May 2009

MODERN DIGITAL RIGHTS MANAGEMENT METHODS

Ben F. Anderson
Worcester Polytechnic Institute

Eric Joseph Renzulli
Worcester Polytechnic Institute

MODERN DIGITAL RIGHTS MANAGEMENT METHODS

An Interactive Qualifying Project Report

Submitted to the Faculty

of

WORCESTER POLYTECHNIC INSTITUTE

in partial fulfillment of the requirements for the

Degree of Bachelor of Science

By

_____

Ben F. Anderson

_____

Eric J. Renzulli

5 May 2009

_____

Professor George T. Heineman, Major Advisor

TABLE OF CONTENTS

Abstract

Previous Digital Rights Management (DRM) schemes used by the music industry on physical media have been ineffective and have caused problems for consumers. As a result, the music industry transitioned to digital content by utilizing a successful internet-based DRM model. The music industry recently adopted DRM-free content, yet the game industry still struggles with problems protecting physical media. Media-based DRM models of the game industry are satisfactory at best, so internet-based DRM models are becoming increasingly popular. Current trends in the game industry suggest that future DRM methods will be internet-based, as DRM-free methods can be fiscally illogical for use in the game industry.

Acknowledgements

There are several people we would like to thank for their assistance with this project.

We solicited both sets of our parents for assistance in proofreading the numerous drafts we produced, and their comments have been invaluable to the completion of this project.

We also would like to thank our advisor, Professor Heineman, for his assistance getting us started once we came to him with a potential topic. Throughout the project, he helped us narrow our focus when we were not sure what topics to research. He also helped us to structure our paper and combine the ideas to form our project.

1. Introduction

For this project we researched various models of Digital Rights Management (DRM) used extensively in the movie, music and gaming industries. DRM is an umbrella term that describes the full range of technical means companies use to protect their intellectual property which is available on digital media. DRM is necessary to protect this intellectual property against unauthorized use.

We decided to investigate the DRM models for the electronic game industry. We began by researching and summarizing most of the major DRM methods of the movie, music and game industries. After our basic analysis was complete, we compared all the summaries to determine the parallels between each popular DRM method. This allowed us to categorize most of the DRM methods based on their effectiveness, and subsequently analyze each model. After completing our analysis in this report, we were able to draw conclusions and recommendations about DRM in the game industry.

Additionally, we outlined the Government's direct involvement in DRM through copyright laws. This involvement has been straightforward, because there is a long tradition of using numerous copyright laws to protect intellectual property rights. Since technology progresses quickly, copyright laws soon become obsolete. Although the Government can't effectively create laws before problems occur, they have stayed on top of the DRM issue by constantly updating and re-writing copyright law as new issues emerge.

While we do not discuss DRM of the movie industry in depth, we mention it because this technology has had its share of problems which newer technologies have tried to learn from. Specifically, we discuss various DVD copy protection schemes. We focus primarily on the Content Scrambling System (CSS) which is the most common DVD copy protection, and was initially used to protect new DVDs from being copied.

As the first major industry to encounter large-scale problems with piracy of intellectual property online, the music industry has had numerous problems finding a suitable DRM model. We discuss some of these problems, which became apparent with the introduction of Napster [1]. The music industry quickly recognized that they needed a method to protect their content that was being freely shared on the Internet.

After we discuss the evolution of DRM and problems encountered with it in the music industry, we turn our attention to the game industry. Since DRM in the entire game industry encompasses hundreds of consoles and protection schemes, we have restricted our focus mostly to the current DRM methods of PC games. While the music and movie industries have found proven and effective DRM methods, the game industry is lagging behind while trying to find its own well-balanced model. Since DRM in the game industry is less mature than in other industries, we feel that an analysis of DRM methods that have worked in other areas in the past will show methods that are likely to be successful for the game industry in the future. We also suggest a model of our own which we believe has potential for success in the game industry.

2. Methodology

This Interactive Qualifying Project consisted of researching DRM extensively in the music and gaming industries. Since DRM is more prevalent in the music and movie industries than it is in the game industry, it was more difficult to obtain information regarding DRM in the game industry. However, DRM in games is becoming increasingly popular so we were able to locate enough information available for the purposes of this project. During all stages of research and analysis, we searched for new information and articles, since DRM is an ongoing issue.

The schedule for this project describes how we gathered, reviewed, organized and analyzed information regarding DRM. The two of us involved in this project shared the responsibilities evenly and met routinely to write the report and perform other tasks.

Initially we researched DRM for the music and movie industries by visiting credible sites on the Internet. Each cited web page was saved in an archive of PDF's, so that in the event a web page was removed or its location changed, we would still have a record of the information that was used. For each collected source document, we wrote a summary and extracted relevant time information to create the timelines which document the evolution of DRM within multiple industries.

We compiled timelines to outline the history of DRM. After selecting the most relevant timelines, we performed more in-depth research on the topics in the timelines in order to discover and document additional supporting evidence. Our goal was to have detailed timelines that related both inter-industry DRM and intra-industry DRM.

Gaming industry DRM was researched using a similar method as that of the music and movie industries. Since the gaming industry is newer and is changing rapidly due to technological advancements, it was harder to locate physical media such as journal publications and books. As a result, we needed to rely heavily on electronic sources using the assistance of Internet search engines.

By the end of the first term, we defined the project objectives. We produced a working thesis statement to guide the work that was completed in the final two terms. Background research continued throughout the entire project, though the majority of the information was identified during the first term. Upon completion of the second term, we had a clear idea of the issues faced by the gaming industry regarding DRM.

One final goal for the completed project was to understand and document the state of DRM for all industries researched in this project and to show how DRM technologies have affected the entertainment industry and its consumers. Through extensive research concerning DRM usage by various entertainment industries clear models emerged that effectively describe how different types of DRM work. We gave a general summary of each model we researched, analyzed each in order to identify the strengths, weaknesses and risks associated with the different models. We stayed objective while identifying each DRM model so that we could effectively compare and contrast these models. This enabled us to predict a trend for the development of effective DRM in the game industry.

3. Legislation

In many areas of society, the Government stays uninvolved and lets events transpire of their own accord. However, when instability occurs, it is necessary for the Government to intervene and fix problems. This was the case with the DRM concerns that weren't able to be solved without intervention. This section describes the important issues regarding Government intervention and DRM.

3.1. Copyright Act of 1976

The Copyright Act of 1976 was passed to replace old copyright laws that were put into place by the Copyright Act of 1909. The advent of new technologies, such as motion pictures, television and radio required new copyright laws to protect these new types of content, and many changes were necessary to bring these laws up to date. The new copyright laws offered copy protection to original works of content produced on any physical medium. When the new Copyright Act was passed, it made old copyright laws obsolete and enforced many new ones [2].

There were many new policies enforced by the Copyright Act of 1976, including the following: Exclusive rights were provided to copyright owners, including the right to reproduce, sell, perform, display and create derivative works of their content. Fair use rights were revised from common law so a clear distinction would be made between fair use and copyright infringement. The copyright protection period was also increased from twenty-eight years to the length of the author's life, plus fifty years. A seventy-five year period was provided for any works created anonymously or any work contracted to an employee. Transfer of copyright was also defined so

that by signing a legal document, copyright ownership could be transferred to another party. The new copyright law automatically protected works created by a party, even if they were not yet registered with the U.S. Copyright Office. However, to pursue a copyright infringement case, the party must register their work with the U.S. Copyright Office. Additionally, other minor clauses are associated with the Copyright Act of 1976 [3].

3.2. Digital Millennium Copyright Act

The Digital Millennium Copyright Act (DMCA) was enacted by Congress in 1998 to protect the rights of digital content. One goal of this law was to enact two World Intellectual Property Organization (WIPO) treaties that had been passed in 1996. Another goal of this law was to update the legislation of copyright management, needed because of the increasing popularity of file sharing over the Internet. The DMCA mainly consists of copyright circumvention legislation under two different areas of prevention. "Access protection restricts unauthorized users from accessing the work, while copy protection prevents unauthorized users from copying the work. This is an important distinction in the legislation." [4] The DMCA provides rights, guidelines and exemptions for both producers and consumers of digital media.

