discs (CDs) are completely unprotected and must be in order to be widely used. Any change to the format would most likely render them unusable in consumer electronics devices. And because of the massive existing installed base of consumer electronics devices a format change, simply to add rights management (and thus reduce consumer usability of the content), would be so costly as to be infeasible.

Many efforts have been undertaken to attempt to protect audio CDs when used on a personal computer (PC). Primarily, making a digital copy of the content on the PC is the function that content producers are attempting

to control. Unfortunately, because these efforts cannot be applied in a true DRM system, many fairly extreme measures must be undertaken in order to regulate the way in which the content is used. Normal system functions must be subverted in order to control these normally available functions. Ironically, this type of work is technically very challenging. Intercepting and blocking normal operating system, and especially file system, functions to prevent all but desired access typically requires very skilled and experienced developers. This area within the operating is usually not well or completely documented, so a significant amount of knowledge is necessary. Additionally, because this software is essentially extending (thus becoming a part of) the operating system, the problems faced in this type of software are some of the most difficult (re-entrancy, restricted access to calls and/or memory at fairly arbitrary times, difficult debugging environment, dependence on hardware, etc). And because it resides in a sort of gray area (it seems a lot like hacking in the pejorative sense), often lesser skilled individuals are doing the work. Thus, the quality of the work is low and additional issues and vulnerabilities arise. The most recent, and certainly most visible, of these attempts was shipped by Sony. The Sony rootkit issue will be discussed further in this paper.

A well designed DRM system can ensure a reasonable level of security. Attempting to apply rights management to unprotected content often can, and has, result in (hopefully) unintended security consequences. As such, content producers would be well-advised to simply abandon efforts to protect audio CDs and focus instead on distributing new content in more protection-friendly formats. Sony has, and will continue to, incurred significant costs due to their misguided efforts to protect their content from piracy. The direct costs consist of having to recall and probably destroy the CDs containing the software, remaster the CDs, and the loss of revenue due to not having product on the shelves near the beginning of the Christmas shopping season. Unfortunately, we'll never be able to know The costs that Sony is sure to incur, but direct through the cost of the product recall and the lost revenue due to not having product in the stores and indirect due to the damage to their reputation and lack of trust by the consumer will hopefully be significant enough to

5. DRM Technologies

In this section we will examine the two major DRM technologies, Apple's FairPlay and the Microsoft Windows Media DRM. Additionally, the Sony Rootkit fiasco will be examined in greater detail.

iTunes DRM

Apple's iTunes system uses a DRM technology called FairPlay which is based on a technology developed by Veridisc [61]. The technology is applied to AAC audio files which are similar to mp3 but have an increased performance and were defined in the MPEG-2 specification.

Capability Summary

Below is a list of DRM enforced restrictions on the use of iTunes media files [61]:

1. A track can be copied to any number of iPod music players
2. A track can be copied to up to 5 of the consumer's computers
3. A track can be burned to CD any number of times
4. A the same playlist of tracks can only be burned to a CD seven times

Compared to other DRM solutions, the unlimited number of times a track can be burned to a CD as well as the number of computers on which the track can play seems to have assuaged consumers need for personal use.

Technical Description

FairPlay works by creating a unique identifier for each computer by hashing hardware identifiers including the C: drive name, BIOS, CPU name and Windows product ID [41]. Each user is allowed to have up to five of these unique hashes. When the user's system sends the hash to the iTunes Server, if it is one of the five allowed hashes, then the server sends back a decryption key for that use's account [53]. The decryption key is stored as cipertext encrypted with the computer's hash so it cannot be moved between computers, though computers can be removed form the service and new ones added, creating a loophole of the hash encrypted decryption key is backed up before disabling iTunes on the computer [53].

Each time a music track is purchased, a new song key is generated. The song key is used to encrypt the track and is stored on Apples servers. Computers that have a valid hash can get the song key to decrypt tracks associated with the computer's user's account [61].

Overcoming DRM Limitations

The FairPlay DRM technology was overcome by hackers such as Jon Johansen [12] as well as RealNetworks which decided to reverse engineer the scheme so that its own competing music files could be played on iPod hardware using a technology called Harmony that Apple has repeatedly worked to thwart [61]. Ironically RealNetworks has worked to reverse engineer Apple's FairPlay technology, possibly breaking the DMCA which it might rely on to protect its own DRM technology called Helix.

Other companies such as VirginMega have attempted litigation to get Apple to license it's FairPlay DRM system so that its digital music tracks can be played on iPod music players [49]. Recently a DRM company called Navio systems has begun to work on reverse engineering the most recent iTunes DRM solution so that it can sell software to companies that wish to have their media playable on iTunes compatible devices such as the iPod [15].

Apple's FairPlay DRM was broken in a couple of ways. The first was to intercept the decrypted audio stream and write it to file. The second method removes the encryption from the music track file, allowing it to be used just as any unencrypted AAC file would be. Besides RealNetwork's desire to have it's media be playable on an iPod, motives for removing the encryption include to a wish to use iTunes files on more than five computers and a desire by Linux users to be able to use iTunes even though Apple only supports Windows and Apple operating systems [41].

