A Survey of Digital Rights Management Technologies

Xiao Zhang, billchang.e@gmail.com (A project report written under the guidance of Prof. Raj Jain) Download

Abstract:

Digital Rights Management (DRM) refers to a broad category of access control technologies aimed at restricting the use and copy of digital content on a wide range of devices. We examine some recent and existing technologies that represent the standards of commercial DRM in most of mainstream media formats including film, e-book, broadcast TV, computer games and music. We discuss the architectures of these systems and their real world adoption and performances. We also look at some of the common pitfalls of DRM technologies and the attempts at building better systems.

Keywords:

Digital Rights Management, DRM, content, distribution, permission, metadata, restricted, protected, e-books, Blu-ray, HD-DVD, Advanced Access Content System, watermark, encryption, decryption, cryptography, Steam, Sony, OpenMG, Apple, FairPlay, Adobe, analog hole, PDF, piracy, FCC, lawsuit, EFF, Mobipocket, Topaz, Ereader, Microsoft, AACS, SecuROM, StarForce, vulnerability, incompatibility

Table of Contents:

1. Introduction

The term "Digital Rights Management" (DRM) is confusing and dividing in today's world. For publishers and rights holders, it can refer to all technologies that protect them from piracy. For the average content consumer, it usually means extraneous mechanisms that cause them inconvenience in normal use. For the pirates, it means the enemy that must be vilified and destroyed. But what exactly is this technology and what does it do?

DRM is defined as a broad range of technologies that grant control and protection to content providers over their own digital media. From the content's point of view, there are three key components to its life cycle: the creation of content, the distribution and upkeep of content, and the use of content. A good DRM scheme should account for all three components, and effectively define the interactions between the user, the permissions and the content itself. Figure 1 demonstrates this in more details.

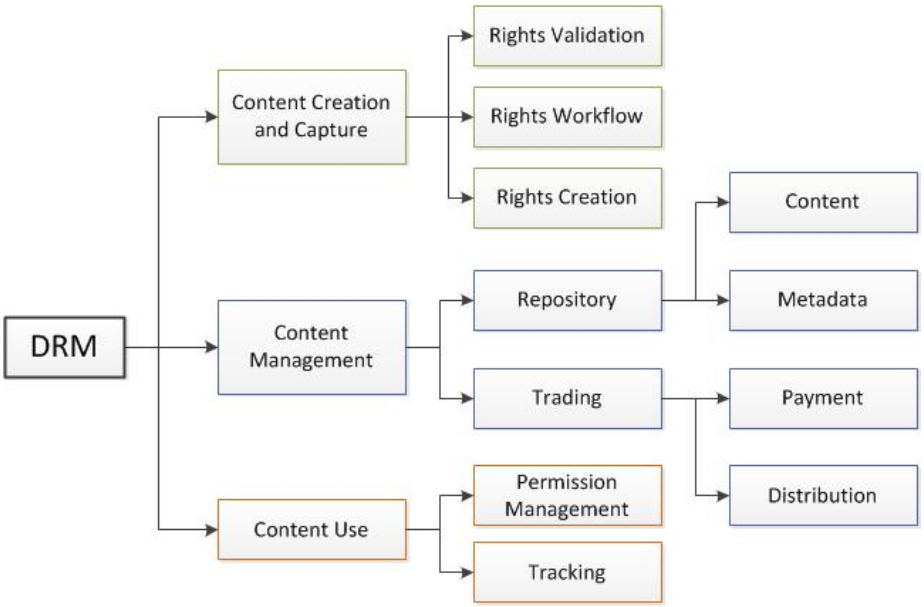

Figure 1. DRM functional architecture

When contents are created, the system needs to immediately ensure that rights are validated, assigned and approved to their owners. In the distribution and storage of content, the system needs to have proper access to the content and metadata, and manages the license and deals. After content has been traded, the system must enforce the rights associated with the content, by providing proper permissions to access, use and modification [Boucqueau07].

A main issue for DRM is the lack of standardized technologies. Furthermore, many traditional DRM technologies have been plagued by usability and legal problems, or suffer from attacks that render them completely useless. As a result, many publishers in the industry developed their own proprietary software to meet the individual needs of DRM in today's media standards.

In section 2, we will examine some existing as well as some recently retired technologies to understand the challenge in managing digital rights. Some of these systems, while trying to accomplish the goals of rights management, negatively affected the user experience in many ways, prompted controversies and criticisms among their customers. We will briefly discuss these here as well. Section 3 examines some general vulnerabilities of DRM systems, as well as the progress and attempts in designing better systems.

2. Recent and Existing Technologies

In the past decade, many DRM technologies have been developed within the industry, but very few have survived over the years. At its core, designing a DRM system is hard; the fundamental challenge lies in the fact that the system must exist on top of the media format itself. Different media formats have vastly different distribution, content creation, metadata and scopes of permissions. They pose different challenges in very different domains. We will examine some of the most popular commercial DRM schemes in film, broadcast TV, e-books, games and music.