The DMCA contains five different sections, called titles. Each section has its own purpose, goal and objective. The first section, Title I, added amendments to the law to comply with several WIPO copyright treaties, and created new restrictions for the circumvention of copyright protection methods. Title II protects Internet Service Providers (ISPs) from prosecution if their subscribers commit copyright violations. Title II also forces each ISP to create acceptable use

guidelines concerning copyright violation. Title III states that any user can copy a program if their computer is either broken, damaged or under repair under the condition that they destroy the copied software after repair and reinstallation. Title IV grants an exemption for the creation of a temporary copy of media that is intended to facilitate transmissions, assuming a broadcasting license has been granted. Title V is irrelevant to our study (for example, it includes a provision that any vessel under 200 feet can't display a trademarked image [5]).

The DMCA has been used in many litigations including one high profile case involving Russian citizen Dmitri Sklyarov. As an employee of ElcomSoft, he developed software that would let users disable restrictions on an electronic book (eBook) for purposes such as using the read-aloud function of an eBook reader. When he went to Las Vegas to deliver a lecture about the weaknesses of Adobe's eBook software, he was arrested for violating the DMCA due to his work at ElcomSoft. However, he was not breaking any law in his home country of Russia or any international laws. Nor was he violating copyright laws. After Adobe withdrew its complaints and dropped charges, the US Government dropped charges against Sklyarov in exchange for his testimony against ElcomSoft. At the trial, ElcomSoft was found not guilty of copyright violations, which led to an exception of the DMCA [6].

Another high profile case in which the DMCA was cited is that of Lenz v. Universal. It involved the use of the song "Let's Go Crazy" by Prince in a video uploaded to YouTube.com. The video Lenz uploaded was a 29 second clip of her son dancing to the Prince song, which could barely be heard in the background. On June 4, 2007, YouTube received a takedown notice for the video from Universal on behalf of Prince. Interestingly, the takedown was not based on any belief that

the video infringed on copyright, but rather on the belief that Prince had a right to have his music removed. Lenz argued that her video was fair use of Prince's song. Additionally she argued that the fair use of something is legal to use under copyright law. Universal believed they could send a takedown notice, and were not required to evaluate if the content in question was being used under fair use guidelines. Eventually, the judge dismissed the case because it was fair use of Prince's song, noting that the clip should go back on YouTube. The court also ruled that copyright owners have to determine if an item in question is being used under fair use before sending a takedown notice. Lenz reacted by counter-suing Universal for legal costs incurred by the case [7].

There are exemption rules of the DMCA that are updated every three years to reflect current issues and technological developments, with six exemptions currently in place. The first exemption states that the copyright of audiovisual material can be circumvented if it is used for educational purposes. The next two exemptions state that copyright can be ignored for damaged or obsolete computer programs and video games. Another exemption is that copyright of eBooks can be disregarded for the use of screen readers or the read aloud functionality. The fifth exemption is that the user of a wireless telephone can update its firmware to connect to a new network if carriers are changed. The last exemption is that CD protection methods can be broken for the purpose of determining security flaws and vulnerabilities that may affect the user's computer [8].

The timeline of the DMCA is as follows [9].

• 1998	The DMCA was passed on October 12th and was made a law on the 28th.
• 1999	Connectix was sued by Sony because their software, Virtual Game Station, allowed playback of PlayStation Games.
• 2001	Ed Felten and his research team were pressured over their work with audio watermarking by the Secure Digital Music Initiative.
• 2001	ElcomSoft programmer Dmitry Sklyarov was arrested over his work on a software program that converted Adobe e-books to PDF.
• 2002	A group of open source programmers were sued by Blizzard over the 'bnetd' program they created to play Blizzard games online against each other.
• 2004	The development and sale of DVD X Copy, a program that allowed users to make backup copies of their DVDs, was shut down by MGM studios.
• 2006	The Sony BMG rootkit scandal infected many computers worldwide. This could have been prevented, as researchers were not comfortable disclosing this information due to liability reasons regarding the DMCA.
• 2008	Real Networks tried to develop software similar to DVD X Copy, but the DVD Copy Control Association halted further progress due to a lawsuit.

3.3. Prioritizing Resources and Organization for Intellectual Property Act

Due to the rise in piracy and copyright infringement, more detailed laws and harsher penalties for breaking copyright were required to help discourage piracy and punish offenders more effectively. These circumstances motivated President George W. Bush to sign the Prioritizing Resources and Organization for Intellectual Properly (PRO-IP) Act on October 13, 2008. The goal of this bill was to amend U.S. intellectual property laws and facilitate inter-agency management of copyright and intellectual property [10].

The PRO-IP Act consists of five different titles. Title I updates laws regarding civil intellectual property, and amends copyright laws concerning personal property and trademarks. Title II revises penalties regarding criminal violations of copyright. Title III creates a new government organization called the Inter-agency Intellectual Property Enforcement Advisory Committee,

charged with the task of coordinating the campaign against piracy. Title III also requires the President to appoint an Intellectual Property Enforcement Coordinator (IPEC), who will lead this committee. Title IV updates the Computer Crime Enforcement Act and reserves capital so the Department of Justice can employ and train additional law enforcement officers and fund future copyright enforcement projects. Title V adds miscellaneous requirements regarding status reports and the prioritization of copyright enforcement [11].

4. Movie Industry

The movie industry initially consisted of only movie theaters, where individuals would have to go to a theater to watch a particular movie. This restricted viewing to a certain time and place, by offering a set number of showings per day at a particular location. Eventually, the movie industry discovered they could make a profit from consumers who desired to watch movies at home. Selling physical copies of movies became popular as consumers who paid for a movie once were able to watch it multiple times. This market quickly expanded to rental stores, on-demand viewing and eventually Internet-based viewing.

4.1. Video Home System

Video Home System (VHS) tapes, released in the late seventies, were the first widely available products to offer home multimedia storage. Sony's Betamax, which was developed at a similar time, was a slightly better medium, but never caught on for various and well documented reasons [12]. One reason was that VHS technology developed faster than Betamax technology. Initially, both VHS and Betamax could store up to an hour of video. However, VHS tapes quickly increased their available play-time to two, and soon after, four hours. The four-hour capacity of VHS tapes made it the perfect medium to record movies, whereas Betamax tapes did not yet have this capability. Another deciding factor was that Sony blocked adult material from being put on Betamax, whereas the Adult Entertainment Industry found a big market with VHS tapes. The combination of these factors ensured the demise of Betamax [12].

VHS tapes, in combination with a Videocassette Recorder (VCR), allowed users to record television programs for later viewing and provided a way to watch major motion pictures at home. Initially, there was a strong opposition to VHS and Betamax format from the movie and television studios, due to the alleged copyright infringement of videocassette recording.

The allegations from the movie industry against video recording technology led to a lawsuit against Sony by Universal [City] Studios. This lawsuit dealt with the issues of fair use regarding copyright law and this technology. Universal believed Sony violated copyright law by allowing owners of VHS or Betamax tapes to record copyrighted materials from commercial broadcasts. Eventually, the Supreme Court decided that using VHS or Betamax tapes to record television did not violate copyright laws and that it was fair use to record television shows or movies [13].

4.2. Content Scrambling System

During the transition period from VHS tapes to DVDs, studios and distributors were seeking a way to protect DVD content. Since VHS tapes didn't have any type of copy protection, anyone with a VCR could record television shows and copy movies to a VHS tape. Distributors wanted to make it harder, if not impossible, for home viewers to record television and copy movies. Thus they looked for ways to incorporate some type of content protection into the new generation of video format, the DVD.