Removing the encryption is done by using the keys stored on the iPod or the user's song key to decrypt the audio stream. Numerous version of the decryption software have been overcome by releases by apple with the most recent occurring in October of 2005. There is currently no widely available tool that can remove the encryption form the most recent version of the iTunes DRM solution.

Windows Media DRM

Most of the major non-iTunes music services use the Windows Media DRM technology [36] including Napster (formerly PressPlay) [40], Yahoo Music (formerly MusicMatch Jukebox) [63], MSN Music [38] and Walmart [60]. The Windows Media DRM is tied to the Windows Media Format (Windows Media Audio or WMA for audio) and is essentially a part of the file format. While this is a closed format, meaning the details of the format are not known, it is widely available within the Microsoft Windows world and is supported by a large number of portable players. Additionally, it is possible to transcode content to a different format such as MP3 or OGG (although this feature is typically limited in protected content). There is a freely available SDK for working with the Windows Media Format for developers who wish to do so.

Capability Summary

The Windows Media DRM system allows content producers the following flexibility:

- Boolean flags for:
  - Backing up the license
  - Collaborative Play (in a peer-to-peer network)
  - Copy to a device
  - Burning to CD (individually)

    - Copy to an SDMI device
    - Copy to a non-SDMI device
    - Playback
    - Burn to CD as part of a playlist
- Properaties for the above rights with the following possible types of values:
    - Unlimited
    - Count
    - From (date)
    - Until (date)
    - From / Until (date range)
    - Count From (# of uses from a start date)
    - Count Until (# of uses until an end date)
    - Count From / Until (# of uses during a date range)
    - Expiration after first use (time limit after first use)
- Player revocation

The Windows Media DRM system itself is agnostic as to what rights content producers / distributors wish to apply. Napster allows unlimited burns to a CD but restricts the number of times the user can burn a playlist (album) to a CD (although interestingly, Napster manages the playlist counts itself and does not rely on the built-in support). The various music services all have different levels of righs associated with the content they sell, although ironically they all offer similar catalogs so the same track from different services will have different usage rights associated with it. Typically the rights are negotiated with the copyright holder on the music and probably have an impact on what they are charged to sell the track.

Technical Description

The Windows Media DRM system uses encryption to protect the content in the files. It relies upon a combination of certificates to manage access. Each piece of software that can access protected content must get a certificate from Microsoft called a stublib. These stublibs are static link libraries that contain the certificate for that application and are sequentially numbered so as to allow fairly easy tracking. When protected content is accessed, a license must be obtained prior to decrypting and playing it (or performing the desired action). That license is specific to the user logged onto the machine. Because users are always unique in time and space (using Globally Unique Identifiers or GUIDs), that content is also tied to that machine. The license for the content is created in such a way as to be unique to the content, unique to the user, and valid for all valid stublibs. The license is stored as part of that user's profile. Licenses can be backed up so as not to be lost if the machine crashes. Because the list of valid stublibs goes into the creation of the license for each content file, stublibs can be revoked.

When a company acquires a stublib from Microsoft, it signs a contract that requires it to abide by the limitations of the content file. Once the company has a stublib, is has the ability to "unprotect" any protected

content for which the user has a valid license. Thus, the risk of piracy is large. This is essentially a trust relationship between Microsoft and the company. Backing up that trust is the ability for Microsoft to revoke the stublib if the company is found to not be conforming to the contract and enforcing the rights specified by the content producers. However, all previously acquired content will still be accessible.

As a side-note, the CSS system used to protect DVDs did not have a revocation capability. After it was broken by acquiring the key from poorly written software, DVDs continued to be published that could be decrypted using that key because the producers didn't have the mechanism in place to revoke that key without disabling the existing set top players.

Overcoming DRM Limitations

Microsoft has gone to considerable trouble to protect their DRM system, including not allowing it to function when being run in a debugger (which considerably complicates debugging the application trying to access the protected content). However, there are several trivial ways to remove all protection from the content. The easiest method is if the content can be burned to CD. If so, it can easily be burned using Windows Media Player (WMP) and then ripped right back to the machine in an unprotected format, again using WMP. WMP will even burn content with CD TEXT information making retrieving the track information easier when ripping if it cannot be retrieved from an online music information database such as GraceNote [28].

A second method is available for content that can be played (which is virtually all content) and that is to capture the bits as they're on the sound card. This exploit was widely publicized as breaking Napster's protection but in reality was already well known and had been in practice for quite some time. This tends to be used by more technical, more dedicated music pirates and isn't as accessible to the general public. There is no known tool to strip the protection off the file.

Sony DRM

Like other music distributors and copyright holders, Sony BMG is concerned with protecting it's music from being copied an distributed between friends as well as preventing it's music being ripped from CDs and shared on P2P networks and Bittorrent sites. The motivation behind this is an assumption that every copy made of a piece of music can possibly be correlated to a lost sale. Evidence of this is provided by organizations such as the RIAA

have been working to prosecute individuals involved in file sharing. Statistics provided by the RIAA show CD sales revenue dropping in 2001 by 2.3%, in 2002 by 6.7% and in 2003 by 6.7% [11].

