

# Digital Rights Management: Evaluation of existing systems

Thesis project done at Information Theory,  
Linköping University  
by

Anders Burström  
Jonas Callander

LITH-ISY-EX-ET-0270-2003

Linköping, 2003

# Digital Rights Management: Evaluation of existing systems

Thesis project done at Information Theory,  
Linköping University  
by

Anders Burström  
Jonas Callander

LiTH-ISY-EX-ET-0270-2003

Linköping, 2003

Examiner: Viiveke Fåk  
Supervisor: Kristin Anderson  
Linköping, October 9, 2003

 <b>LINKÖPINGS UNIVERSITET</b>	<b>Avdelning, Institution</b> Division, Department  Institutionen för Systemteknik 581 83 LINKÖPING	<b>Datum</b> Date 2003-10-09
---	---	------------------------------------

<b>Språk</b> Language Svenska/Swedish X Engelska/English	<b>Rapporttyp</b> Report category Licentiatavhandling X Examensarbete C-uppsats D-uppsats  Övrig rapport _____	<b>ISBN</b>
		<b>ISRN</b> LITH-ISY-EX-ET-0270-2003
		<b>Serietitel och serienummer</b> Title of series, numbering <b>ISSN</b> _____
<b>URL för elektronisk version</b> <a href="http://www.ep.liu.se/exjobb/isy/2003/270/">http://www.ep.liu.se/exjobb/isy/2003/270/</a>		

<b>Titel</b> Title  <b>Författare</b> Author	Digital Rights Management, Utvärdering av existerande system  Digital Rights Management, Evaluation of existing systems.  Anders Burström Jonas Callander
--	---

<b>Sammanfattning</b> Abstract <p>The aim of this report is to examine if existing Digital Rights Management systems are useful and satisfying to the consumer, copyright owner and distributor. If not, is it possible to design a useful and satisfying Digital Rights Management system?</p> <p>During the past few years, copyright owners of music, movies and other media have seen how piracy has increased with the introduction of affordable broadband technology. Record and movie corporations have pushed for a solution to piracy and one of them is Digital Rights Management. They want their customers to pay for and then enjoy the digital media but at the same time protect the rights of the copyright owner. That is what Digital Rights Management is all about; protect the copyright owner while allowing the consumer to enjoy their digital media. Digital Rights Management can restrict the users rights to copy and transfer the contents to other devices as well as restrict the number of times a user is allowed to use the media.</p> <p>The present DRM systems are focusing on preventing digital media from being freely distributed by limiting the ability to copy or move the media. This puts limitations on fair use such as making personal copies of music. Copyright owners and distributors want more consumers to discover DRM, but so far, the consumers have shown little interest.</p> <p>This report is based on various resources on the Internet such as white papers on Digital Rights Management, our own experimentation and on Microsoft Media Rights Management SDK documentation.</p> <p>We do not believe it is possible to design a DRM system that consumers, copyright owners and distributors are satisfied with. It is not possible to combine the demands of copyright owners and the consumers' claims of fair use.</p>
--

**Nyckelord**

Keyword

Digital Rights Management, DRM, Upphovsrätt, Copyright

# Digital Rights Management

## Evaluation of existing systems

Anders Burström

Jonas Callander

### **Abstract**

The aim of this report is to examine if existing Digital Rights Management systems are useful and satisfying to the consumer, copyright owner and distributor. If not, is it possible to design a useful and satisfying Digital Rights Management system?

During the past few years, copyright owners of music, movies and other media have seen how piracy has increased with the introduction of affordable broadband technology. Record and movie corporations have pushed for a solution to piracy and one of them is Digital Rights Management. They want their customers to pay for and then enjoy the digital media but at the same time protect the rights of the copyright owner. That is what Digital Rights Management is all about; protect the copyright owner while allowing the consumer to enjoy their digital media. Digital Rights Management can restrict the users rights to copy and transfer the contents to other devices as well as restrict the number of times a user is allowed to use the media.

The present DRM systems are focusing on preventing digital media from being freely distributed by limiting the ability to copy or move the media. This puts limitations on fair use such as making personal copies of music. Copyright owners and distributors want more consumers to discover DRM, but so far, the consumers have shown little interest.

This report is based on various resources on the Internet such as white papers on Digital Rights Management, our own experimentation and on Microsoft Media Rights Management SDK documentation.

We do not believe it is possible to design a DRM system that consumers, copyright owners and distributors are satisfied with. It is not possible to combine the demands of copyright owners and the consumers' claims of fair use.