This new protection was called the Content Scrambling System (CSS). CSS uses a variety of keys and encryption algorithms to protect DVDs [14]. Every DVD player is embedded with a

player key unique to its manufacturer. Each player key must be obtained from the DVD Copy Control Association (DVD CCA) prior to becoming an authorized DVD player manufacturer. Additionally, every disc is embedded with two types of encrypted keys, the disc key and multiple title keys. When a DVD is inserted in an authorized player, the disc key is decrypted using the player key. The unencrypted disc key is then used to decrypt the title keys. Each title key is then used to unscramble a particular file contained on the DVD. Finally, video files are unscrambled on-the-fly as they are played [15].

When CSS was first introduced only closed source operating systems could read and play encrypted DVDs. The DVD playback source code was denied to developers of open source operating systems, such as Linux, as this would have quickly led to public availability of the source code. Fifteen-year-old Norwegian Jon Johansen was frustrated that he could not play retail DVDs on his Linux computer and decided to write a program that would allow him to do so. Surprisingly, it didn't take very long for Johansen to crack and decode CSS. He shared his findings with others involved in Linux media player development, which resulted in the distribution of this code throughout the Internet. Due to a complaint from US based DVD CCA and the Motion Picture Association of America (MPAA), Johansen was tried multiple times for his involvement in breaking CSS, but was acquitted each time [16].

DVDs released today still use CSS as part of their copy protection, allowing them to be easily copied. This copy protection system cannot be changed as everyone who owns a DVD player would need to buy new hardware to play the same media with a different copy protection scheme. As a result, movie studios have been unable to protect their DVDs. The speed at which

CSS was broken shows that neither it nor future schemes may prove to be very effective at the protection of content. This trend toward ineffective protection continued when the protection used on Blu-Ray discs[1] was broken within two years of its release. Movie studios and developers hoped that Blu-Ray protection would not be broken for at least ten years. However, developing technologies, such as powerful computers, in addition to skilled crackers, continue to allow copy protection methods to be broken faster than expected as in the case of Blu-Ray discs.

[1] "Blu-ray Disc (also known as Blu-ray or BD) is an optical disc storage medium. Its main uses are high-definition video and data storage. The disc has the same physical dimensions as standard DVDs and CDs." [http://en.wikipedia.org/wiki/Blu-ray_Disc]

5. Music Industry

The music industry developed to help musicians distribute their content. The release of records allowed this industry to develop rapidly, as it was the first time that sound could be recorded and played back at a later time. Over time, better storage methods were developed that made it easier to manufacture, distribute and enjoy music. The music industry has endured a great deal of technological advancement, moving from storing data on vinyl records to magnetic tapes, and finally to today's digital audio formats. The popularity of the music industry continues to grow as modern distribution methods make it very easy for anyone to acquire music.

5.1. iTunes

iTunes, developed by Apple Computer Inc., is a free application that allows users to download, organize and play many types of multimedia, including music, television shows and movies. Any Windows or Macintosh user can download this program from the Internet. Users can import any previously acquired music from both digital and physical sources free of charge. To enhance the iTunes experience, Apple's extensive online store allows users to browse, preview and purchase multimedia content. Most individual music tracks cost $0.99, while buying whole albums offers a slight discount. Television shows typically cost between one and four dollars, with price variations due to iTunes specials or picture quality. Movies cost between three and twenty dollars, depending on whether you rent or buy the movie or if it is an iTunes special [17].

iTunes is unique as it is the largest and most successful online multimedia store to date. The iTunes software (Mac only) was introduced in January 2001 and was followed by the

introduction of the most popular portable music player, the iPod, in October 2001. A Windows version of iTunes was released two years later in October 2003. The iTunes store was opened in April 2003 and quickly became popular. This was due to the fact that iTunes already worked with a physical player, the iPod, making it the most streamlined process for transferring music to a digital audio player [18].

Apple realized there was a potential for music piracy, and quickly developed a complex DRM scheme, called FairPlay, to protect music distributed through iTunes. When you create or activate an iTunes account on a new computer, iTunes generates a unique authorization number for that computer. Up to five computers can be authorized simultaneously using the same account. During a purchase, iTunes facilitates DRM with 'keys', which are used to encrypt each song. When you purchase a song, a 'user key' is generated and downloaded with the song. Also included with the download is a 'master key', which is used to encrypt the file. Upon downloading, the song is scrambled by your computer using the 'master key'. The 'user key' and 'master key' are stored on Apple's servers and locally by iTunes in an encrypted key library. When the song is played, your 'user key' is used to decrypt the 'master key'. Finally, the decrypted 'master key' is used to un-scramble the song data and the song is ready for playback [19].

Any track that uses Apple's FairPlay DRM is subjected the following set of restrictions; each track may be copied to an unlimited number of iPods or iPhones; each track may be played on up to five authorized computers simultaneously; each playlist containing tracks with DRM may be burned to a CD up to seven times. This limit is to help combat mass duplication and distribution.

Any single track may be burned to an audio CD an unlimited number of times without DRM [19].

These conditions offer each user a great deal of control over their music. Consequently, most users don't even notice that they are using a system with DRM. However, the number of users who oppose DRM, in any form, is growing. Apple's stance on this issue is similar to the opinions of iTunes users, as both parties would like to see all music DRM-free. Users don't want DRM because it would tie their music to a specific account or computer. Apple initially only offered iTunes songs with their proprietary FairPlay DRM because the licensing terms with music labels required Apple to have some form of protection for their music. However, Apple now discourages DRM as they believe music should be playable on any computer or device at any time, without any restrictions [20][21].

This makes iTunes unique, as many other online multimedia stores employ DRM. Recently Apple has begun to provide DRM-free music from certain record labels at a higher quality for the same price. The shift of quality in the DRM-free music offers users an incentive to buy, or upgrade to, DRM-free music. Apple's philosophy is that multimedia should be DRM-free, but they use DRM on this content if it is desired by the record label [22]. On January 6, 2009, Apple announced that they would begin to offer every track DRM-free and discontinue selling tracks with FairPlay DRM in April 2009, as they were able to negotiate with record labels to provide music DRM-free. They also announced that users will have the option to remove DRM protection from their music by paying a small fee for each song [23].

The iTunes music store has been the most successful online multimedia store because it offers a wider range of songs and services. The only true competitors to the iTunes store are the revised (and now legal) Napster and Amazon. The Amazon store is the closest model to the iTunes store. Users can browse Amazon.com to preview and purchase tracks, all of which are DRM free. The album and individual track prices closely resemble those on iTunes. This model could rival the iTunes model because Amazon offers totally DRM-free music at the same price as iTunes DRM enabled music. Napster originally allowed anyone with an Internet connection to download music illegally, but now they use a model similar to iTunes and Amazon. Napster also offers a subscription-based model. Users who choose the subscription-based model pay a monthly fee for an unlimited amount of music. However, when a subscription lapses, the music can no longer be played.

A basic timeline of online music stores is as follows [18].

• 1/ 9/2001	Apple introduces iTunes
• 10/ 23/2001	Apple introduces iPod
• 4/28/2003	Apple opens iTunes music store
• 5/19/2003	Roxio uses the newly acquired Pressplay to re-launch Napster
• 10/16/2003	Windows support added
• 2/6/2005	Napster launches Napster-to-go
• 5/2006	Napster launched free.napster.com
• 5/29/2007	Apple adds DRM-free music for $1.29 (iTunes plus/Higher Bitrate)
• 9/25/2007	Amazon MP3 store opens, offering DRM-free tracks for $0.99
• 10/16/2007	Apple drops price of DRM-free tracks to $0.99
• 1/6/2009	Apple announces they will remove all DRM from the iTunes music store by April

5.2. Sony XCP

DRM in audio compact discs (CDs) has never been very effective. Just as with floppy discs, the first audio CDs released did not contain any copy protection. However, as audio CDs became more popular, record labels sought ways to deter copyright infringement. Early attempts at copy protection for audio CDs were flawed and easy to bypass through simple methods, such as marking the perimeter of the disc with a permanent marker or holding down a key while inserting the disc into your computer.