2.1. Film Media

In the early days of DVD technologies, a DRM system called Content Scrambling System (CSS) was developed by the DVD Forum on film DVDs. It uses a simple encryption scheme designed to prevent byte-for-byte copying of a MPEG (digital video) stream. The key for the encryption is split and separately stored in the lead-in area of the restricted DVD and the DVD drive itself, and the encryption algorithm employs a proprietary 40-bit stream cipher [Schneier99]. The technology was first introduced in 1996, and was compromised in 1999 by a brute force attack. Like many other encryption algorithms before it at the time, the weakness of the scheme was blamed on the regulations placed on any exportation of cryptographic systems from the United States which limited systems to use keys of no more than 40-bit long [Schneier99][Grimmett01]. More recently, due to the rapid adoption of new media technologies such as HD-DVD and Blu-ray, new DRM systems today concern mostly with these platforms.

2.1.1. Windows Vista Protected Media Path

To the dismay of the anti-DRM advocates, Microsoft introduced many new I/O technologies into their new generation of OS in late 2006. Among them is Protected Media Path (PMP), a set of technologies designed to add a layer of access control to video and audio streams. It consists of two main subsets, Protected Video Path (PVP) and Protected User Mode Audio (PUMA).

Windows Vista uses something called the Protected Media Path - Output Protection Management (PMP-OPM), It is a redesign over the Certified Output Protection Protocol (COPP) introduced in Windows XP. PMP-OPM monitors all processes that access and produce media signals. A subset of PVP called User-Accessible Bus (PVP-UAB) encrypts video and audio data that are passed through the PCI-E bus, protecting it from any illegal interception before it reaches the graphics card. When a software process tries to access a DRM-restricted video stream, PVP will first check if the software is signed by Microsoft. If the process is unsigned, the access is automatically rejected. Even if a process is able to intercept the stream, it will not be able to use it due to the encryption [Ionescu07].

Protected Media Path has a crucial requirement that the graphics driver must have a way to identify whether the hardware is trustworthy - that is, if the device is allowed to play video with copy protection. There is a clear implication to this requirement: the driver must be signed by Microsoft in order to playback protected content. This has attracted criticism from the open source community speculating that PMP would affect the development of official free/open source graphics drivers from their manufacturers. Furthermore, it has been demonstrated that one can bypass the DRM check altogether by using

specialized drivers [Ionescu07].

2.1.2. Advanced Access Content System

A cryptographic system that adds copy protection to HD DVD and Blu-ray Disc (BD) has been developed by the AACS Licensing Administrator (AACS LA), which consists of an assortment of publishers including Disney, IBM, Intel, Microsoft, Panasonic, Sony, Toshiba, and Warner Bros.. The system features several nested layers of encryption and a robust revocation system, as well as a sophisticated key generation process. Figure 2 shows the AACS system in details.

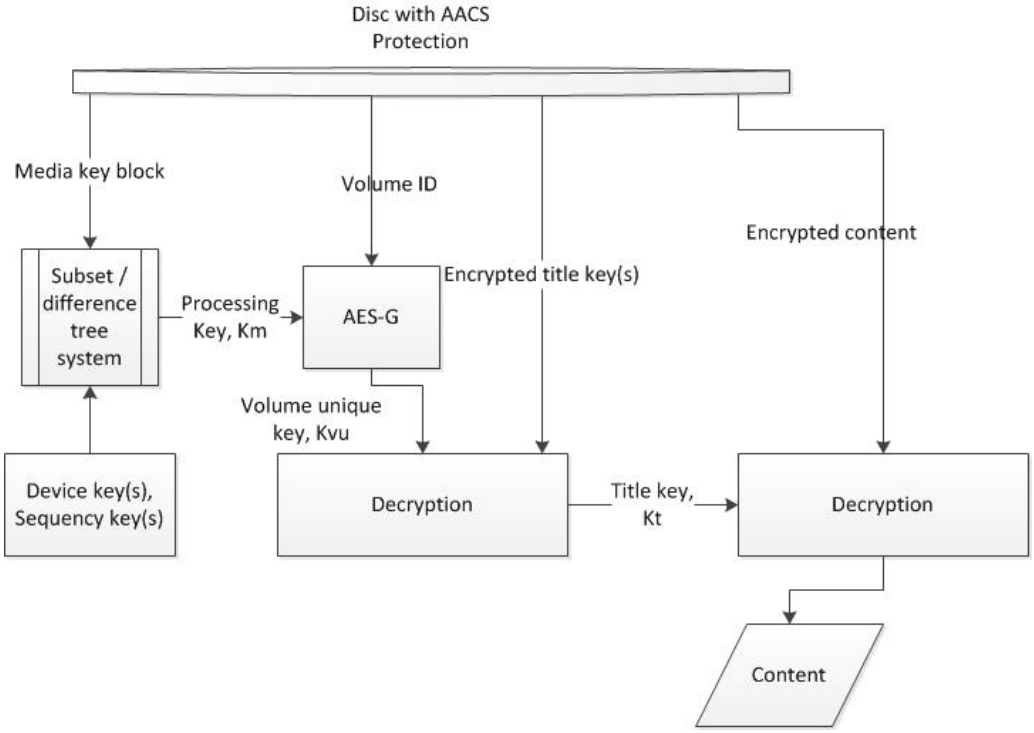

Figure 2. Advanced Access Content System (AACS)

There are three parts to the AACS scheme: copy protection, modification/decryption protection, and renewability/revocation. AACS prevents exact copying by using the Volume ID (VID) and a special key to let the drive handle this VID. To decrypt a disc, the user needs to acquire the Volume Unique Keys, which consists of the Volume ID and the processed device key. The device key is processed through the subset/difference tree system. Note that unlike CSS, where all players of a given model are controlled by the same shared decryption key, AACS provides each individual playback device with its unique set of decryption keys through a broadcast scheme. This enables licensors to revoke individual players by invalidating the decryption keys associated with the player. Therefore, if a given player's keys are compromised and published, the AACS LA can simply revoke those keys in any future content, making the keys and player useless for decrypting new titles. This is what the subset/difference tree system accomplishes. The resulting key, called the media key (Km), combined with the volume ID (VID) are then run through a one-way encryption scheme (AES-G) to yield the volume unique key (Kvu) needed to decrypt the title key(s). The decrypted title key (Kt) can then be used to decrypt the content [Doom9].