# Digital Rights Management

## Evaluation of existing systems

Anders Burström

Jonas Callander

<b>1. INTRODUCTION .....</b>	<b>3</b>
<b>2. COPYRIGHT AND DIGITAL FORMATS.....</b>	<b>5</b>
2.1. WHAT IS COPYRIGHT?.....	5
2.2. COPYRIGHT IN THE US AND FAIR USE .....	5
2.3. DIGITAL COPYRIGHT AND THE EUROPEAN COMMUNITY .....	6
<b>3. DIGITAL MEDIA .....</b>	<b>8</b>
3.1. PIRACY .....	8
3.1.1. <i>The origins of digital piracy</i> .....	8
3.2. THE INTERNET .....	9
3.2.1. <i>Entrée: Shawn Fanning</i> .....	9
3.2.2. <i>Napster's offspring</i> .....	10
3.3. PIRACY PREVENTION .....	10
3.3.1. <i>Copy protection, the early days</i> .....	10
3.3.2. <i>The CD-ROM</i> .....	11
3.3.3. <i>DVD</i> .....	11
3.4. REGIONAL CODES .....	12
3.4.1. <i>DeCSS</i> .....	13
<b>4. CRYPTOGRAPHY .....</b>	<b>14</b>
4.1. ALGORITHMS .....	15
4.2. DIGITAL RIGHTS MANAGEMENT AND CRYPTOGRAPHY .....	16
4.3. IDENTIFICATION AND SIGNATURES .....	17
4.3.1. <i>Identification protocols</i> .....	17
4.3.2. <i>Digital signatures</i> .....	17
4.3.3. <i>Certificate Authorities</i> .....	18
<b>5. MICROSOFT DIGITAL RIGHTS MANAGEMENT .....</b>	<b>19</b>
5.1. PURPOSE OF MICROSOFT WINDOWS MEDIA DIGITAL RIGHTS MANAGEMENT .....	19
5.2. OVERVIEW .....	19
5.3. SECURITY OVERVIEW .....	20
5.3.1. <i>Keys and encryption</i> .....	20
5.3.2. <i>Security on the user's computer</i> .....	21
5.3.3. <i>Secure Audio Path</i> .....	21
5.4. SYSTEM UPGRADES.....	23
5.5. TESTING MICROSOFT WINDOWS MEDIA DIGITAL RIGHTS MANAGEMENT .....	24
5.6. CRACKING WINDOWS MEDIA AUDIO .....	24
5.6.1. <i>"UnFuck.exe"</i> .....	24
5.6.2. <i>"FreeMe.exe"</i> .....	26
5.7. XBOX.....	26
5.7.1. <i>Xbox security</i> .....	27
<b>6. PRIVACY AND DRM.....</b>	<b>28</b>
6.1. WHO CAN WE TRUST? .....	28
6.2. POSSIBLE SOLUTIONS .....	28
6.3. CONSUMER PRIVACY .....	28
6.3.1. <i>Privacy according to Microsoft</i> .....	29
<b>7. THE STATE OF DRM TODAY .....</b>	<b>31</b>
<b>8. CONCLUSION .....</b>	<b>33</b>
<b>9. REFERENCES .....</b>	<b>34</b>
9.1. BOOKS AND DOCUMENTS .....	34
9.2. INTERNET RESOURCES .....	34

## 1. Introduction

Digital Rights Management (DRM) is a way to distribute digital media to authorized users and to prevent unauthorized usage of the digital media. A DRM system has three main actors; the copyright owner, the distributor and the consumer. All of these have different interests that must be fulfilled in order for the system to be useful.

This essay will try to answer the following questions:

Are the existing DRM systems useful and satisfying to the consumer, copyright owner and distributor? If not, is it possible to design a useful and satisfying DRM system?

The DRM subject spans over a vast area including:

- Copyright laws
- Cryptography
- Consumer privacy
- Copy protection
- Digital media
- Piracy

A DRM system should offer the following to a consumer in order to be attractive:

### **Reliability**

- The service must be reliable; otherwise, it will not be attractive.

### **Value**

- The service must be priced right and/or offer other benefits to the consumer.

### **Privacy**

- The service must give the consumer the privacy he/she demands.

### **Availability**

- The service must be available whenever the consumer wants. It must also carry the same variety of products as any other mean of distribution. The service must also be available on different platforms.

### **Common format**

- The service must use a format shared by other services to be widely accepted.

### **Fair use**

- The system must offer some form of fair use to be attractive.

# Digital Rights Management

Evaluation of existing systems

Anders Burström

Jonas Callander

A DRM system must offer the following to a copyright owner to be of use:

## **Piracy prevention**

- The content owner wants to disable copying beyond “fair use”.

## **Security**

- The DRM system must use a high level of security. The DRM system must use a high level of security to make it difficult to circumvent the protection.

## **Payment**

- The DRM system must give the copyright owner the option to get paid for the copyrighted material.

A DRM system must offer the following to a distributor to be of use:

## **Payment**

- The service must generate money.

## **Satisfaction**

- Both copyright owners and consumers must be satisfied with the system the distributor provides.

In this essay we will try to find out if these demands are met in the present DRM systems.



## **2. Copyright and digital formats**

In this section, we have chosen to briefly study the laws surrounding copyright and their effect on digital media. Since most copyright laws agree to the World Intellectual Property Organization (WIPO) Copyright Treaty, we can assume that most of what we are about to discuss applies all over the world with some exceptions.

### **2.1. What is copyright?**

Copyright is a form of protection provided by laws to the authors of literary, dramatic, musical, artistic, and certain other intellectual works [27]. This protection is available to both published and unpublished works. Copyright protection subsists from the time the work is created in fixed form and immediately becomes the property of the author who created the work. The law enables copyright owners to control use of their material in a number of ways, such as making copies, issuing copies to the public, performing in public, broadcasting and use on-line. The purpose of copyright is to allow creators to gain economic rewards for their efforts, thereby encouraging future creativity and the development of new material. Most uses of copyright material therefore require permission from the copyright owner.