Sony, one of the largest producers of audio CDs, realized that these methods weren't protecting their audio CDs very effectively, so they licensed commercially available products from two companies specializing in DRM. These two companies, First 4 Internet and SunnComm, developed Extended Copy Protection (XCP) [24] and MediaMax CD-3 [25] respectively. Sony hoped these copy protection schemes would be an effective way to manage their digital rights, but a fundamental flaw in the two schemes led to a commercial debacle [26].

In June 2004, Sony began selling CDs with MediaMax and XCP copy protection. 52 CDs were released with XCP and 50 CDs were released with MediaMax. Both copy protection schemes were designed to install hidden software that would monitor and prevent unauthorized actions, such as copying the CD more than three times or ripping the music to MP3. Both of these protection schemes could be considered malware because they disrupt the normal functionality of the user's computer without prior authorization. An unintended side effect of this software opened a security hole, which allowed other programs, such as viruses, Trojan horses and other

malware, to access and compromise the integrity of a system. Also known as a rootkit,[2] this defective software would also consume a significant amount of system resources, slowing the entire system down. Unfortunately, it took more than a year for security experts to detect this flaw [27].

This software was malicious because it installed itself without the users knowledge and couldn't be easily uninstalled. Shortly after the rootkit was discovered, Sony provided an uninstaller that would remove their intrusive software. However, the uninstaller was also flawed, creating a larger disaster. After running the uninstaller, the users' system was even more compromised than before. It's been estimated that XCP and MediaMax infected over 500,000 computers by 2006. Sony finally released a properly working uninstaller that completely removed the rootkit software [28].

Many individuals decided to sue Sony over their rootkit software and these cases were granted class action status on December 1, 2005. As a result, Sony agreed to compensate anyone who purchased a MediaMax or XCP CD and to provide an appropriate uninstaller. Sony also agreed to recall all infected XCP CDs and replace them with DRM-free CDs. Purchasers of MediaMax protected CDs were given one free download to replace the infected CD as well as an additional MP3 album download. XCP victims were provided either three free album downloads or a $7.50 compensation and one free album download [29].

---

[2] "A rootkit is malware which consists of a program (or combination of several programs) designed to take fundamental control (in Unix terms "root" access, in Windows terms, "Administrator" or "Admin" access) of a computer system, without authorization by the system's owners and legitimate managers." [http://en.wikipedia.org/wiki/Rootkit]

Due to Sony's DRM mishaps, other record labels have been hesitant to adopt copy protection schemes. Even though newer DRM programs are not as invasive or stealthy as XCP or MediaMax, they are seldom used to protect music CDs. Although some labels still use DRM, a growing number believe that DRM may not be worth the tradeoff between company interest and consumer satisfaction. As a result, the music industry is moving towards offering all music DRM-free. Consumers prefer DRM-free music as it offers them total control over the use of their music.

The timeline of the Sony rootkit is as follows [30][31].

• 6/2004	Sony begins selling CDs with XCP/MediaMax protection
• 10/31/2005	Mark Russinovich, security researcher for Microsoft's Sysinternals website, discovers Sony's rootkit and posts information about it on his blog.
• 11/3	Sony releases 'patch' that supposedly removes the rootkit. Ed Felten analyzes 'patch' and determines that it doesn't work.
• 11/6	Russinovich confirms and shows rootkit sends information to Sony.
• 11/9	BitDefender finds Trojan horse that exploits XCP flaws.
• 11/10	US Homeland Security comments that XCP uses some open source components, which is an infringement of these components.
• 11/11	Sony stops shipping CDs with XCP.
• 11/12	MediaMax threat discovered.
• 11/13	Researchers discover uninstaller has security issues.
• 11/15	Sony recalls infected CDs.
• 11/16	Unsecure uninstaller removed from Sony website.
• 11/17	MediaMax installer discovered to be unsecure as well. Amazon offers refunds to purchasers of XCP/MediaMax CDs.
• 11/18	List of all MediaMax infected titles released and exchange for 'clean' CDs/MP3s offered.
• 11/21	EFF files class action lawsuit against Sony. New MediaMax uninstaller released.
• 11/29	Newsweek announces that Sony knew about the rootkit since October 3rd.

• 12/6	Sony releases working rootkit uninstaller.
• 2/8/2006	Class action lawsuit overturned in lieu of private lawsuits.

6. Game Industry

When games were first becoming popular, DRM did not exist. Even though DRM was developing rapidly in other industries, it was falling behind in the game industry. The complexity of the hardware made it difficult for developers to design and program games even without DRM. Consumers knew very little about the hardware or how to copy or reverse engineer the software at this point. However, the progression of time and technology made it easier to crack and duplicate games in general. Newer technology has forced the game industry to rapidly develop and implement complex piracy prevention methods. Since DRM in the entire game industry encompasses hundreds of consoles and protection schemes, we have restricted our focus to the current DRM methods of PC games.

6.1. SecuROM

SecuROM is a copy protection method created by the Sony Digital Audio Disc Corporation and is commonly used to protect computer games. According to the SecuROM website, this product has two forms of copy control for disc based media. The first type of control is achieved through software that uses robust encryption. The second and more complex type of control is achieved through hardware. In the manufacturing process, a unique disc signature is embedded on each disc. During the initial launch of the protected application, a validation routine is run to ensure that the disc is authentic. This authentication occurs when the unique signature has been detected, meaning that the disc was manufactured by a SecuROM authorized facility. If the disc does not pass authentication, an error message will be displayed informing the user that the program will not launch. SecuROM also offers online product activation, which is similar to

disc-based verification. Under this method a license is obtained through online activation, saved to your computer and then checked upon execution of the application. If the license is valid, the program will launch [32].

Game publisher Electronic Arts (EA) Games is known for using SecuROM in their games including The Sims, BioShock, Mass Effect, Spore and recent titles in the Command & Conquer series. Rockstar North, a subsidiary of Rockstar Games, uses SecuROM for popular titles such as Grand Theft Auto: Vice City and Grand Theft Auto: San Andreas. Unreal Tournament 2003 and 2004, made by Atari, also use SecuROM [33]. As one of the largest copy protection methods available, many software publishers choose SecuROM to prevent average users from violating the terms of use. Although advanced hackers have broken most protection schemes, SecuROM has deterred most of their users from illegally distributing and acquiring games.

In the past few years, there have been numerous controversies over SecuROM. It has created numerous problems for gamers as well as many controversies which have led to legal cases against SecuROM and the respective game publisher. The biggest SecuROM controversy was over the game Spore, published by EA. Even before this game was released, many gamers complained about the use SecuROM in Spore, and EA's games in general, due to their past experiences with SecuROM. Initially, EA announced that Spore would be using a modified version of SecuROM where Internet authentication would occur every ten days. Additionally, each product key could only be used on a maximum of three computers. After angry gamers flooded retail web sites such as Amazon.com with negative reviews due to their use of

SecuROM, EA changed this copy protection. EA appeased consumers and allowed each product key to be activated on up to five computers. Additionally each user was provided the ability to deactivate any of their activated computers. We believe that because users were unwilling to deal with SecuROM's excessive protection scheme, cracked versions of Spore, without SecuROM, were downloaded illegally at least half a million times on BitTorrent[3] sites within a week of the game's release [34]. Consumers who purchased Spore with SecuROM found that the DRM used in Spore has aspects similar to a rootkit[2]. They discovered that some components are specially hidden and aren't removed with the uninstallation of Spore. This led to a class action lawsuit against EA, which is still pending, as SecuROM was not disclosed in the game packaging and the user wasn't given the option to approve the installation of its hidden components [35].