AACS allows for a system called "managed copy" where consumers can make legal copies of the discs they have purchased. The system permits three kinds of coping: an exact copy of the disc for the purpose of backup; a high-resolution copy for storage on a media server; and a low-resolution copy used on a portable player. The final AACS specification also makes it a requirement to use Cinavia detection (a proprietary audio watermarking system) on commercial Blu-ray disc players [AACS11].

2.1.3. Watermarks

Digital watermarks refers to a steganographical technique that embeds some data in the original content. Although not a DRM system by itself, digital watermarks are commonly used in film media to aid various DRM systems in recording the copyright owner, distributor and purchaser information, and subsequently in traitor tracing, a technique to track the source of leaked copyrighted material.

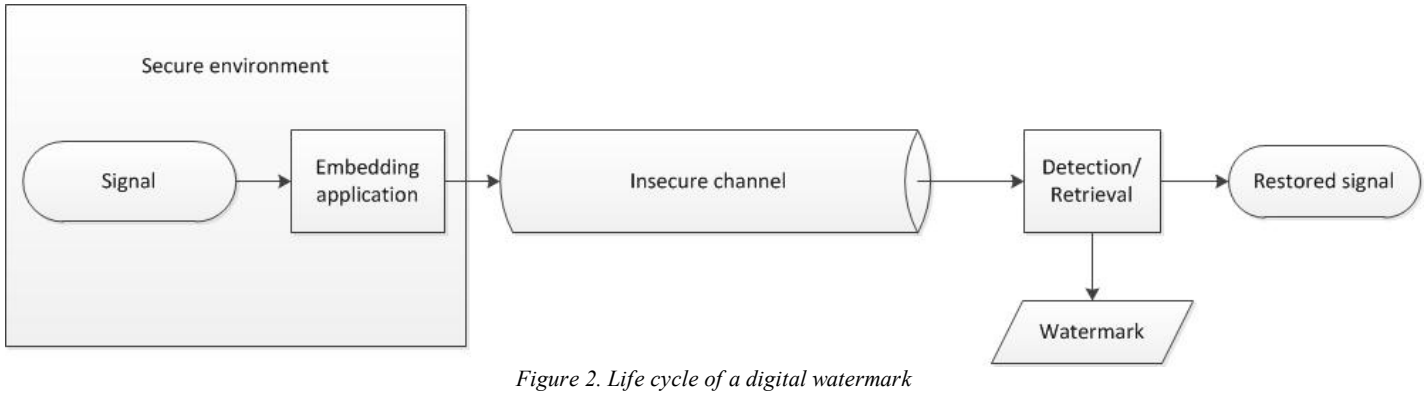

Figure 2. Life cycle of a digital watermark

Figure 3 shows the life cycle of a digital watermark. Similar to an encryption system, a watermark is first embedded into the signal in a secure environment, during the content creation phase. Note that the embedded watermark could be visible or invisible, depending on the purpose of use. The signal that contains the watermark will then go through an insecure channel (such as a distribution process), where an attack could potentially intercept and modify the signal. Such modifications can include cropping or distorting of an image or video, adding effects such as noise or dithering, lossy compression, or deletion of parts of the signal. Finally, detection (or extraction) is used to retrieve the watermark. If the signal is modified, the detection algorithm might not be able to retrieve the watermark, in which case the watermark is called "fragile." On the other hand, if a watermark can be retrieved correctly despite any modification, the watermark is called "robust" [Lee00].

Digital watermarks can be viewed as a special case of metadata where the data is carried in the signal itself instead of on the side. While normal metadata can be extracted, modified and detached from the content body, watermarks are more resilient to modifications. Nevertheless, methods exist to remove most watermarks, but such removal often causes the content signal to be degraded or distorted in some variable degree. A watermarking system can actively deny copying or modification upon detecting it, or it can work to provide detection for some other protection system [watermark]. In addition, a watermark can simply be used as a subtle labeling tool for digital content that lacks metadata attachments.

2.2. Broadcast TV

In the United States, the FCC ruled in " Digital Broadcast Television Redistribution Control" that " No party shall sell or distribute in interstate commerce a Covered Demodulator Product that does not comply with the Demodulator Compliance Requirements" [DMCA05], and that hardware must implement functionality to "actively thwart piracy." New television receivers after July 1, 2005 using the ATSC standard were supposed to incorporate the broadcast flag - a set of status bits indicating the permission status of the stream [Lening05]. After numerous struggles with the Supreme Court, the FCC finally eliminated the broadcast flag on August 22, 2011 [FCC11]. Meanwhile, the DVB Project, an international industry consortium with more than 270 members, have been developing a set of internationally accepted open standards called Digital Video Broadcasting (DVB).