### **2.2. Copyright in the US and fair use**

There are exceptions to copyright, so that some minor uses may not violate copyright. In the U.S., this is called “Fair use” and since it is a vital part of the complexity surrounding DRM, we will explain what it is and why it must be taken into consideration.

Fair use is a limitation on the exclusive rights of copyright holders. It allows consumers to make a copy of part or all of a copyrighted work, even where the copyright holder has not given permission or objects to the use of the work. Fair use is decided by a judge, on a case-by-case basis, after balancing the four factors listed in section 107 of the Copyright statute [13]. The factors to be considered include:

1. The purpose and character of the use, including whether such use is of a commercial nature or is for non-profit educational purposes;
2. The nature of the copyrighted work;
3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
4. The effect of the use upon the potential market for or value of the copyrighted work.

Courts have found that using copyrighted work for socially beneficial uses should be considered fair use. The following purposes have been accepted as fair use by U.S. courts: criticism, comment, news reporting, teaching, scholarship, research and parodies. In addition to these rulings, the Supreme Court held that time-shifting (for example, private home taping of a television program with a VCR for later viewing) is fair use [14].

Although there is no court ruling, many lawyers consider the following uses also to be fair uses:

Space-shifting or format-shifting - that is, taking content you own in one format and putting it into another format, for personal, non-commercial use. For instance, "ripping" an audio CD (that is, making an MP3-format version of an audio CD that you already own) is considered fair use by many lawyers.

Making a personal back-up copy of content you own - for instance, burning a copy of an audio CD you own.

If space-shifting and format-shifting are considered fair use, DRM will be hard to implement. How will a DRM system know if you make an mp3-file for your own mp3-player or if you make it for distribution on a peer-to-peer file-sharing program? Some people claim there is no way of telling whether a copy is being made for fair use or for piracy, since the methods are the same. The only thing separating the two is human intent, which no technological device will be able to foresee [17]. A simple solution to the problem would be to prevent copying altogether and ignore the space- and format-shifting aspects of fair use. There is no doubt that this type of action will upset some of the consumers.

### **2.3. Digital copyright and the European Community**

In the European Community, the laws are similar to those in the United States, but since the European Community consists of several independent member states, the laws may vary from one country to another. In recent years, there have been several proposals to make a common copyright law. The so-called InfoSoc directive was accepted in 2001 and the member states are currently making adjustments to their copyright laws to comply with this directive. One thing that differs from the fair use rights in the U.S., is that it is up to every member state of the EC to choose whether fair use, such as making copies for personal use, is legal or not. Article 5.2 in the InfoSoc directive states that the member countries of the EC may provide exceptions or limitations to the copyright. The list of exceptions is comprehensive. An excerpt from Article 5, paragraph 2b of the InfoSoc directive reads as follows [15]:

# Digital Rights Management

## Evaluation of existing systems

Anders Burström

Jonas Callander

2. Member States may provide for exceptions or limitations to the reproduction right provided for in Article 2 in the following cases:

(b) in respect of reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the rightholders receive fair compensation which takes account of the application or non-application of technological measures referred to in Article 6 to the work or subject-matter concerned;

Quote: InfoSoc directive, article 5, paragraph 2b

The InfoSoc directive makes it possible for a member state to accept or ignore fair use.

From Article 6 of this directive we learn the following:

Obligations as to technological measures

1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.

Quote: InfoSoc directive, article 6, paragraph 1

This means that breaking a copy protection system is illegal in all EC states. Let us for a moment consider the Swedish copyright law<sup>1</sup>. This law state, in paragraph 12, that it is legal to make copies of music CD's for personal use [21]. This could, however, be illegal if the CD itself is equipped with copy protection. With the InfoSoc directive we wind up in something that looks like Catch 22, since making copies for personal use is legal, as long as you do not circumvent the copy protection, which you have to do in order to make the copy. In short, the copyright owners can now fully decide if making personal copies will be allowed throughout the entire EC, regardless of the copyright laws in the individual countries. There is, however, a paragraph in Article 6 that can change this:

4. Notwithstanding the legal protection provided for in paragraph 1, in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned.

Quote: InfoSoc directive, article 6, paragraph 4

We are not in any way educated to deal with this type of juridical formalism, but from what we understand, this paragraph bounces the problem back to the member states. It is up to the member countries governments to uphold the rights of fair use if they want to. This could mean that a member country, such as Sweden, can demand that circumventing copy protection on CD's can be legal.