Dropping sales and the assumption that the cause is the ease of copying and distributing the music online with out any compensation to the copyright holder has encouraged companies like Sony BMG to begin distributing CDs with DRM technologies. The difficulty of securing media content stored on a compact disk has caused these technologies to impair personal or fair use of the media and have also, in the case of the Sony Rootkit scandal, shown that Sony is willing to use technology commonly considered toe be malware at best and illegal at worst to protect their rights, at the expense of the consumer. This section will cover the Sony's DRM technologies, provide an overview of the XPC copy protection and a history of the events that have occurred in the previous month.

Sony's CD DRM Technologies

Sony BMG uses two types of Digital Rights Management technologies. Their original technology is MediaMax provided by SunnComm and the newer technology, referred to in the media as the Sony Rootkit, is XPC developed by First4Internet. Sony's MediaMax technology has been available for some time but did not gather the media attention that it's newer technology does. MediaMax has been included on an order of magnitude more CDs (20 million) than XPC which has been distributed on about 2 million, so if consumers had a significant issue with MediaMaxx it is likely that this would have come to light by now. Comparing the two technologies might show the type of DRM which the public is willing to accept versus that which it is not. In this section we will provide a brief comparison of the capabilities of XPC versus MediaMax.

Both XPC and MediaMax are active on the computer at all times after the installation regardless of whether a protected CD is in one of the computer's drives or not [51].

Both XPC and MediaMax periodically contact Sony's servers with information about the user's IP address and the CD identifier [51].

Both XPC and MediaMax do not provide the user with the option to uninstall the DRM software after the user has completed using the CD [51].

Both XPC and MediaMax install regardless of the wishes of the user. XPC doesn't provide the user with the option to install or not. Meanwhile MediaMax provides a EULA acceptance screen which the user can decide to accept or not. However, even if the user rejects the EULA the MediaMax DRM software may install itself [24].

While it might seem unreasonable to have software installed and running on a system continuously even if the CD is only played once, to have a computer report to a company on the usage of a CD you have already purchased, or to make it difficult to uninstall the software once the CD no longer needs to be used on the computer, it seems that the majority of consumers have been willing to accept this type of use of their systems by Sony BMG's DRM.

XPC and MediaMax are very similar in features except for the addition of a 'Rootkit' in the XPC software. A rootkit is a piece of software that usually performs two tasks on the system it is install on. The first is to hide the files it uses and processes it runs from the operating system such that there is no indication that the rootkit has been installed. The second is to provide anyone with knowledge of the rootkit's installation to use the rootkit to access the computer to use its resources as needed. This type of access is sometimes referred to as having a backdoor into a system [62]. Rootkits are normally used in hacking activities but in this instance First4Internet reused rootkit software and used it to implement Sony BMG's DRM requirements.

The use of the rootkit made MediaMax and XPC different in two fundamental ways. First Sony was attempting to completely hide their DRM software using technology that is normally used by hackers – in effect hacking all of the computers of consumers that purchased their XPC protected CDs. Second the use of such a rootkit, besides it's duplicitous nature, leaves the computer open to other attacks.

XPC Technology and Discovery

The Sony XPC technology began to gain media attention with the publication of a description of how the rootkit was discovered on October 31, 2005 while an anti-rootkit tool was being tested [44]. The test showed that a computer that should not have had an installed rootkit had hidden directory, application and device drivers, eliciting further investigation from the programmer, Mark Russinovich.

The rootkit hooked into the system call table causing it's own function to be executed rather than the function that is part of the kernel. Hooking like this allows the rootkit to return any values it would like, in this case spoofing the system into thinking that that a specific directory and application didn't exist. Once the driver containing the alternate function was identified, the location of the driver was found and the directory containing the driver and other files was accessed [44].

The driver that was responsible for the cloaking was disassembled and it was discovered that the driver hid any registry key, file or directory that started with the string 'sys'. Once the driver was disabled and the system

rebooted the hidden files were reviewed with a utility that showed the publisher of some of the files to be 'First 4 Internet'. The company's web site was checked and the XPC software they sold for DRM on CDs became the primary suspect. From there the recent use of a Sony BMG CD on the computer was revealed to be the source of the rootkit [44].

Further exploration showed that the XPC software scanned executing programs every couple of seconds and cost a couple of percentage of CPU usage. This was likely done to monitor for blacklisted CD burning software [54]. There was no uninstaller provided on the system and it was discovered that simply removing the software would render the cd-rom drive unusable. It could only be resorted by removing the XPC DRM installed filters on the CD-ROM device [44].

Sony Rootkit History

Sony knew about the possible issues with First4Internet's XPC DRM software before the media picked up the story, but they did nothing to immediately protect consumers from an insecure DRM software product they had been distributing, possibly because they may not have fully understood the technology involved.