There have been numerous other cases regarding the use of SecuROM in computer games. However, many of these controversies have been over games that used a modified version of SecuROM and dealt with the invasive and undetectable nature of the "rootkit" installer. Expansions of The Sims 2 were protected by SecuROM and had severe problems such as incorrect program execution, optical drive malfunction, interference with antivirus programs, and even complete system failure. BioShock was released with SecuROM including custom activation and install limitations. Shortly after launch, gamers discovered that BioShock included software that exhibited rootkit-like behavior. However, it was later proven that there

[3] "BitTorrent is a peer-to-peer file sharing protocol used to distribute large amounts of data. The initial distributor of the complete file or collection acts as the first seed. Each peer who downloads the data also uploads them to other peers. Relative to standard Internet hosting, this provides a significant reduction in the original distributor's hardware and bandwidth resource costs. It also provides redundancy against system problems and reduces dependence on the original distributor." [http://en.wikipedia.org/wiki/BitTorrent_(protocol)]

was no rootkit present in BioShock's installation. After the false rootkit accusations, 2K Games decided that customer satisfaction was more important than DRM. The activation and install limits for BioShock were removed a year after its release in order to appease customers. These are only a few examples in which SecuROM has been a problem. Many other cases exist, although not all of them have had as great an impact on the gaming community [36].

6.2. StarForce

StarForce is professional copy protection software designed to discourage software piracy. StarForce is well-known by gamers for its invasive techniques which can cause problems such as optical drive failure. There are several different variations of StarForce and each is designed to protect content at different levels.

The most basic copy protection software offered by StarForce is FrontLine (FL) Disc. FL Disc includes features such as basic protection from unauthorized cracking, emulation or copying. There are several tiers of protection for FL Disc, ranging from basic CD based protection to a higher level of protection that is successful in deterring highly skilled hackers. FL Disc can protect both Compact Discs (CDs) and Digital Versatile Discs (DVDs) depending on the licensed tier.

The next tier of copy protection above FL Disc is FL Universal. FL Universal offers most of the same features as FL Disc in addition to the ability to protect content that is not distributed via physical media. This is achieved through online serial number verifications. FL Universal

features, such as the number of times the user can activate the game and how long before reactivation is required, can be customized by each game publisher. The online portion of FL Universal is another type of copy protection offered by StarForce, called FL ProActive.

As a subset of FL Disc and FL Universal, DiscFree technology provides additional features for the game publisher to provide customized options for the gamer. DiscFree allows a gamer to play the game without the need to have the original disc. DiscFree also allows a gamer to create an archival backup of the original game disc. The only time the disc needs to be in the drive is during the initial installation and during the first launch of the game. This feature reduces the wear and tear on the disc and the optical drive, as well as providing a faster launch time and decreased system resource usage compared to StarForce DRM without DiscFree technology [37].

Of all the copy protection software packages available to game distributers, StarForce is arguably the most invasive technology and has a bad reputation among gamers. However, StarForce is different from other game related DRM controversies. Other copy protection software schemes, such as SecuROM, created issues that were caused by modifications of the licensed copy protection software. StarForce related problems were caused by the way StarForce was designed and not by modification of their software. Protection Technology, developer of StarForce, could be blamed for DRM related problems, instead of the game publisher.

Among the problems present with this software were hidden drivers that could not be uninstalled, security issues, optical drive failure and general system corruption. However, no

lawsuit was filed against Protection Technology. Instead, a five million dollar class action lawsuit was filed against Ubisoft for using StarForce protection in their games. Eventually, the case was dismissed and Ubisoft discontinued the use of StarForce. Several other game publishers have stopped using StarForce, partly due to the outcome of this trial and partly due to gamer complaints [38].

6.3. Steam

Steam is a digital distribution platform developed by Valve, which launched on September 12, 2003. Steam is used for the Internet-based distribution and DRM management of PC games running on Windows. It can be downloaded free of charge from their homepage. Once installed, Steam allows users to purchase and download games from a large game library. Downloaded games must be launched through Steam. Steam can also be used as a game manager for games purchased in physical media form. In this case, Steam is only used to launch the game and does not affect the DRM scheme used for that particular game [39].

Steam offers many features that facilitate the gaming experience for its users. One basic feature is that the Steam store is automatically opened when Steam is opened. An external browser is not required to download content, so users can browse through the game list and download any game through Steam. Upon browsing through different tabs, users can view a list of their installed games and are able to launch these games within Steam. Users can also view a list of available multiplayer game servers, and upon joining a server, Steam will automatically run the game and join the server.

Steam also has the ability to start in an offline mode, which offers users the ability to play single player games without being connected to the Internet. However, a game must be updated to the latest version before it is available to play in offline mode. Many features are disabled in offline mode, so most users choose to stay in online mode. Offline mode mainly appeals to users with slower Internet connections, or in situations where the Internet or Steam servers are temporarily unavailable. Another useful feature Steam provides is the ability to backup games that have been downloaded. Users are able to open the backup wizard, where they can customize various backup options including which games to backup, and the automatic separation of files for disc bound backups. After a backup is complete, it can be used to restore game content without the need to download the entire game again. Instead, you simply run the executable provided by the backup wizard while you are in online mode, and the games are restored to the game list.

When Steam was launched in 2003, only a few games were available because Valve was only allowing their own games to be released. Those available included Counter Strike, Day of Defeat, Half-Life, and Team Fortress. Over the next two years, Valve released several new games through Steam, including a sequel to Half-Life and a remake of Counter Strike. Starting in 2006, Valve allowed other game publishers to release their games through Steam. These included several games originally published in physical form by Activision. In the following years, the number of games released through Steam increased significantly. This is partially due to the fact that other game developers are beginning to launch games on Steam and in physical form at the same time. Additionally, many older games continue to be re-released on Steam [40].

Steam automatically manages DRM for any game purchased and downloaded from the Steam store. This DRM is Internet-based and verifies that the copy of a particular game is legitimate upon launch. Additionally, Valve games that are purchased in physical form include a unique Steam code, and upon installation, users input this code, which registers the game with Steam. After registration, the physical copy is no longer required to play the game. The only requirement to play a purchased game is to logon to Steam with your unique username and password.

7. DRM Models

Through exploring the DRM usage by various entertainment industries we have found that clear models have emerged which effectively describe the behavior of how different types of DRM work. Each DRM model is unique, and each provides certain benefits and drawbacks for both producers and consumers. We have analyzed a number of them and will discuss them here. We have stayed objective while identifying each DRM model so that we can effectively compare and contrast these models.

7.1. Media-based DRM

The first effective DRM method for physical content was media-based DRM. These first attempts at DRM were primitive, yet effective at protecting content. Methods such as Macrovision's[4] analog copy protection as well as user-interactive instruction manual based protection schemes made it difficult to enjoy illegally acquired content. This technology made its way from analog mediums to digital mediums, first with CDs, then DVDs, and eventually Blu-Ray discs.

These media-based DRM schemes provided several benefits, including the ease at which it could be included on most types of media and integrated into the final product. Additionally, no hardware upgrades ever are necessary to use media-based DRM multimedia. On the other hand, there are fundamental weaknesses with this media-based system. Since this form of DRM

[4] "Macrovision has licensed to publishers a technology that exploits the automatic gain control feature of VCRs by adding pulses to the vertical blanking sync signal. These pulses do not affect the image a consumer sees on his TV, but do confuse the recording-level circuitry of consumer VCRs." [http://en.wikipedia.org/wiki/Copy_protection#Copy_protection_for_videotape]

cannot be changed after the manufacturing process is complete, it only needs to be broken once per product to make it available to everyone for illegal use. Furthermore, any issues or problems with the DRM cannot be easily fixed. Effective media-based DRM can also be costly to develop.

To evaluate media-based DRM, we need to consider several perspectives. The *consumer* point of view regarding this type of DRM is the most varied among current DRM methods ranging from transparent and satisfactory DRM to intrusive and inadequate DRM. When a new media-based DRM scheme is first cracked, it becomes very easy for crackers to break similar and future versions of that same DRM method. Once a particular item has been cracked, it is very easy to distribute copies through the Internet. Needless to say, consumers who don't plan on purchasing this product like this feature. On the other hand, for consumers who actually purchase a product, media-based DRM methods can be problematic.

Producers and distributors have a different point of view regarding media-based DRM. Their objective with this type of DRM is to protect copyrighted works to the best of their ability, and to cover the largest demographic of consumers. Overall, this type of DRM has not been effective as all types of media-based DRM are eventually broken. However, as this technology was developed before the Internet existed, it was the only feasible way to protect content on a large scale. Even though Internet-based DRM is becoming more popular, media-based DRM is still the best solution for target consumers who own the appropriate hardware.