---

<sup>1</sup> Upphovsrättslagen 1960:729, URL

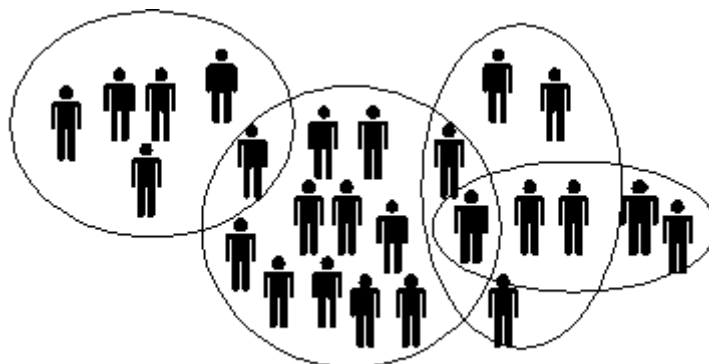
### 3. Digital media

#### 3.1. Piracy

The unauthorized use or reproduction of copyrighted or patented material is called piracy. As long as there has been copyrights and patents, there have been people violating the laws prohibiting copying. The problem itself is as old as the laws. When it comes to copyright violation of music and films, there used to be a somewhat natural solution. The degradation was huge for each copy made. An analogue copy will always be of lower quality than the original. A digital copy is a perfect copy and impossible to differentiate from the original. The possibility of making perfect copies is considered to be a large threat to the copyright holders.

##### 3.1.1. The origins of digital piracy

Prior to the Internet copying occurred around groups of friends and acquaintances. The objects copied were music on cassettes and computer programs. The means of distribution was the postal service or in-person contacts. Copy protection was weak at its best. These networks of people are called “sneaker-networks” or “interconnected small-worlds networks”, and the connection between the networks consisted of members who were part of two or more networks. For example, most people have a social group of a few score of people. Each of these people has a group of friends that partly overlap with their friends’ friends, and also introduces more people. It is estimated that, on average, each person is connected to every other person in the world by a chain of about six people from which arises the term “six degrees of separation” [1].



A sneaker network [1]

In 1987 the Fraunhofer Institute in Erlangen, Germany began working on a high quality, low bit-rate audio coding. Without data reduction, digital audio signals typically consist of 16 bit samples recorded at a sampling rate more than twice the

actual audio bandwidth<sup>2</sup>. This results in a quantity of more than 1400 Mbit to represent one second of stereo music in CD quality [16]. By using the Fraunhofer audio coding, the original sound data from a CD shrunk by a factor of 12, without losing sound quality. In 1992 the algorithm was submitted to the International Standards Organization (ISO) and integrated into the MPEG-1 specification. It eventually became known as the ISO-MPEG Audio Layer-3 standard, MP3 [19].

### 3.2. The Internet

In the late 1990's the Internet had become mainstream. The MP3-format and the evolution of high capacity, low priced hard drives had allowed anyone to store large amounts of music on their computers. Programs that allowed music to be converted directly from a CD to MP3-files (CD-ripping) became easy to use even with little or no experience. The Internet became the natural successor of the "sneaker-net", at least for music distribution. Prior to 1999 the music was stored on centralized servers, FTP or HTTP, on universities, companies and Internet Service Providers. Copyright-holders or their representatives sent "cease and desist" letters to these web-site operators and web-owners citing copyright infringement and in a few cases followed up with legal action. The threats of legal action were successful attacks on those centralized networks, and MP3 web and FTP sites disappeared from the mainstream shortly after they appeared.

#### 3.2.1. Entrée: Shawn Fanning

In 1998 an 18-year old name Shawn Fanning enrolls at Northeastern University in Boston, USA. He will drop out the year after. The main reason is that he wants to spend more time developing a software he has created in order to exchange files over the Internet. He calls the software Napster. Napster is a P2P (peer-to-peer) program with a centralized database and a searchable index enabling users to do searches on file names. Since the files are not stored on a centralized server, but stored on the user's computers, the copyright owners can do nothing but watch in the beginning. Napster's popularity explodes. At the peak of its popularity it claims to have over 60 million users. In the end it is the centralized database that becomes the target for a series of lawsuits. The RIAA (Recording Industry Association of America) charges that Napster broke the law by allowing the illegal exchange of files over its network with the understanding that the majority of the songs traded are copyrighted. On 2 July 2001 Napster is shut down and a year later it files for bankruptcy.

---

<sup>2</sup> e.g. 44.1 kHz for a CD

### 3.2.2. Napster's offspring

Somewhere around Napster's final days new P2P-programs began to pop up. They shared many of Napster's features, but lacked the centralized database, which had been the target of the lawsuits against Napster. They also made it possible to share other content than music such as software and movies. The copyright owners still has not found an effective way to shut down these file sharing services. The future will tell if the large P2P-programs for file sharing will prevail, piracy however, will probably exist regardless of the measures taken to prevent it. Today anyone with a high speed Internet connection can download almost any movie or album.

### 3.3. Piracy prevention

#### 3.3.1. Copy protection, the early days

In the seventies most software was stored on tapes that lacked any form of copy protection. For this reason they were easy to duplicate unless other factors, such as tape quality and/or recorder settings, generated problems. In 1976 the 5.25-inch floppy disk was introduced and quickly gained popularity as a result of the reduced loading time compared to the tapes [9]. The first floppy disks were even easier to copy than the tapes. User clubs formed where one copy was bought legally and copied illegally to the members of the club. Even companies and schools used this system to make copies for their computers. The software industry began equipping their programs with copy protection. A floppy disk has a list of what data is contained on it, where it is stored and what type of data it is. This part of the disk is called a catalog or directory. On the copy protected disks the catalog was moved or altered in format. This type of protection kept a large portion of the pirates away and most of the large-scaled piracy was stopped.