A user in Manhattan found the rootkit while trying to clean rootkit problems out of some of his company's computers on September 30th. The problem was reported to F-Secure, an anti-virus software company on October 4. F-Securie communicated the security problem with the XPC DRM software to Sony BMG on October 4th [30].

Sony BMG, upon being notified asked First 4 Internet to begin investigating, meanwhile F-Secure provided a more complete report on October 17th, including the notion that the rootkit would leave the computers of consumer who installed Sony BMG's XPC DRM software open to malicious attacks. Nothing progressed because First 4 Internet claimed that the security hole was unknown and that the next version of XPC would fix the problem. Neither Sony BMG, First 4 Internet or F-Secure went public with any of the security concerns.

On October 31 Mark Russinovich published the rootkit discovery as summarized in the prior section, bringing the rootkit into the public eye for the first time. Sony responded by releasing an uninstall tool on November 3rd [50].

Ed Felten revealed on his 'Freedom-To-Tinker' web site that the Sony rootkit uninstall actually failed to uninstall the rootkit and in some cases opened up the consumer to an even larger security hole. After installing Sony's fix it would be possible for any web page visited to potentially download, install and execute any software on the users computer [25].

Also on the 9th McAfee releases a patch to it's anti-virus software to remove the cloaking of the rootkit, but not the DRM software itself [46]. The Electronic Freedom Foundation posted a list of Sony DRM Rootkit infected CDs [17], released an evaluation of the Sony EULA that accompanies their DRM software [20] and began to organize a class action lawsuit against Sony BMG. Sony's EULA included the following agreements [20]:

- If you don't possess the CD you must delete all copies of the CD
- The music can only be on computers that you personally own – not those owned by schools or companies
- Sony can install any software it would like on your computer to enforce copy protection
- Sony will never have to pay damages of more than $5 for problems caused by any software installed from their CD

By November 10th viruses that use the Sony XPC DRM software rootkit to spread had been discovered on the Internet.

On November 11th Sony BMG decided to stop shipping CDs that use the XPC DRM software. On the 14th they began pulling the infected CDs from store shelves [29]. At this point it was estimated that up to half a million computers are infected with Sony's XPC DRM software rootkit [46]. On November 14th, Microsoft announced that its virus software will detect and remove the rootkit portion of the XPC software [22].

On November 21 the Electronic Freedom foundation announced it's part in a class action lawsuit against Sony BMG requiring remediation for the damage done by Sony BMG's XPC and MediaMax DRM software [18].

Conclusion

The most important result of the Sony rootkit scandal may be the publicity that the problems with the Sony rootkit in particular and those of DRM in general had elicited. Consumers, after reading the news form the last month, might be more likely to check for DRM before purchasing a CD so that they have the appropriate expectations of what they will be able to do with the media they have purchased.

Beyond that, the Sony rootkit scandal will likely encourage companies to pay closer attention to the type of DRM software the include with their products, rather than rely on software vendors to verify that the DRM software is secure and doesn't use tools commonly believed to be malicious.

One of the more interesting pieces of the scandal is that some security companies initially treated the XPC rootkit differently that a normal rootkit because it was distributed by a legitimate company. This implies that they

may grant companies more leeway in monitoring and running software on consumer computers than they would grant hackers – even if the exact same technology is used for both. This causes a situation where hackers may be able to piggyback on the 'legitimate' DRM-related use of the software tools they normally use and implies an ongoing security risk whenever DRM is involved.

6. The Future of DRM

The future direction of digital rights management depends on the advancement of two things: the systems that implement DRM technologies and the laws and rulings passed that define the rights of consumers versus those of intellectual property owners. Both of these factors are changing as the impact of existing laws become better understood and technologies that implement them evolve to adhere to the laws while hoping to prevent any backlash that inconvenience might bring from customers. This section will provide an overview of some of the trends in the legislative status of DRM as well as the newer directions that DRM technology is taking.

The Future of DRM Legislation

Digital Rights Management is sure to garner more attention as the size of the market for digital media increases. Certain segments such as mobile media are expected to grow in revenue to $37 billion by 2010 [10], while the market for DRM technology solutions is expected to increase from $36 million in 2003 to $274 million in 2008 [26]. As the economic impact of digital rights management increases the need to clearly define the laws under which IP owners and consumers must work will become increasingly important. Below are some examples of the DRM related legislation that are currently undecided, the results of which will impact DRM implementations in future years.

DRM Related Lawsuits

Companies that exceed the limits of the law in an effort to protect their IP will come under increased scrutiny as the number of effected users increases. Sony BMG is in the process of having a class action lawsuit brought against them due to their XPC DRM software which negatively impacted over 20 million consumers [18]. As the limits to which companies can go to protect their IP are more clearly defined the technologies used will shift to meet those needs.