2.2.1. Content Protection and Copy Management (DVB-CPCM)

Developed mainly as a DRM application for European digital television, the DVB Content Protection and Copy Management (DVB-CPCM) is a standard that specifies methods of adding information to digitally streamed content to describe permissions and usage rights on all CPCM-enabled devices.

Similar to the broadcast flag standard, content providers implement a variety of flags stored together with the content to indicate how it may be used. These flags are called the Usage State Information, and they describe how the content can be consumed, copied or exported on a CPCM-enabled device. The flags can specify limits on either the viewing time, or the number of concurrent devices streaming the content. It is important to note that CPCM only concerns with how content is handled after it is delivered - CPCM works strictly in the local environment and the Authorized Domain, which refers to the collection of all DVB-CPCM compliant devices that exist in a single household, whether purchased, rented or temporarily controlled by a family member. There is a fundamental difference between this and the majority of today's CA and DRM techniques in that the latter typically operate on a single device or type of devices [DVB].

2.3. E-books

The area of E-book DRM is a hotly debated topic. Some argue that DRM makes E-book publishing complex, while others have shown that eliminating or relaxing DRM might be good financially for the publishers due to the increase in legitimate buyers outweighing the effects of piracy [Oestreicher-Singer et al 04]. There are four main E-book formats available today, they are Mobipocket, Topaz, ePub and PDF. The challenge of implementing DRM schemes on E-book formats is complicated by the rapid changes in the hardware devices that read them, as well as the changes in businesses that publish/sell E-books. As a result, many technologies end up being obsolete not long after they are adopted.

2.3.1. Adobe Adept DRM

Adobe's Adept DRM is developed by Adobe and used in the Adobe DRM software Adobe Content Serve, and is applied to ePubs and PDFs, which can be read by many third-party e-book readers, as well as Adobe's Digital Editions software. The DRM uses a complex crypto system. Each book is encrypted using a per-book key, and this key is encrypted again using a per-user key and RSA with PKCS#1 v1.5 padding . The cipher used to encrypt the book content is AES in CBC mode with a random generated IV [Icabbages09a].

On paper, this encryption scheme ensures a strong DRM mechanism. However, it was soon observed that the software used to read ePubs and PDFs, Adobe Digital Editions, uses a very weak obfuscation to hide the per-user key. An attack that uses reverse-engineering on the software reveals a rather easy method of retrieving the per-user key from the software and use it to decrypt other Adept encrypted PDF or ePub file. Newer versions of the Adobe Digital Editions use more cryptic ways of hiding the per-user key, but attacks still exist to retrieve it from the registry [Icabbages09a].

2.3.2. Apple FairPlay

FairPlay is a DRM scheme from Apple. It was initially used for its music store to protect audio files, but was soon also adopted in ePub files designed for Apple's iBooks app on iOS devices. The system encrypts the file using AES in combination with MD5 hashes. For key management, FairPlay uses a master key for decryption, and a user key which decrypts the master key, both of which are stored together with the data in the file. Due to the local nature of the key storage and encryption processes, similar to Adobe's Adept DRM, many attacks exist to break the encryption by reverse-engineering the local applications and retrieving the user key, or exploiting the authentication process and disguising the attack as legitimate software to obtain unlocked files [Roughlydrafted07].

2.3.3 Mobipocket and Topaz

Amazon has engineered its own version of DRM in their Kindle for PC application (K4PC). The Kindle proper and Kindle for iPhone/iPod app both use a single "device" encryption key for all restricted content. K4PC uses the same (proprietary) encryption algorithms, but also uses a per-book session key for the actual en/decryption. Furthermore, the obfuscation that is used in hiding the device key is highly sophisticated [icabbage09b].

2.3.4. Microsoft Reader and Ereader

Microsoft Reader is Microsoft's own E-book application that exclusively reads e-books in the .lit format. The application contains its own DRM software. The system imposes three levels of control, each with increasing limit on how the file can be used. The first level is called sealed e-books, which have no restriction and only prevents modification to the document text itself. The second level is called inscribed e-books. These files include a digital ID tag that identifies the owner of the e-book, thereby discouraging any illegal copying and sharing of the file. The last level is called owner exclusive e-books. These files are encrypted and linked to the user's online account. The computer that downloads the file is the only device that is allowed to view the file [Booksonboard].

2.4. Computer Games

It is estimated that video game sales figures are expecting to grow from $66 billion worldwide in 2010 to $81 billion by 2016 [Takahashi11], and a large portion of those sales are happening on the PC platform. In more recent years, computer games have seen a shift in the method of distribution from retail to digital download [NPD10]. Along with it, the DRM schemes have adapted or vanished to facilitate growth in this vast market. The purpose of computer game DRM for retail units is usually to prevent whole-disc copy of the content, or limit the number of installations of a game. The latter has generated many criticisms both from players and within the industry due to some severe cases where the DRM system rendered a game unplayable to the purchaser after a period of time even on the same computer. Furthermore, many consumers find the DRM mechanisms intrusive and burdensome to their game play experience.