At this point some pirates began forming groups to break copy protection, an activity often referred to as "cracking". The software producers tried many different variants of copy protection. Some of the methods used involved using hidden files, drilling a small hole in the floppy media to simulate a bad sector or to deliberately mark a couple of sectors as bad [10]. When the program was run, it restored the directory to its correct place or searched for the bad sector on the disk to verify that it was the original disk. There were also attempts, mostly by CAD-software producers, to implement a device (often referred to as a "dongle") that had to be attached to one of the computers ports in order to make the software run. These forms of "hardware locks" were somewhat effective since you need access to advanced and expensive data analysis equipment to figure out how they work.

### 3.3.2. The CD-ROM

With the introduction of the CD-ROM some of the piracy problems were briefly solved. In the early nineties computer hard drives were trailing behind the CD in storage capacity. It would take several hard drives to store the information contained on one CD. But as hard drives evolved, the storage capacity on a CD remained the same, and soon CDs could be copied as well. When the CD-burners showed up, the software- and music industries got a whole new problem.

For software producers the solution was to implement new forms of copy protection on the CDs. In the beginning this was made by making illegal table of contents on the CD, hence making the recording software unable to make a copy. Other protections involved making large dummy files linked to other files on the CD, to oversize or overburn the CD making the copy too large to burn, or to introduce physical errors on the discs.

The most recent CD-ROM copy protection schemes consist of software based solutions with digital signatures and encrypted wrappers that secure the content of the CD. When a user inserts an original disc in a CD-ROM drive, the authentication software reads the digital signature, allowing the program to be decrypted and run normally. If an unauthorized copy is loaded, the authentication software will no longer be able to find the digital signature, and the copy will not run.

The audio CD producers have also begun applying copy protection to their products. In general, they all share the aspect of making the CD unreadable by a computer CD-ROM drive, thus rendering it useless to rip [11]. This is done by “hiding” information that the CD-ROM drive needs to navigate on the CD. For instance: a CD-ROM drive always reads the last session on a multi-session CD. A CD player, however, can not use multi-session CDs and will therefore only read the first session.

### 3.3.3. DVD

In 1994, there were two competing formats for future multimedia storage. Sony and Philips had developed the MMCD (Multimedia CD) and Toshiba and Warner the SD (Super Disc). In 1995, the companies agreed on a single standard format they called DVD (Digital Versatile Disc). The DVD is a high capacity CD-size disc for video, multimedia, games and audio applications. Capacities for the read-only disc range from 4.7GB to 17.1GB. There are several different DVD formats available on the market.

### 3.4. Regional codes

Motion picture studios want to control the home release of movies in different countries because theater releases are not simultaneous. Also, studios sell distribution rights to different foreign distributors and would like to guarantee an exclusive market. Therefore they required that the DVD standard include codes that can be used to prevent playback of certain discs in certain geographical regions. Each player is given a code for the region in which it is sold. The player will refuse to play discs that are not coded for its region. This means that a disc bought in one country may not play on a player bought in another country. Some people believe that region codes are an illegal restraint of trade, but there have been no legal cases to establish this.

Regional codes are entirely optional for the maker of a disc. Discs without region locks will play on any player in any country. It is not an encryption system, it is just one byte of information on the disc that the player checks. There are 8 regions (also called "locales") [8]. Each region is assigned a number. Players and discs are often identified by the region number superimposed on a world globe. If a disc plays in more than one region it will have more than one number on the globe.

- |  |
|--|
| <ul style="list-style-type: none"><li>1: U.S., Canada, U.S. Territories</li><li>2: Japan, Europe, South Africa, and Middle East (including Egypt)</li><li>3: Southeast Asia and East Asia (including Hong Kong)</li><li>4: Australia, New Zealand, Pacific Islands, Central America, Mexico, South America, and the Caribbean</li><li>5: Eastern Europe, Indian subcontinent, Africa, North Korea, and Mongolia</li><li>6: China</li><li>7: Reserved</li><li>8: Special international venues (airplanes, cruise ships, etc.)</li></ul> |
|--|

Regioncodes around the world.

Some players can be "hacked" with special command sequences from the remote control to switch regions or play all regions. Some players can be physically modified ("chipped") to play discs regardless of the regional codes on the disc. Many retailers sell players that have already been modified for multiple regions, or in some cases they simply provide instructions on how to access the "secret" region change features already built into the player.

The high quality of video and audio has made DVD a very popular product. A 4.7GB DVD can store 133 minutes of MPEG-2 coded video. To protect the content of DVD movies the companies involved chose the CSS (Content Scrambling System) developed by Matsushita. CSS uses a 40-bit proprietary encryption algorithm, designed to comply with the strict US crypto-export regulations [7].

Descrambling requires a pair of keys. One of the keys is unique to the disk, while the other is unique to the MPEG file being descrambled [2]. The keys are stored on the lead-in area of the disk, which is generally only read by compliant drives. The goal of the CSS was twofold. First and foremost, it was designed to prevent bit-by-bit



copying of the MPEG file since such a copy would not include the keys. Secondly, it would force the manufacturers to make compliant devices since CSS scrambled discs will not play on non-compliant devices. A company called DVDCCA (DVD Copy Control Association) was formed to license CSS to DVD hardware manufacturers, disc manufacturers and producers of related products.