Electronic Freedom Foundation

Foundations like the Electronic Freedom Foundation monitor DRM laws and often take the side of the media consumer in court cases. Their goal is to protect the rights of users and consumers against companies that may be impeding them or suing under laws such as the DMCA. They are currently involved in a number of lawsuits including the Sony BMG lawsuit listed above. Other significant DMR lawsuits they were involved in include the following:

- MGM vs. Grokster – in March of 2005, the EFF worked to defend the company that created the Grokster, Morpheus and Kaza in a Supreme court case that led to the decision that a distributor can't be held liable for the actions of the software's users. This meant that the software could be used to share files though the users could be held responsible [37].
- Blizzard v. BNETD – In September of 2005 the Eighth Circuit Court upheld a ruling that the people who reverse engineered a game server so they could play games without using Blizzard's service had broken the DMCA. The EFF worked on the case to help to protect the rights to reverse engineer a software program [9].
- American Liberty Association v. Federal Communications Commission – This lawsuit was about adding a 'Broadcast Flag' that would have made if possible for companies to enforce that not HDTV content could be recorded on digital recorders such as Tivo. The Broadcast Flag was thrown out by the D.C. Circuit Court of Appeals meaning that the FCC could not mandate what happened in a piece of hardware after a digital signal is received [7].

Digital Media Consumer Rights Act

Given the complaints about the DMCA [23] and the belief that it infringes on the 'fair use' doctrine by making it illegal to circumvent protection even for fair use by the consumer [33], a Digital Media Consumer Rights Act [16] was introduced to Congress in 2003 and again in March of 2005. The DMCRA includes specific changes that would counteract the following issues in the DMCA.

The DMCA prohibits circumventing the protection on media even if the protection is being circumvented for the purposes of fair use. That is, it is illegal for someone to circumvent the protection to make a backup copy even though such a backup is allowed under fair use. The DMCRA would modify federal law so that "it is not a violation of this section to circumvent a technological measure in order to obtain access to the work for purposes of making noninfringing use of the work" [16]. In addition the DMCRA would change the law so that copy protection could be removed for scientific research [16]. Threats against research have been made under the DMCA including an instance when Recording Industry Association of America threatened to sue a research team led by Ed Felton when they planned to publish research about weaknesses in the DRM used to watermark music files [19].

Super DMCA Legislation

Beyond the standard DMCA law passed by congress, right holders such as the Motion Picture Association of America have been working to pass laws at the State level to grant them additional control of their intellectual property. These laws which expand the right holder's ability to control their IP are termed 'Super DMCA" Legislation. The MPAA created a model bill that was used as a base by lobbyists to present before state congresses [34]. The gist of the model bill as interpreted in [34] includes rules such that anything not specifically allowed becomes forbidden. Laws have passed in states such as Arkansas, Delaware, Florida, Illinois, Maryland, Michigan, Pennsylvania and Virginia, while failing or being vetoed in states including Colorado and Oregon [21].

The Future of DRM Technology

In this section we'll cover attempts to solve the limitations in the current generation of DRM technology. These limitations commonly leave consumers unhappy since they lack the ability to make 'fair use' of the content they have purchased while leaving the content providers open to having their intellectual property made available to the public without the guarantee of payment.

Overview

While in the past DRM technologies have mostly been concerned with securing a specific copy of media to run on a specific device or in a specific viewer, these technologies have been seen to limit the personal use hat consumers have the right to. Once a consumer has purchased some media they expect that they won't have to buy it again just because their hard drive crashes or they need to make some other change to their computer. Further there seems to be an expectation that the user shouldn't have to purchase the item more than once if they want to listen to the song in their car, at work and at home. As a result consumers might be inclined or even encouraged to work around the DRM that exists today so that they can listen to or watch the media when and how they'd like.

This problem of personal use has been implemented in technology in some fairly arbitrary ways - for instance limiting the number of times a user can make a copy of a CD. The company owning the IP, working with the DRM technology had to decide how many times to let a consumer copy something in a way that was in accordance with personal use. Selecting a number of copies doesn't guarantee that the personal use is maintained since it is similar to giving the user 3 chances to get it right. At the same time it doesn't stop the consumer from making a copy for the purpose of giving it to a person who didn't pay for the right to own that media. In effect the most common DRM technologies neither guarantee the company the benefits they'd hope to see or the consumer the right to only purchase something once and use it as and where they wish. Newer DRM architectures hope to take a step toward making it possible for the rights of companies to be protected while allowing consumers to use the media in reasonable ways.

The first is an overview of 'Project DReaM' which is an initiative by Sun Microsystems to define an open architecture for implementing DRM systems that are able to interoperate. The second is description of a system that could be used on home networks to allow consumers to use DRM protected media on any of their devices. The final section will discuss the limitations of current operating systems which make the implementation of a DRM system capable of meeting the core requirements impossible and possible solutions. Neither may succeed in the end, but both attempt to bridge the gap between the DRM technologies currently available and the laws which govern the rights of intellectual property owners and consumers.

Sun Labs DReaM

The goal of Sun Labs DReaM architecture is to provide DRM solution that is open and allows for proprietary DRM technologies to interoperate [26]. The fundamental difference between DReaM and the current set of popular DRM technologies includes providing access based on who the user is rather than the device and allowing access to be managed dynamically.