Many games utilize some form of "online DRM," where players are required to log in to an online service with their unique account name and password to play their games. Each game contains an activation serial number, which when registered, gets added to the player's account permanently. This method works well for games with an integral multiplayer component, or games that are distributed through broadband, such as on Steam. For games distributed on discs, many publishers use SecuRom.

2.4.1. SecuRom

SecuRom is a proprietary copyright protection scheme developed by Sony DADC. It aims to prevent whole-disc copy of software programs. Some have noted that "SecuROM... installs a shell extension that prevents Windows Explorer from deleting 16-bit executables," and is therefore a controversial DRM scheme [SecuROM09].

Some early versions of SecuROM modifies a CD-ROM's q-channel in order to make a protected original distinguishable from a copy. "A set of nine locations where the Q-Channel is purposely destroyed is computed by a specific function that calculates nine sector numbers; if the corresponding Q-channel is not readable at these locations, the CD is considered being original [SecuROM09]."

More recent versions of SecuROM started to use a technique called "data density measurement." To understand how this works, consider that the data density on normal CD/DVD ROMs are not uniform; the outer sectors have a much lower density compared to the inner sectors of the disc. SecuROM protects a disc by using a vendor specific pattern to construct this difference. It defines a set of check marks spread over the disc and uses two SCSI read commands on any given one, and measure the difference of the two to denote the time it takes for the disc to spin a full cycle. There are a total of 72 such marks, and they all have different data densities. The pattern in which the marks correspond to the densities can therefore be used to compared to the vendor specific pattern to decide if the disc is genuine or not [SecuROM09].

SecuROM v4.84 and later version introduced "Trigger Functions" that give the developer the freedom to program authenticity checks at any point in the application. This makes circumvention even more complicated since there are many different ways in which the triggers can be implemented [SecuROM09].

Many argue that the authentication checks placed in by SecuRom can sometimes lock up or slow down their games. Others criticize the intrusive nature of the shell extension. In practice, even though SecuRom prevents the exact copying of the disc, many disc emulation methods exist to circumvent it and allow pirated discs to be run using modified binaries.

2.4.2. Ubisoft Uplay

Uplay is a social network application activated either in-game or from the Uplay website, designed to work with all Ubisoft-published titles. It is known to employ a number of aggressive DRM schemes over the years, most notably the copy protection technology StarForce, for which it received enormous criticisms from the users. More recently, Ubisoft added "online DRM" to many of its big titles. This scheme forces the player to log on to the game's online service in order to play the game, regardless of whether the game has an online component. This also means that the games will simply be unplayable if the online service is down [Ubisoft]. Not surprisingly, this DRM scheme becomes a huge burden in the face of Denial-of-Service (DoS) attacks. In March 2010,

there was a severe outage to the Ubisoft DRM, and about 5% of legitimate buyers were unable to play Assassin's Creed II and Silent Hunter 5 games [Bramwell10]. Ironically, modified binaries can bypass the online check completely, resulting in the scenario where illegally obtained games can be played during a time when legally purchased ones cannot, thereby almost incentivizing piracy.

2.4.3. StarForce

StarForce is a copy protection application developed by Protection Technology. It installs a hidden IDE driver for the CD/DVD ROM drive and prevents whole disc copies on the hardware level. There exist many problems with this way of handling DRM. One is that uninstalling a game protected by StarForce does not remove the custom drivers from the system. Even though some later versions of the software provides uninstall services, many still complain that the drivers cause instability and crashes, or in some cases slowdowns of the drive or even irreversible hardware failures [Glop]. As a result of the outrage from the community, Ubisoft, among many other publishers, have abandoned StarForce and switched to SecuRom for disc copy protection [Thorsen06].

2.4.4. Steam

Originally used by Valve to distribute its own games, Steam has now become a primary game distribution and multiplayer platform on PC. The platform has seen immense growth in the past few years, mostly due to the support from big publishers and developers. As of October 2011, Steam boasts a massive 1,400 games and 35 million active user accounts [Mudgal11]. As an online distribution platform, Steam registers games sold to its users to their user accounts. For games purchased through the Steam store, Steam automatically adds them to the game library of the user; for offline games, Steam offers a way for user to authenticate their games the first time they play them. After the initial authentication, games can be played in offline mode without users connecting to their Steam accounts.

In 2009, Steam made any extra DRM mechanism obsolete by providing "Custom Executable Generation" for executable files that are unique for each user, but gives the user the option to install the software on multiple PCs via Steam or using software backups without any limitation [Cavalli09].

2.5. Music

The music industry has seen immense shift in user adoption from audio CDs to internet music. One of the earlier and worst examples of audio CD DRM is Sony BMG's Extended Copy Protection (XCP) and MediaMax CD-3 software. Not only was the protection not effective (the audio tracks can still be recorded and ripped), the protection installs a rootkit (a software that gains total control of the computer) to the system without informing the user [Borland05]. Furthermore, there's no easy way to uninstall the software, and trying to do so could render the CD drive inoperable [Borland05]. This sparked massive public outrage, and spawned a class action lawsuit against Sony BMG and a subsequent settlement [EFF].

Today, many online music stores sell audio files that have some DRM that restricts the usage and copy of the files. However, due to the analog nature of audio, many DRM schemes can be easily bypassed on the hardware level. As a result, many stores simply offer DRM-free music.