### **3.4.1. DeCSS**

In October 1999, an anonymous group of programmers based in Germany developed a program that would decrypt DVD content on Windows or Linux computers without using software licensed from the DVDCCA. They developed the software by reverse engineering (that is, by studying how a licensed program interacts with the DVD, and replicating that behaviour), and they were aided by both the weakness of the CSS encryption method and an error propagated by one of the DVD CSS licensees (a US-based company called Xing) [18]. They called the Windows program DeCSS and the Linux program css-auth.

With the release of DeCSS and css-auth the DVD protection was lost. Pirates started ripping DVD content and distribute it in the form of compressed DivX or MPEG files. Recently, with the introduction of high-speed Internet connections, entire .vob files, which are complete DVD movies of about four GB, are being distributed and burned on recordable DVDs with little or no loss of quality.

## 4. Cryptography

All Digital Rights Management solutions use some form of encryption, so it is vital that the reader has some basic knowledge on the subject. This section goes through the basics on frequently used terms related to cryptology.

Information security issues on physical documents have been protected by complex mechanisms and protocols all through the history of mankind. For example, to protect paper currency from counterfeiting special inks and material are used. Another example is handwritten signatures that have been used for a long time to validate information on documents. We learn to produce a handwritten signature and use this daily to confirm our identity and validate documents [5].

Information was typically stored and transmitted on paper but now most is stored and transmitted digitally. Information has been kept confidential by storing the physical document in a secure location. It has been fairly easy to keep this confidentiality during transportation to the receiver for example by keeping the document in a sealed envelope. Digital information is easily copied, altered and spread, which makes it much more difficult to protect compared to information on physical documents [25]. Some digital information also needs to be protected in the same way that information has been protected in the past. It must be possible to:

- Identify the source of the digital information.
- Validate the digital information.
- Protect the digital information from unauthorized copying.
- Keep the digital information confidential.

Cryptography (science of secret writing) is not intended to be the only means of digital information security, but rather one of several tools. The goals of cryptography is the following:

1. *Confidentiality* is a service used to keep the content of information from all but those authorized to have it. *Secrecy* is a term synonymous with confidentiality and privacy. There are numerous approaches to providing confidentiality, ranging from physical protection to mathematical algorithms which render data unintelligible.

2. *Data integrity* is a service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution.

3. *Authentication* is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc. For these reasons this aspect of cryptography is usually subdivided into two major classes: *entity authentication* and *data origin authentication*. Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed).

4. *Non-repudiation* is a service which prevents an entity from denying previous commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary. For example, one entity may authorize the purchase of property by another entity and later deny such authorization was granted. A procedure involving a trusted third party is needed to resolve the dispute.

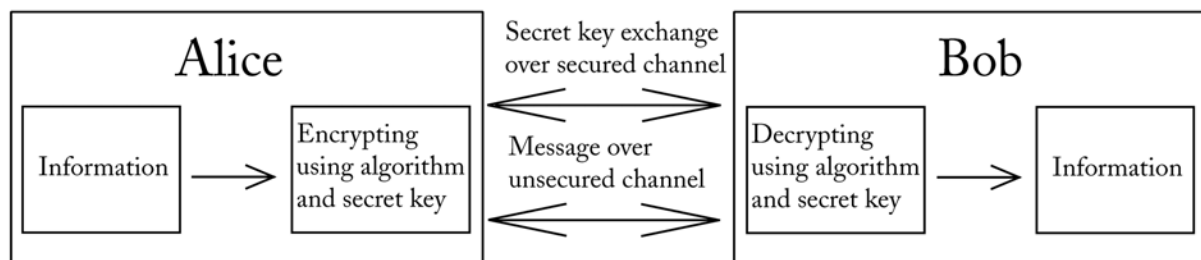
Quote: Handbook of Applied Cryptography, by A. Menezes, P. van Oorschot, and S. Vanstone.

The purpose of encrypting digital information or plaintext as it is called in cryptography is to ensure that the information is kept secure. With a key and an algorithm, a ciphertext (encrypted message is called ciphertext) is created. To decrypt the ciphertext and retrieve the information the correct key and algorithm is needed. While the information is protected inside the ciphertext, it is intended to be safe to transmit the information through unsecured channels, such as the Internet. The algorithm is seldom secret, but the key always is [25].

### 4.1. Algorithms

There are two main types of encryption algorithms, symmetric and asymmetric algorithms. Symmetric algorithms use the same key for encryption and decryption, or in some case, the decryption key is easily derived from the encryption key.

Symmetric algorithms can be divided into block ciphers and stream ciphers (cipher: A method of encryption and decryption) [5]. Block ciphers break up the plaintext message and then encrypt a block at a time. Stream ciphers encrypt a single bit at a time. Stream ciphers are suited for real time applications, such as broadcasting. Both the source and the destination use the same key which means we face a major challenge: how to exchange the secret key securely and efficiently [25].