The right to access content is traditionally tied to a device with current technologies. The DReaM architecture includes disconnecting the rights to access content from the device and grant it to the consumer. This would presumably allow for the fair use of content that an individual has purchased since they would have access to it on all of the devices they had access to. Rather that the device holding the right to view the content, the users ability to authenticate would provide the DRM software with enough information to determine if the user can view the content.

The key to making this possible is to completely disconnect the system that manages what content a consumer has the right to view from the technologies used to protect the content from inappropriate access. To facilitate this, the companies that build DRM tools would begin focusing on the means to protect the content and then use an open standard to authenticate and authorized the user to view the content. The base requirement for companies that work on DRM tools is that they would no longer rely on the authenticating the device for viewing the content, but instead would rely on a service that would respond with access limits based on the user credentials.

Since the access is based on the user's roles, the possibility opens up for content providers to sell access to individuals or groups. One can imagine different pricing is a movie or song is purchased for a family versus an individual;. Also, roles can be shifted or promoted as the membership and needs of those in the group of consumer's changes. These capabilities do not exist with the current set of device centric DRM systems.

DRM Security for Home Networks

One of the keys to a DRM system that allows for fair or personal use is a system that allows the consumer to use the same digital media on all of the devices they own that are capable of playing the content. For instance, one would not expect to purchase a CD in a store and then

expect to only be able to play the CD in the first CD player they listen to it on. Instead the consumer expects to be able to play the CD at home, in their car and perhaps at work. Toward a DRM implementation capable of supporting this requirement, a solution has been proposed that will allow digital media content to move between devices on a home network while guaranteeing that the right of the user to access the content is authorized in accordance with the copyright holder's license[42].

Similar to the Sun DReaM architecture the proposal is to move away from compliant devices and toward a model where a domain is authorized to access the protected content. The domain is first created, then devices are registered and each device is authorized through the sharing of a symmetric 'Master' key using a public key infrastructure [42]. Devices are removed from the network via blacklisting mechanism referred to as a revocation list, which prevents the device from receiving and decrypting new digital content [42]. Each device on the domain that attempts to distribute media to another device on the domain checks the revocation list before delivering the content [42].

The content is stored in an encrypted format and is only unencrypted to tamper proof memory. This would prevent a malicious user from reading the memory and creating an unencrypted copy of the media. Each device's master key would also be stored in the tamper proof memory. The media is encrypted and decrypted with a content key that is stored only after being encrypted with the master key. The media is only stored after being encrypted with the content key. The master key grants access to the content key which allows for decryption of the content. Every time a device is revoked from the network a new master key must be determined and the content keys re-encrypted so that the revoked device can no longer access content [42].

This encryption and key distribution network will allow the media to move between authorized devices on a personal use network, while only being stored in an encrypted format that prevents a malicious user from creating an unencrypted copy. This type of authenticated network should grant the consumer a better personal use environment while protecting the copyright holder's rights to control their content.

Conclusion

While the implications of copyright laws are being refined in court and new laws to protect or reign in the rights of copyright holders are being proposed, technologies are slowly evolving that should help protect the right of the copyright holder and the consumer's right to fair use.

One of the main trends seems to be a movement toward a loosening of the constraints that DRM technologies have placed on digital content since they seem to be encouraging consumers to obtain media that isn't DRM protected. It seems that the most likely near term result will be technologies that give the consumer enough ability to use digital media as they would that purchased in a store.

7. Conclusion

The current DRM systems do a fairly good job of protecting the interests of the copyright holders. In general, they are difficult to completely circumvent and instead must be worked around to remove the protection mechanism from the files containing the content. The services that make use of DRM systems for distributing content have, at best, a confused privacy policy and no umbrella policy covering your data from the instant it leaves your machine. We are left to assume the worst about what is being done with that data, but it is probably not unreasonable given the context and the motivations that the distributors have for tracking information about the consumers.

The current DRM systems do such a good job of protecting the interests of the copyright holders that they substantially reduce rights granted under the Fair Use of the Copyright Act. Unfortunately, attempting to exercise these rights by circumventing the DRM system runs afoul of the DMCA and the courts have shown a willingness to rule in favor of the copyright holder in these types of cases.

Addtionally, overzealous attempts to protect content that is essentially unprotectable has created major security vulnerabilities on the computers affected. Several exploits have been successfully run against these vulnerabilities, so this is not a laboratory or theoretical issue. It exists in the wild.

Despite the current state of affairs, there seems to be a gradual understanding that overly restrictive systems do not create enough value for consumers to purchase the content and consumers can and will pay a little more for more flexibility. While the current situation is fairly depressing from the perspectives of legal issues, privacy and security, there is cause for hope that these issues are going to be better understood and the consumer might not end

up losing both their privacy and Fair Use rights just for the opportunity to purchase content in a more convenient setting.