2.5.1. Sony OpenMG

Sony created a proprietary DRM system in its OpenMG Jukebox software. It achieves copy protection by using its own file format that supports encryption. The corresponding music organization application, OpenMG Jukebox, uses a system of checking files in and out of the local library to ensure that only legal and limited numbers of copies exist [Youn]. The OpenMG file format is only playable on certain devices and Windows Media Player, and there are many inconveniences regarding deletion of files that are protected by it [Youn].

2.5.2. Apple FairPlay (iTunes)

FairPlay is a DRM scheme from Apple specifically to enable DRM content on iTunes. The system encrypts the file using AES in combination with MD5 hashes. For key management, FairPlay uses a master key for decryption, and a user key which decrypts the master key, both of which are stored together with the data in the file. Due to the local nature of the key storage and encryption processes, similar to Adobe's Adept DRM, many attacks exist to break the encryption by reverse-engineering the local applications and retrieving the user key, or exploiting the authentication process and disguising the attack as legitimate software to obtain unlocked files [Roughlydrafted07]. In 2009, Apple announced that all iTunes music will be available without any DRM [Apple09].

3. Vulnerabilities

Present DRM systems suffer from many vulnerabilities and weaknesses. As technologies become more transparent to the public, attackers can exploit these weaknesses and circumvent DRM mechanisms. The most obvious attack on a DRM system is by completely bypassing it.

3.1. Bypass of DRM Technologies

The most simple and intuitive bypass of a digital DRM technology is by converting it to analog. This is known as the "analog hole" - the vulnerability that all media formats must be experienced in analog form by the user, and thereby must be susceptible to unauthorized use and copy in the analog form. It is clear that the analog hole is a hard problem to tackle, since any protection scheme that interferes with the analog signal is essentially interfering with the user experience of the content, and is usually frowned upon.

An example of the above dates back to the time when Macrovision tried to use a distorted signal to trick the automatic gain control on the VCR. However, due to the design of TVs at the time, many users were forced to connect their DVD players through their VCR, which caused the Macrovision DRM scheme to interfere with the DVD output. Many users were falsely convinced that the problem existed in their DVD players instead. Furthermore, many TVs did not support the Macrovision technology, and ended up producing poor quality signals [Roberts99].

In the field of high definition video, Intel has developed a copy protection scheme aimed to" plug" the analog hole, known as High-bandwidth Digital Content Protection (HDCP). Each HDCP receiver device is checked before a video stream is started to see if the device is authorized to accept the stream.

Each HDCP transmitter keeps a record of 40 56-bit secret keys and a 40-bit long record called Key Selection Vector (KSV). Then the transmitter and receiver exchange their KSVs. Using a special algorithm (Blom's scheme), the two devices each calculates a number based on the KSV sent from the other device, and then exchange the resulting numbers to generate a stream cipher that ends up being used to exclusive-or the content data, producing the encrypted data. Note that the protocol repeated the process and reproduces a secret key after the transmission of every frame. A special revocation list is kept to ensure that devices can be revoked upon keys being compromised [HDCP09].

There are several problems with HDCP. First, connecting an HDCP device to multiple displays could prove difficult, since the transmission protocol is restricted to a pair of devices sharing a secret. Secondly, additional control latency could be added due to the encoding/decoding processes, causing very undesirable effects in certain interactive media or video capturing. Furthermore, in September 2010, an HDCP master key that allows the generation of valid device keys (which then makes the key revocation feature of HDCP obsolete) was released to the general public. [kravets10] Intel has confirmed that the crack is genuine, and believes the attacker reverse-engineered the master key, indicating the weakness in the encryption scheme itself.

3.2. DRM and cryptography

Most high definition media formats demand great system resources to be devoted to the use of processing media data. Throwing in the overhead of a crypto system will adversely affect the quality of the media itself. As a result, symmetric ciphers that places heavy burden on the processing resources of a device is generally considered only relevant for media formats such as e-book or documents. For multimedia, public key systems are usually employed, while using strong encryption algorithms. For instance, Microsoft has been known to use the advanced elliptic curve cryptography in its DRM schemes. [MSDRM01]

However, the fundamental difference between a crypto system and a DRM system is that a DRM system must restrict access on a per use basis. A DRM system that employs a crypto system suffers from the flaws of a weak crypto system; the key distribution is, at its core, an impossible task. In the case of E-books and music files, cryptography has all but accomplished the goals of DRM. Attackers have been able to reverse-engineer software designed to legitimately decrypt protected files, and thereby obtain the key stored locally on the user's computer. The strength of the encryption instead then lies in the strength of the obfuscation of the locally stored key. As Figure 4 shows, the strength of the local DRM system is only as strong as the method in which the authorized application hides its key.