Symmetric algorithm

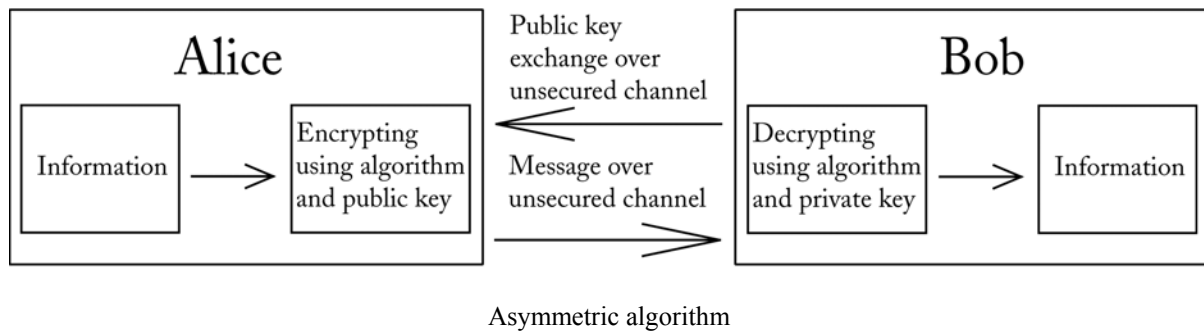
Asymmetric algorithms, or public key encryption, use a different key for encryption and decryption. The decryption key cannot be derived from the encryption key. The decryption key is referred to as the private key, and the encryption key as the public key.

# Digital Rights Management

## Evaluation of existing systems

Anders Burström

Jonas Callander



Alice only needs the public key to encrypt the message and Bob is the only one able to decrypt the ciphertext. Not even Alice can decrypt the cipher, even though she knows its contents. Bob needs to keep the private key secret, which means there is no need to exchange the private key with anyone. Anyone who possesses the public key can encrypt messages that only Bob can decrypt. Asymmetric encryption is in general substantially slower than symmetric encryption [5].

Symmetric and asymmetric encryptions are often used together. A public key is used to encrypt a symmetric secret key and then exchanged. After that, the communication uses a symmetric encryption. This solves the issue of exchanging the symmetric secret key over an unsecured channel [25].

## 4.2. Digital Rights management and cryptography

A cryptography model usually consists of Alice sending Bob some data, while Eve tries to attack the communications. In this model it is always assumed that both Alice and Bob can be trusted and that they know some secret, which Eve wants. In the DRM model, even Bob cannot be trusted with any keys or even unencrypted data. In fact, Bob must be assumed to be hostile. Cryptography can solve the problem of securing communications in DRM, but it is not a complete solution.

Cryptography protects the actual data, but in DRM, there is also a need to protect the actual executable programs that play the content. A successful DRM system requires some form of trusted software component to perform integrity checking, content decryption and to enforce the usage rights associated with the content. The DRM system must be able to preserve its integrity and hide the decryption keys in a hostile environment. As attackers develop more effective attacks, the lifetime of a DRM system must be considered limited. In case of a security breach, the software must be easy to replace or upgrade.

### 4.3. Identification and signatures

Most people have been through an identification and authentication process, perhaps through a login procedure on a computer. The identification is the user name and to prove our identity we authenticate ourselves with the password.

This identification works well enough in most situations, but sometimes the need for security is higher. Perhaps we do not want to share our secret password before we are certain that the receiving end is whom we intend to share our password with.

#### 4.3.1. Identification protocols

Before Alice shares her secrets with Bob, she needs to know if Bob is who he claims to be. This is done through following a protocol which ends with Alice accepting or rejecting that Bob is who he claims to be. The identification protocol needs to meet the following minimum objectives [5]:

- Bob is able to successfully authenticate himself to Alice.
- Alice cannot reuse an identification exchange with Bob to impersonate Bob to a third party. (Transferability)
- Any third party should not be able to carry out the protocol and playing the role of Bob and cause Alice to accept that the third party is Bob. (Impersonation)