Risks come with every form of DRM, and media-based DRM is no different. The main problem with media-based DRM is that once a particular scheme has been broken, it will always be broken. Distributors can lose a significant amount of money from their investment in DRM, especially if the product is cracked or pirated quickly after being released. Additionally, if a media-based DRM product has a significant problem, it can be very expensive and difficult to fix. The last main risk associated with media-based DRM is that some forms of copy protection have a bad reputation. Problems created by media-based DRM schemes can occur when installing or playing the game, and this can affect the sales of products released with this type of DRM.

7.2. Internet-based DRM

The continuous growth of the Internet has helped Internet-based DRM become a popular method of content protection for digital media. This DRM made its first major appearance with FairPlay in 2003. The next major appearance of Internet-based DRM was in the game protection technology used by Steam. Eventually, this form of DRM became the preferred method to protect many forms of multimedia distributed through the Internet.

There are several strengths of Internet-based DRM, including its rapidly attained success over other DRM methods. This success can be attributed to several factors, including the level of transparency that Internet-based DRM provides to the consumer, as well as the robust nature of Internet protection methods. Two main weaknesses of Internet-based DRM are the instability

and reliability issues associated with DRM servers (i.e. server downtime), as well as difficulties that users with low-speed Internet connections may encounter.

From the consumer perspective, Internet-based DRM has several annoyances. Restrictions for television shows and movies acquired digitally don't satisfy all consumers, rental times usually prevent further viewing 24-48 hours after the initial viewing, and multimedia can take several hours to download even with a fast Internet connection. Producers and developers favor Internet-based DRM due to the fact that it's easier to control content and retroactively fix issues or problems. The entertainment industry also favors this type of DRM, as continuous protection of their content is more effective than other methods of DRM. Using this method, it is also easy to determine the number of downloads and play counts. Internet-based DRM is successful since the detection of illegitimate content results in the immediate deactivation or deletion of content.

Several risks exist with Internet-based DRM as well. One big risk is that if any DRM servers have a problem or go offline, the Internet-based content may become unusable. The content also relies on an Internet connection to function properly. Another issue includes problems with re-downloading already purchased content as some online stores only allow one or two downloads. Additionally, many people like to have a physical copy of their multimedia, rather than just a digital copy. On the plus side, Internet-based DRM is more environmentally friendly than other methods of DRM because there is no packaging or manufacturing process.

7.3. DRM-free

The latest approach to DRM by the entertainment industry is DRM-free content. DRM-free multimedia has started becoming more popular due to consumer dissatisfaction with other troublesome DRM methods. Consumers are able to enjoy all aspects of DRM-free multimedia, including the lack of restrictions placed on content usage, future-proof content and problem free functionality.

Companies are finding that they can save money by not investing in DRM technologies. In addition the risk of a costly law suit and customer service expenses incurred trying to trouble shoot DRM problems for customers make DRM technologies less than attractive for publishers and distributors. However, DRM-free content offers no protection from piracy or copyright infringement and companies can easily lose money through illegal file sharing. This is especially true in the gaming industry. Unlike the movie or music industry, which get a significant amount of income from movie and concert ticket sales, the game developers rely more exclusively on retail sales. Consequently, game developers believe it's necessary to include some form of DRM with their product.

One risk associated with DRM-free content is that piracy is a substantial issue. However, a large percentage of multimedia with DRM is pirated as much as DRM-free content. One question for the industries has been whether the protection afforded by DRM content is worth the level of customer dissatisfaction. Another is whether the amount of money lost due to piracy is worth the cost of DRM technology. In short, DRM-free content appeases consumer demand while lowering the overall cost of a given product. Additionally, many companies are realizing that

content will be pirated regardless of whether or not DRM is used, and rather than risk a potential lawsuit of customer dissatisfaction, they are transitioning to DRM-free content.

7.4. Console-based DRM

The final DRM category explored in this report is related to consoles. Manufacturers need some way to protect their systems from being exploited to play unauthorized content. As console gaming progressed, more advanced protection mechanisms have been implemented. The first cartridge based games had no form of protection, and could easily be modified. Over time cartridges became more and more complex and became more difficult to copy or modify game content. Then the physical size of games increased to the point which made cartridges obsolete, as they had a limited storage capacity. Therefore, disc-based games have become the storage medium of choice for the past several generations of consoles, and have moved from CDs to DVDs, and now to Blu-ray discs.

Console manufactures use DRM to protect their assets, mainly by using hardware-based DRM. This form of DRM is hard to break, as only complex software modifications and physical hardware modifications can break this DRM. Manufacturers have complete control over console hardware, versus the lack of control over personal computer hardware, which allows them to use hardware-based DRM effectively. Since all consoles are manufactured identically, console DRM methods are more specialized and stronger than any PC DRM method. In addition, games are designed to work effectively with console DRM. This specialization makes console games

and hardware more difficult to break and allows consumers to enjoy console games without having to deal with any DRM-based issues.

8. Conclusion

Since we have completed the analysis of the movie, music and game industries and outlined several popular DRM methods currently in use, we are ready to form inter-industry comparisons that will support our thesis. We will compare and contrast DRM methods of the game industry to methods used in the music and movie industries. Finally, we will form predictions and make recommendations about DRM and its future in the game industry.

8.1. Movie Industry vs. Game Industry

A major similarity exists between the movie industry and the game industry, which is that both industries parallel one another in their content delivery systems. These industries rely mainly on a physical media-based distribution method, and have been slowly transitioning to digital content distributed via the Internet. Since either industry would not be able to profit from only providing digital content, they must continue to develop and sell products based on physical media. In both industries, digital distribution is becoming recognized as a new method for content distribution. Many manufacturers still continue to produce physical media, and additionally make this content available online to widen their consumer base and make more money in the process.

8.2. Music Industry vs. Game Industry

The DRM trends of the game industry have followed the DRM trends of the music industry. Initially, when portable music players became popular, music contained no DRM. The first games manufactured also contained no forms of DRM. Both industries continued to release products without DRM until piracy became an issue. Around this time, the music industry tried

to implement copy protection for CDs while the game industry had already developed copy protection for both CDs and DVDs. The music industry's attempt at copy protection was a failure, while the game industry experienced consumer dissatisfaction due to invasive DRM methods. Since the music industry had several different sources of revenue, they were less inclined to protect physical media with unpopular DRM, and have been willing to go DRM-free. However, the game industry has fewer alternative sources of revenue, which makes developers more inclined to protect their content with disc-based DRM.

In 2003, both industries once again followed similar paths with the launches of the Steam and iTunes online stores. Internet-based DRM was quickly becoming popular, and the music and game industries were transitioning towards this new form of DRM. Since audio content is smaller than game content, the music industry was able to expand digital distribution methods more rapidly than the game industry. However, shortly after online music distribution matured, the game industry began to embrace digital distribution methods. Recently, these methods have become more popular with consumers due to faster Internet connections and a wider selection of games.

8.3. Predictions

Looking at the history of the music and game industries, it is clear that the music industry is leading the game industry in terms of DRM usage. Music CDs have been mostly DRM-free for their lifespan. When the industry initially tried to use DRM, it did not work correctly, infected many computers and enraged consumers. Then, the success of iTunes demonstrated that

effective DRM could be implemented without any major issues. iTunes' initial DRM scheme was very effective, ensuring that songs downloaded from their store could only be played by the user who purchased the song. Eventually, iTunes provided some DRM-free music, and discovered that consumers would be willing to pay more for DRM-free music. Recently, iTunes has made all their music DRM-free to satisfy consumers and follow Apple's evolving prominence in the music industry.