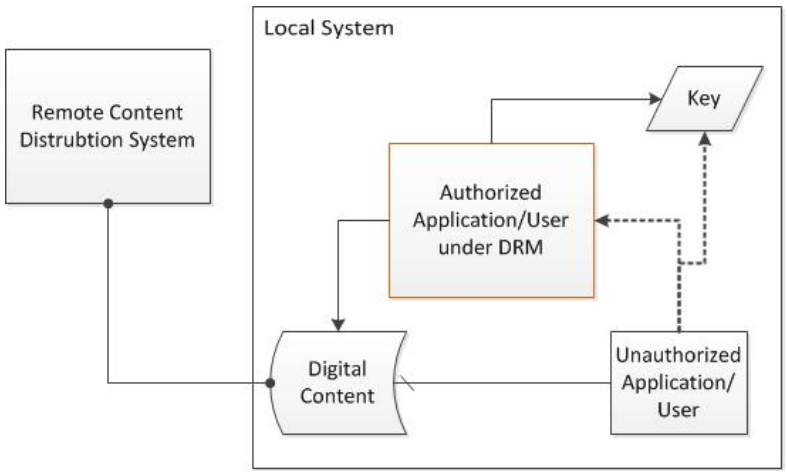

Figure 4. Local DRM security bypass

As discussed before, many systems already attempt to strengthen the key management aspect of DRM. Amazon's more recent DRM schemes extensively employ session-key mechanism, while other more recent standards like AACS have specifically designed systems to revoke keys on devices known to have made unauthorized use of content. Similar to all existing security problems, designing DRM systems that revolve around cryptography will remain a "white hat vs black hat" game.

3.3. Incompatibility

Perhaps an even greater concern for DRM in general is the nature of technology. As media standards and formats change and evolve over time, old media with DRM-restrictions become hard to migrate to the new systems. Many authentication services may also become unavailable, and the DRM scheme becomes obsolete.

There are many examples of obsolescence in the E-book and online music industries. In August 2006, Amazon stopped sales of PDF and LIT e-books with DRM restrictions, and informed their customers that they will lose the ability to access their files 30 days after that from online services as well as on new devices [Mobileread]

Introduced in 2006, the Zune player initially did not support content that used Microsoft's own PlaysForSure DRM scheme their own products used [Derek06]. And in another striking example, in April 2008, Microsoft sent out an email to former customers of the retired MSN Music store: "As of August 31, 2008, we will no longer be able to support the retrieval of license keys for the songs you purchased from MSN Music or the authorization of additional computers. You will need to obtain a license key for each of your songs downloaded from MSN Music on any new computer, and you must do so before August 31, 2008. If you attempt to transfer your songs to additional computers after August 31, 2008, those songs will not successfully play." [Paul08]

To some degree, these side effects of DRM are unavoidable; they are part of the effects of technological advancement. However, many argue that DRM systems place unnecessary burden on publishers and their customers in these scenarios.

4. Conclusion

DRM systems have been developed as early as in the 1980s. Throughout the decades, the publishing industry has seen immense changes to the technologies that power our digital world. As methods of distribution changes, the responsibilities and scopes of a DRM system changes as well. Moreover, as we crave for more media consumption in this new age, the need for robust and effective DRM systems seems all the more urgent.

In this paper, we looked at many of the existing technologies, and realize that they only provide partial solutions to an immense problem. As our media formats continue to evolve, we can only expect greater challenges in designing future DRM systems. These challenges include buildings better crypto systems that incorporate advanced key management, as well as more secured client applications.

References

[Boucqueau07] Jean-Marc Boucqueau, "Digital Rights Management", 3rd IEEE International Workshop on Digital Rights Management Impact on Consumer Communications, January 11 2007

[Grimmett01] Jeanne J. Grimmett, "Encryption Export Controls, Congressional Research Service report," RL30273, 2001

[Doom9] "Understanding AACS (including Subset-Difference)", http://forum.doom9.org/showthread.php?t=122363

[DVB] "DVB Content Protection and Copy Management", http://www.dvb.org/technology/dvb-cpcm/

[Oestreicher-Singer et al 04] Oestreicher-Singer, Gal and Arun Sundararajan, "Are Digital Rights Valuable? Theory and Evidence from the eBook Industry", Proceedings of the International Conference on Information Systems, 2004

[Icabbages09a] "Circumventing Adobe ADEPT DRM for EPUB", 2009, http://i-u2665-cabbages.blogspot.com/2009/02/circumventing-adobe-adept-drm-for-epub.html

[Icabbages09b] "Circumventing Kindle For PC DRM (updated)", 2009, http://i-u2665-cabbages.blogspot.com/2009/12/circumventing-kindle-for-pc-drm.html

[Booksonboard] "BooksOnBoard Mobile Device Selection Guide", http://www.booksonboard.com/index.php?F=Device_Selection_Chart

[SecuROM09] "CD Protection - SecuROM," 2009, http://www.encrypt.ro/cd-encryption/cd-protection-securom.html

[Ubisoft] "Online Services Platform Q and A," http://support.uk.ubi.com/online-services-platform/

[Bramwell10] Tom Bramwell, "Ubisoft DRM was 'attacked' at weekend," 2010, http://www.eurogamer.net/articles/ubisoft-drm-was-attacked-at-weekend

[Mudgal11] Kartik Mudgal, "35 Million Active Gamers on Steam; Valve hints at an Improved Source Engine," 2011, http://gamingbolt.com/35-million-active-gamers-on-steam-valve-hints-at-an-improved-source-engine

[Cavalli09] Earnest Cavalli, "Steam Update 'Makes DRM Obsolete'," 2009, http://www.wired.com/gamelife/2009/03/steam-update-ma/

[Kravets10] David Kravets, "Intel Threatens to Sue Anyone Who Uses HDCP Crack," 2010, http://www.wired.com/threatlevel/2010/09/intel-threatens-consumers/