7. References

[1] 17 U.S.C. § 106

[2] 17 U.S.C. § 107

[3] 17 U.S.C. § 1201

[4] 17 U.S.C. § 1201 (a)(2)

[5] 17 U.S.C. § 1201 (c)(1)

[6] 17 U.S.C. § 1030

[7] American Library Association v. Federal Communications Commission, (2005). http://www.eff.org/IP/Video/HDTV/ALA_v_FCC/

[8] Bishop, M. *Computer Security: Art and Science.* Boston: Addison-Wesley, 2003

[9] Blizzard v. BNETD, (2005). http://www.eff.org/IP/Emulation/Blizzard_v_bnetd/

[10] Booz Allen Hamilton, *MEF mDRM White Paper*, (July 2005). Available at <http://www.m-e-f.org/pdf/mDRM_WP_execsumm.pdf>

[11] John Borland, 'Bots' for Sony CD Software Spotted, November 2005. Available at http://news.com.com/Bots+for+Sony+CD+software+spotted+online/2100-1029_3-5944643.html?tag=nl

[12] John Borland, Program Points Was to iTunes DRM hack (2003), Available at http://news.com.com/2100-1027-5111426.html

[13] Alex Cameron, Infusing Privacy Norms in DRM, (2004). Available at http://idtrail.org/files/Alex_Cameron-Infusing_Privacy_Norms_in_DRM.pdf

[14] Julie Cohen, *DRM and Privacy*, (2003). Available at https://www.law.berkeley.edu/institutes/bclt/drm/papers/cohen-drmandprivacy-btlj2003.html

[15] Cory Doctrow, DRM Company Vows to Hack iTunes DRM (November 2005). Available at http://www.boingboing.net/2005/11/21/drm_company_vows_to_.html

[16] *Digital Media Consumer Right's Act*. Available at <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h1201ih.txt.pdf>

[17] Electronic Freedom Foundation, Are You Infected by Sony-BMG's Rootkit, (November 2005). Available at http://www.eff.org/deeplinks/archives/004144.php

[18] Electronic Freedom Foundation, EFF Files Class Action Lawsuit against Sony BMG, (November 2005). Available at http://www.eff.org/news/archives/2005_11.php#004192

[19] Electronic Freedom Foundation, Felten, et al., v. RIAA, et al. (2001). Available at http://www.eff.org/IP/DMCA/Felten_v_RIAA/

[20] Electronic Freedom Foundation, Now the Legalese Rootkit: Sony-BMG's EULA, November 2005). Available at http://www.eff.org/deeplinks/archives/004145.php

[21] EFF, State-Level "Super DMCA" Initiatives Archive, (2003). Available at <http://www.eff.org/IP/DMCA/states/#effresources>

[22] Joris Evers, Microsoft will Wipe Sony's Rootkit, (November 2005). Available at http://news.com.com/Microsoft+will+wipe+Sonys+rootkit/2100-1002_3-5949041.html

[23] *Executive Summary, Digital Millenium Copyright Act, Section 104 Report*. Available at <http://www.copyright.gov/reports/studies/dmca/dmca_executive.html>

[24] Ed Felten, MediaMax Permanantly Installs and Runs Unwanted Software, Even is User Declines EULA, (November 2005). Available at http://www.freedom-to-tinker.com/?p=936

[25] Ed Felten, Sony's Web-Based Uninstaller Opens a Bigger Security Hole; Sony Recalls Discs, (November 2005). Available at http://www.freedom-to-tinker.com/?p=927

[26] Gerard Fernando, Tom Jacobs, Vishy Swaminathan, *Project DReaM - An Architectural Overview*, (September 2005). Available at <http://www.openmediacommons.org/collateral/DReaM-Overview.pdf>

[27] Fetscherin, M. and Schmid, M. 2003. Comparing the usage of digital rights management systems in the music, film, and print industry. In *Proceedings of the 5th international Conference on Electronic Commerce* (Pittsburgh, Pennsylvania, September 30 - October 03, 2003). ICEC '03, vol. 50. ACM Press, New York, NY, 316-325.

[28] GraceNote. http://www.gracenote.com

[29] Jefferson Graham, Sony to Pull Controversial CDs, Offer Swap (November 2005). Available at http://www.usatoday.com/tech/news/computersecurity/2005-11-14-sony-cds_x.htm?csp=34

[30] Steve Hamm, Sony BMG's Costly Silence (November 2005). Available at http://www.businessweek.com/technology/content/nov2005/tc20051129_938966.htm

[31] Ian Kerr, Jane Bailey, The Implications of Digital Rights Management for Privacy and Freedom of Expression, (2004). Available at http://www.commonlaw.uottawa.ca/faculty/prof/ikerr/CVArticles/Chief%20Treasures%20of%20the%20World%20-%20What%20Happens%20When%20Law%20Protects%20the%20Technologies%20that%20Protect%20Copyright.pdf

[32] L. Korba, S. Kenny, *Applying Digital Rights Management Systems to Privacy Rights Management*, (2002). Available at http://www.iit-iti.nrc-cnrc.gc.ca/iit-publications-iti/docs/NRC-44955.pdf

[33] Rik Lambers, *Restriking the Balance: from DMCA to DMCRA*, (January 2005). Available at <http://www.indicare.org/tiki-print_article.php?articleId=70>

[34] Fred von Lohmann, State "Super-DMCA" Legislation: MPAA's Stealth Attack on Your Living Room. Available at <http://www.eff.org/IP/DMCA/states/200304_sdmca_eff_analysis.php>

[35] Qiong Liu, Reihaneh Safavi-Naini, Nicholas Paul Sheppard. 2003. Digital rights management for content distribution. In *Proceedings of the Australasian information security workshop conference on ACSW frontiers*. (Adelaide, Australia). Australian Computer Society, Darlinghurst, Australia, 49-58.