The music industry developed internet-based DRM very quickly, but the game industry will be slower to reach this level of growth. We believe that the digital distribution of games will follow the same path that iTunes has taken. Currently, Steam offers a wide selection of games, all of which are protected by Steam's self managed DRM scheme. iTunes and Steam are similar as both DRM implementations are unobtrusive relative to other DRM methods. Additionally, both have similar content delivery systems. We predict that Steam will eventually follow in the footsteps of iTunes and offer DRM-free games. Our prediction is strengthened by the fact that recently some games have been released without DRM. The success of these games has shown developers that it doesn't matter if they use DRM.

Most current disc-based DRM methods are intrusive and have many problems. We believe that the future of DRM lies in Internet-based protection. Physical media will continue to be released to serve users without an Internet connection. These users should not be punished if they cannot register their game on the Internet, and DRM-free physical media would allow these users without an Internet connection to enjoy their games. Considering most gamers have an Internet connection, this should not be a large issue. Additionally, game developers would save money

due to the lack of investment costs for disc-based DRM. This is why we believe that disc-based games will eventually become DRM-free.

8.4. Recommendations

Since current DRM methods are flawed and have numerous problems, we believe that current methods will soon become outdated. We have devised a new model to encompass physical media as well as digitally distributed media, which will be based off a combination of previously successful models.

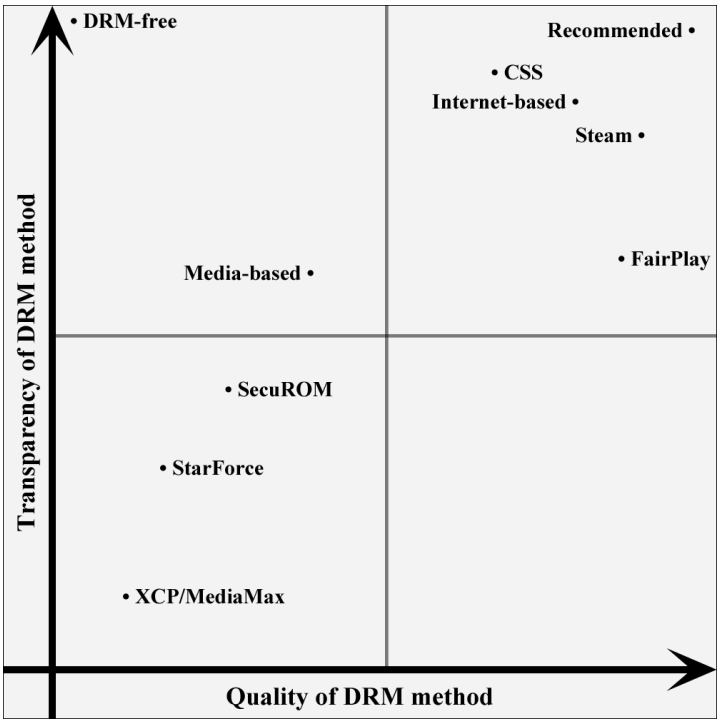
Currently, DRM for games is catered to developers' interests, rather than the interests of consumers. We have several recommendations for developers to consider when designing and implementing DRM strategies. Our first recommendation is that DRM should not be included on any physical media. Since current disc-based forms of DRM are an annoyance to gamers, removing this protection would satisfy consumers while saving development and related customer support costs.

Our second recommendation is that DRM for the game industry should transition to a completely Internet-based model. Apple's success with iTunes has shown that Internet-based DRM can appear transparent to the user. Through additional research, the game industry should be able to develop a successful model. Valve has already developed such a model, Steam, but there are still opportunities for improvement.

Under our new model, physical discs would not contain any forms of DRM, while digital content would utilize Internet-based DRM. However, we believe that physical copies should still include key-based validation under certain circumstances. Games installed on computers with Steam, or another supported digital distribution program, will require the program to validate the key. If a game supports online play, the digital distribution program will be required to validate the key before playing online. Otherwise, games containing no online content will not require DRM to play. Any game acquired through a digital distribution program will be automatically managed.

8.5. DRM Conclusions

To summarize all of the DRM methods we have analyzed, we created a chart to show the transparency versus the quality of each method, as well as how we view each method in relation to the others. The vertical axis represents the transparency of each DRM method, as the higher a method lies on the vertical axis, the more transparent it is. The horizontal axis represents the quality of each DRM method, as the further a method lies to the right, the more effective and robust it is. The point where both axes intersect represents a bad DRM method with no transparency. A point halfway up the vertical axis represents a DRM method that is noticeable, but not too intrusive. A point at the top of the vertical axis represents a DRM method that is fully transparent to the user. A point halfway along the horizontal axis represents a DRM method that offers satisfactory protection. A point all the way to the right represents a DRM method that offers excellent protection. Excluded from this graph are all issues regarding piracy and cracking, as DRM methods work effectively until they are cracked and the DRM protection becomes obsolete.



The music industry currently uses a successful Internet-based DRM model as past DRM schemes used on physical media have caused problems for consumers and have been ineffective. Additionally, the movie industry is currently using a successful model for Internet-based distribution. Due to the success of these models in the movie and music industries, we believe that future DRM models in the game industry will be well-balanced Internet-based models that satisfy developers, producers, distributors and consumers.

Glossary

Analog – Continuous representation of data

Bitrate – Data rate in bits per second

Blu-Ray Disc – High density storage disc with a maximum capacity of 50 gigabytes

BitTorrent – A peer-to-peer file transfer protocol

Game Cartridge – Self contained detachable data storage device

DVD Copy Control Association (DVD CCA) – An organization with the primary responsibility of licensing CSS technology

CD – Compact Disc, with a maximum storage capacity of 700 megabytes or 80 minutes of audio

Copyright – Rights granted to owners of unique intellectual property

Crack[er] – [One who] To remove, subvert or otherwise bypass copy protection

Digital – Discrete representation of data

"Don't Copy That Floppy" – A campaign to educate gamers about the issues of game piracy

DVD – Digital Versatile Disc, with a maximum storage capacity of 8.54 gigabytes

eBook – A digital representation of a book

EULA – End User License Agreement, a contract between a software producer and the consumer

Floppy Disc – A magnetic storage device with a maximum capacity of 1.44 megabytes

License – To grant permission of use

Linux – Open source operating system

Macrovision – A corporation that develops and licenses various copy protection methods

Malware – Software designed to harm a computer, such as destroying or corrupting data

Media/Medium – The term for a storage device that holds data

MP3 – MPEG-1 Audio Layer 3, a commonly used compression format for digital audio

on-the-fly – An operation that is performed spontaneously alongside other operations

Piracy/[Pirate] – [One who commits the act of] infringing upon copyright

Ripping – The process of copying multimedia content from an external source to a computer

Rootkit – A malicious program that compromises the security of a computer

Server – A computer dedicated to running a small number of programs for a particular purpose

TOS – Terms of Service, an agreement a user must accept before using a given service

WIPO – A U.N. organization created to promote international copyright protection

YouTube – An online, community powered, video sharing website

Bibliography

[1]. "How the Old Napster Worked." Howstuffworks. 28 Mar. 2009 <http://computer.howstuffworks.com/napster3.htm>.

[2]. Cunningham, Richard. "The Copyright Law Act Of 1976 Is Still Relevant In Today's Digital Age by Richard Cunningham." ArticleCity.com 7 July 2007. 15 Feb. 2009 <http://www.articlecity.com/articles/legal/article_987.shtml>.

[3]. "Copyright Act of 1976." Wikipedia, The Free Encyclopedia. 27 Nov 2008, 06:02 UTC. 15 Feb 2009 <http://en.wikipedia.org/w/index.php?title=Copyright_Act_of_1976&oldid=254374345>. .

[4]. Lounder, Jeremy N., and Brian G. Weber. "Sony Copy Protection." Dept. of Computer Science at Worcester Polytechnic Institute (2006).

[5]. THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998 U.S. Copyright Office Summary. United States of America. US Copyright Office. Dec. 1998. 17 Nov. 2008 <http://www.copyright.gov/legislation/dmca.pdf>.

[6]. LESSIG, LAWRENCE. "Jail Time in the Digital Age." Ne York Times. 30 July 2001. 17 Nov. 2008 <http://query.nytimes.com/gst/fullpage.html?res=9806e0d9123df933a05754c0a9679c8b63>.