[Mobileread] "Amazon Drops Lit/Pdf eBooks", http://www.mobileread.com/forums/showthread.php?threadid=7223

[Derek06] Derek, "Microsoft's Zune Won't Play Protected Windows Media," Electronic Frontier Foundation, 2006

[Paul08] Thurrott Paul, "MSN Music Store Support Notification," Winsupersite, 2008

[Apple09] "Changes Coming to the iTunes Store," 2009, http://www.apple.com/pr/library/2009/01/06Changes-Coming-to-the-iTunes-Store.html

[MSDRM01] " Microsoft's Digital Rights Management Scheme - Technical Details," 2001, http://cryptome.org/ms-drm.htm

[AACS11] Advanced Access Content System (AACS): Introduction and Common Cryptographic Elements Book, 2011, http://www.aacsla.com/specifications/AACS_Spec_Common_Final_0952.pdf

[Watermark] How to protect digital works: images, photos and documents, comparison of watermarking methods and tools, http://www.watermarker.com/how-to-protect-digital-images.aspx

[Lening05] Carey Lening, Copyright Protection of Digital Television: The "Broadcast Flag," 2005, http://fpc.state.gov/documents/organization/45183.pdf

[Takahashi11] Dean Takahashi, "With online sales growing, video game market to hit $81B by 2016 (exclusive)", 2011, http://venturebeat.com/2011/09/07/with-online-sales-growing-video-game-market-to-hit-81b-by-2016-exclusive/

[Schneier99] Bruce Schneier, "DVD Encryption Broken," 1999,
http://www.schneier.com/essay-193.html

[Ionescu07] Alex Ionescu, " Update on Driver Signing Bypass," 2007,
http://www.alex-ionescu.com/?p=24

[Lee00] Insup Lee, "EMTM 553: E-commerce Systems, Lecture 7a: Digital Watermarking," 2000,
http://www.cis.upenn.edu/~lee/00emtm553/watermark.ppt

[DMCA05] Gerard M Stegmaier; Pike and Fischer, Inc.; United States. "The Digital Millennium Copyright Act. 2005 Supplement," 2005,
http://books.google.com/books?id=nL0s81x-gVwC&lpg=PA993&ots=w8llG9MHt8&dq=DMCA%202005%20supplement&pg=PP2#v=onepage&q=DMCA%202005%20supplement&f=false

[FCC11] FCC, "Genachowski Announces Elimination of 83 Outdated Media Rules," 2011,
http://www.fcc.gov/document/genachowski-announces-elimination-83-outdated-media-rules

[Roughlydrafted07] "How FairPlay Works: Apple's iTunes DRM Dilemma," 2007,
http://www.roughlydrafted.com/RD/RDM.Tech.Q1.07/2A351C60-A4E5-4764-A083-FF8610E66A46.html

[NPD10] NPD, "PC FULL-GAME DIGITAL DOWNLOADS SURPASS RETAIL UNIT SALES," 2010,
https://www.npd.com/press/releases/press_100920.html

[Glop] "Boycott Starforce",
http://www.glop.org/starforce/

[Thorsen06] Tor Thorsen, "Ubisoft officially dumps Starforce," 2006,
http://www.gamespot.com/news/ubisoft-officially-dumps-starforce-6147655

[Halderman05] J. Alex Halderman, "Sony Shipping Spyware from SunnComm, Too," 2005,
https://freedom-to-tinker.com/blog/jhalderm/sony-shipping-spyware-sunncomm-too

[Borland05] John Borland, "FAQ: Sony's 'rootkit' CDs," 2005,
http://news.cnet.com/FAQ-Sonys-rootkit-CDs---page-2/2100-1029_3-5946760-2.html

[EFF] Electronic Frontier Foundation, "Sony BMG Litigation Info,"
https://www.eff.org/cases/sony-bmg-litigation-info

[Youn] Brian Youn, "Sony MZ-N1 NetMD Walkman,"
http://www.minidisc.org/brian_youn/mzn1/page3.html

[Roberts99] Eric Roberts, "Macrovision Demystified," 1999,
http://www-cs-faculty.stanford.edu/~eroberts/cs181/projects/1999-00/dmca-2k/macrovision.html

[HDCP09] "High Bandwidth Digital Content System, Revision 1.4," 2009,
http://www.digital-cp.com/files/static_page_files/5C3DC13B-9F6B-D82E-D77D8ACA08A448BF/HDCP%20Specification%20Rev1_4.pdf

List of Acronyms

AACS	Advanced Access Content System
AACS LA	AACS Licensing Administrator
COPP	Certified Output Protection Protocol
CSS	Content Scrambling System
DRM	Digital Rights Management
DVB	Digital Video Broadcasting
DVB-CPCM	DVB - Content Protection and Copy Management
HDCP	High-bandwidth Digital Content Protection
K4PC	Kindle for PC
OPM	Output Protection Management
PMP	Protected Media Path
PUMA	Protected User Mode Audio
PVP	Protected Video Path
AES	Advanced Encryption Standard
MD5	Message Digest Algorithm 5
BD	Blu-ray Disc
FCC	Federal Communications Commission
MSN	Microsoft Network

Last modified: November 28, 2011
This and other papers on latest advances in network security are available on line at http://www1.cse.wustl.edu/~jain/cse571-11/index.html

Back to Raj Jain's Home Page