[36] Microsoft Windows Media DRM. http://www.microsoft.com/windows/windowsmedia/drm/default.aspx

[37] *MGM Studios, Inc. v. Grokster, Ltd.*, 259 F. Supp. 2d 1029, 1038 (C.D. Cal. 2003). Also available at http://www.eff.org/IP/P2P/MGM_v_Grokster/

[38] MSN Music. http://music.msn.com/

[39] Deidre Mulligan, John Han, Aaron Burstein. 2003. How DRM-Based Content Delivery Systems Disrupt Expectations of "Personal Use", (2003). In *Proceedings of the 2003 ACM workshop on Digital rights management* (Washington, D.C). ACM Press, New York, NY, 77-89. Also available at http://www.sims.berkeley.edu/~john_han/docs/p029-mulligan.pdf

[40] Napster. http://www.napster.com

[41] Andrew Orlowski, iTunes DRM Cracked Wide Open for GNU/Linux, (2004). Available at http://www.theregister.co.uk/2004/01/05/itunes_drm_cracked_wide_open/

[42] Bogdan C. Popescu, Frank Kamperman, Bruno Crispo, Andrew Tanenbaum, (2004) A DRM Security Architecture for Home Networks. In *Proceedings of the 4th ACM workshop on Digital rights management.* (Washington, D.C.). ACM Press, New York, NY, 1-10. Also available at <http://www.cs.vu.nl/~bpopescu/papers/drm04/drm04.pdf>

[43] RIAA 2004 Year End Statistics (2005). Available at http://www.riaa.com/news/newsletter/pdf/2004yearEndStats.pdf

[44] Mark Russinovich, Sony, Rootkits and Digital Rights Management Gone To Far (October 2005). Available at http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html

[45] Pamela Samuelson (2003). DRM {and, or, vs.} the Law. *Communications of the ACM*, 46(4), 41-45

[46] Bruce Schneier, Real Story of the Rogue Rootkit, (November 2005). Available at http://www.wired.com/news/privacy/0,1848,69601,00.html

[47] Marvin L. Smith. 2004. Digital rights management & protecting the digital media value chain. In *Proceedings of the 3rd international conference on Mobile and ubiquitous multimedia.* (College Park, Maryland). ACM Press, New York, NY, 187-191

[48] Tony Smith, Real Fires Back at Apple in DRM Dogfight, (2004). Available at http://www.theregister.co.uk/2004/07/30/real_rebuffs_apple/

[49] Tony Smith, Virgin Demands Apple License iTunes DRM (2004). Available at http://www.theregister.co.uk/2004/08/06/apple_vs_virgin/

[50] Sony Anti-Customer Technology Roundup and Time-Line (November 2005). Available at http://www.boingboing.net/2005/11/14/sony_anticustomer_te.html

[51] Sony BMG – Malware Feature Comparison (December 2005). Available at http://www.baum.com.au/%7Ejiri/ae/blog/01132660259

[52] *Sony Corp. of America v. Universal City Studio*, 464 U.S. 417, 455, 78 L. Ed. 2d 574, 104 S. Ct. 774 (1984)

[53] Aaron Swattz, Behind the Tunes Music Store, (2002). Available at http://www.aaronsw.com/2002/itms/

[54] Summary of Sony's XPC DRM System available at http://hack.fi/~muzzy/sony-drm/info.html

[55] Pasi Tyrvainen, Concepts and a Design for Fair Use and Privacy in DRM, (February 2005).

[56] *Universal City Studios v. Corley*, 273 F.3d 429 (2d Cir. 2001).

[57] *Universal City Studios v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000)

[58] U.S. Congress. *Public Law 105-304*: *Digital Millenium Copyright Act*, 105th Congress, 1998. Available at http://thomas.loc.gov/cgi-bin/toGPO/http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ304.105.pdf

[59] Poorvi Voora, Dave Reynolds, Ian Dickinson, John Erickson, Dave Banks, *Privacy and Digital Rights Management* (January 2001). Available at http://www.w3.org/2000/12/drm-ws/pp/hp-poorvi2.html

[60] Walmart. http://downloads.walmart.com/swap/

[61] Wikipedia. "FairPlay" http://en.wikipedia.org/wiki/FairPlay (2005)

[62] Wikipedia. "Rootkit" http://en.wikipedia.org/wiki/Rootkit (2005)

[63] Yahoo Music. http://music.yahoo.com/