[7]. Lenz v. Universal, No. C 07-3783 JF (UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA SAN JOSE DIVISION August 20, 2008).

[8]. "Digital Millennium Copyright Act." Wikipedia, The Free Encyclopedia. 17 Nov 2008, 10:35 UTC. 17 Nov 2008 <http://en.wikipedia.org/w/index.php?title=Digital_Millennium_Copyright_Act&oldid=252339959>.

[9]. Von Lohmann, Fred. "DMCA: Ten Years of Unintended Consequences." Electronic Frontier Foundation. 28 Oct. 2008. 17 Nov. 2008 <http://www.eff.org/deeplinks/2008/10/dmca-ten-years-unintended-consequences>.

[10]. Hengl, Suzanne. "Prioritizing Resources And Organization For Intellectual Property Act Of 2008." Baker Botts L.L.P. | Home. 16 Feb. 2009 <http://www.bakerbotts.com/file_upload/PrioritizingResourcesAndOrganizationForIntellectualPropertyActOf2008.htm>.

[11]. "Public Law, Summary." THOMAS (Library of Congress). 16 Feb. 2009 <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:SN03325:@@@D&summ2=1&>.

[12]. Owen, Dave. "The Betamax vs VHS Format War." Media College - Video, Audio and Multimedia Resources. 8 Jan. 2008. 28 Mar. 2009 <http://www.mediacollege.com/video/format/compare/betamax-vhs.html>.

[13]. Balio, Tino. "BETAMAX CASE." Museum of Broadcast Communications. 1 Dec. 2008 <http://www.museum.tv/archives/etv/B/htmlB/betamaxcase/betamaxcase.htm>.

[14]. Barry, Mark. "Cryptography in Home Entertainment - A look at content scrambling in DVDs." June 2004. 22 Nov. 2008 <http://www.math.ucsd.edu/~crypto/projects/markbarry/index.htm>.

[15]. "Content Scramble System." Wikipedia, The Free Encyclopedia. 24 Oct 2008, 22 Nov 2008 <http://en.wikipedia.org/w/index.php?title=Content_Scramble_System&oldid=247438970>.

[16]. Harmon, Amy. "Free Speech Rights for Computer Code?" New York Times. 31 July 2000. 22 Nov. 2008 <http://www.nytimes.com/library/tech/00/07/biztech/articles/31rite.html>.

[17]. "How iTunes Works." Howstuffworks. 11 Nov. 2008 <http://electronics.howstuffworks.com/itunes.htm/printable>.

[18]. "iTunes version history." Wikipedia, The Free Encyclopedia. 29 Oct 2008, 11 Nov 2008 <http://en.wikipedia.org/w/index.php?title=ITunes_version_history&oldid=248451305>.

[19]. Eran, Daniel. "How FairPlay Works: Apple's iTunes DRM Dilemma." RoughlyDrafted Magazine. 26 Feb. 2007. 11 Nov. 2008 <http://www.roughlydrafted.com/rd/rdm.tech.q1.07/2a351c60-a4e5-4764-a083-ff8610e66a46.html>.

[20]. Jobs, Steve. "Apple - Thoughts on Music." Apple. 6 Feb. 2007. 11 Nov. 2008 <http://www.apple.com/hotnews/thoughtsonmusic/>.

[21]. Markoff, John. "Jobs Calls for End to Music Copy Protection." New York Times. 7 Feb. 2007. 11 Nov. 2008 <http://www.nytimes.com/2007/02/07/technology/07music.html>.

[22]. "FairPlay." Wikipedia, The Free Encyclopedia. 7 Nov 2008. 11 Nov 2008 <http://en.wikipedia.org/w/index.php?title=FairPlay&oldid=250338773>.

[23]. "Changes Coming to the iTunes Store." Apple. 6 Jan. 2009. 28 Mar. 2009 <http://www.apple.com/pr/library/2009/01/06itunes.html>.

[24]. "Extended Copy Protection." Wikipedia, The Free Encyclopedia. 6 Nov 2008, 13:38 UTC. 15 Nov 2008 <http://en.wikipedia.org/w/index.php?title=Extended_Copy_Protection&oldid=250026907>.

[25]. "MediaMax CD-3." Wikipedia, The Free Encyclopedia. 28 Oct 2008, 01:35 UTC. 15 Nov 2008 <http://en.wikipedia.org/w/index.php?title=MediaMax_CD-3&oldid=248109143>.

[26]. Kantor, Andrew. "Sony: The rootkit of all evil?" USA Today. 16 Nov. 2005. 15 Nov. 2008 <http://www.usatoday.com/tech/columnist/andrewkantor/2005-11-17-sony-rootkit_x.htm>.

[27]. Pogue, David. "Sony BMG's Copy-Protecting Watchdog." New York Times. 9 Nov. 2005. 6 Dec. 2008 <http://www.nytimes.com/2005/11/09/technology/circuits/09POGUE-EMAIL.html>.

[28]. "Sony BMG CD copy prevention scandal." Wikipedia, The Free Encyclopedia. 16 Sep 2008, 05:10 UTC. 15 Nov 2008 <http://en.wikipedia.org/w/index.php?title=Sony_BMG_CD_copy_prevention_scandal&oldid=238745581>.

[29]. Marson, Ingrid. "Sony settles 'rootkit' class action lawsuit." CNET News. 29 Dec. 2005. 6 Dec. 2008 <http://news.cnet.com/sony-settles-rootkit-class-action-lawsuit/2100-1002_3-6012173.html>.

[30]. Methvin, Dave. "The Sony XCP Rootkit." PC Pitstop: Free PC Scans and Tune-up Utilities. 25 Nov. 2005. 15 Nov. 2008 <http://www.pcpitstop.com/spycheck/sonyxcp.asp>.

[31]. Doctorow, Cory. "Sony anti-customer technology roundup and time-line." BoingBoing. 14 Nov. 2005. 3 Dec. 2008 <http://www.boingboing.net/2005/11/14/sony-anticustomer-te.html>.

[32]. "SecuROM™ Frequently Asked Questions." SecuROM. 18 Nov. 2008 <http://www.securom.com/support_faq.asp>.

[33]. THE DAEMONS HOME, ed. "Game Database." THE DAEMONS HOME. 18 Nov. 2008 <http://www.daemon-tools.cc/dtcc/gamedb.php?letter=all>.

[34]. Ernesto. "Spore: Most Pirated Game Ever Thanks to DRM." TorrentFreak | Torrent News, Torrent Sites and the latest Scoops. 13 Sept. 2008. 19 Nov. 2008 <http://torrentfreak.com/spore-most-pirated-game-ever-thanks-to-drm-080913/>.

[35]. "Spore (2008 video game)." Wikipedia, The Free Encyclopedia. 19 Nov 2008, 16:30 UTC. 20 Nov 2008 <http://en.wikipedia.org/w/index.php?title=Spore_(2008_video_game)&oldid=252801483>.

[36]. "SecuROM." Wikipedia, The Free Encyclopedia. 18 Nov 2008, 20:07 UTC. 20 Nov 2008 <http://en.wikipedia.org/w/index.php?title=SecuROM&oldid=252632684>.

[37]. "Solutions for Multimedia Protection." Software Copy Protection, licensing and copy protection, DRM, Protect your software. 20 Nov. 2008 <http://www.star-force.com/solutions/all/multimedia/>.

[38]. Keiser, Joe. "Ten Most Annoying DRM Methods." EDGE. 1 Oct. 2008. 21 Nov. 2008 <http://www.edge-online.com/features/ten-most-annoying-drm-methods?page=0%2c3>.

[39]. "What is Steam." Welcome to Steam. 20 Jan. 2009 <http://store.steampowered.com/about/>.

[40]. "List of Steam titles." Wikipedia, The Free Encyclopedia. 20 Jan 2009, 22:11 UTC. 21 Jan 2009 <http://en.wikipedia.org/w/index.php?title=List_of_Steam_titles&oldid=265366302>.