#### 4.3.2. Digital signatures

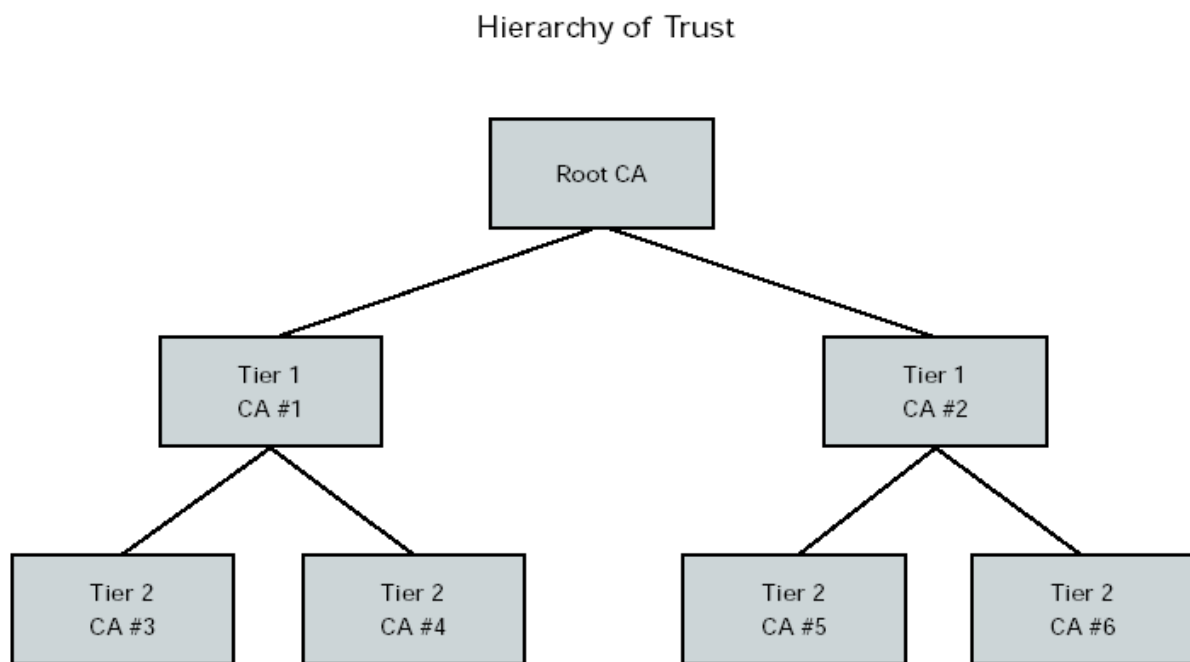
Identification protocols and digital signatures are closely related. Digital signatures use asymmetric encryption to sign documents. Digital signatures have a few more objectives to fulfil compared to identification protocols, such as signatures must be verifiable and non-repudiative. In other words: if a dispute arises where a party denies that it signed a document, an unbiased third party should be able to solve the dispute without requiring access to the signer's private key, which is used to sign the document. The digital signature also needs to authenticate the document to ensure that the document is not altered in any way [5].

Signatures are created by using a hash function, an algorithm using the signer's private key and the document. The result is a "fingerprint" which is generally much smaller than the signed document. Even though it is much smaller than the document, it is unique to this document. This fingerprint is the signature and is normally attached and transmitted with the document. To verify the signature the public key and the document is needed. Using the same hash algorithm, the public key, the document and the same signature will generate two matching values if the document is unaltered [5].

### 4.3.3. Certificate Authorities

For Alice to be certain that the document is authentic and comes from Bob, Alice needs to know that she has the correct public key. The public and private keys are only numbers; they do not have any natural association with a person. In a transaction only involving two parties, Bob could simply communicate his public key over the phone.

However, this is not practical when dealing with communication with artificial entities on the Internet such as commercial corporations. The solution is the use of trusted third parties. The trusted party is a “Certificate Authority” that associates a signer with a specific public key. The certificate authorities issue certificates with the subscriber’s public key and algorithm included. To authenticate the certificate the certificate authority digitally signs it. The certification authority’s public keys can be used to verify the certificate [3].



Certificate Authorities hierarchy [3]

If you trust the certificate authority, you trust that you have the correct public key. The certificate authorities work in a hierarchy to verify each other. You might say that if you trust one, you trust all certificate authorities.

## 5. Microsoft Digital Rights Management

This section is focused on Microsoft's contribution to Digital Rights Management. Since Microsoft is such a force in the personal computer industry they are often able to set standards for the industry. For that reason it is interesting to take a closer look at their solution. Microsoft is also the only manufacturer of DRM systems that provides extensive documentation and information about their products. In the past Microsoft have not showed much interest in Digital Rights Management. During the last few years their interest has increased, which is not strange when you consider that many of Microsoft's future products are DRM related, such as Palladium (Microsoft's vision of the "secure PC" and "secure OS"). Information in chapter 5.2 to 5.3.3 comes from Windows Media Rights Manager 9 Series SDK [22], unless stated otherwise.

### 5.1. Purpose of Microsoft Windows Media Digital Rights Management

The purpose of Microsoft's DRM solution is to deliver protected digital media material that authorized users easily can enjoy on their computer.

With Windows Media DRM, retailers and record labels can set up Internet music stores to distribute digital media files. Content providers can also remain confident that their digital media files will stay protected, no matter how widely they are distributed.

Quote: Microsoft DRM information

<http://www.microsoft.com/windows/windowsmedia/wm7/drm/benefits.aspx>

The protected digital media file can only be played in Windows Media Player and the content provider can set up a large number of rules for the protected media file.

### 5.2. Overview

The digital media file is packaged and encrypted with Windows Media Rights Manager. The key to unlock the encrypted file is stored in an encrypted license, which is distributed separately. To the encrypted file, other information is added to a content header, such as the URL where the license can be acquired. The encrypted file is saved in Windows Media Audio (.wma extension) format, or Windows Media Video (.wmv extension) format.

To play the file the user needs a media player that supports Windows Media Rights Manager. This means Windows Media Player 7 or later. Each player is unique and linked to the host computer.

When encrypted and packaged, the file can be distributed through any digital means. Whenever a user tries to play the file and a valid license is not found, the process of acquiring a license begins. Before a license is granted, the user might have to register, or pay for the license. The license is then downloaded from the URL specified in the content header of the file.

The license contains the key to unlock the encrypted file and the rules for the license. These rules may include how many times the user may play the file before the license expires or if the user can backup and restore the license. It is also possible to specify the level of security the license demands to allow the file to be played. The license is generated for the specified file and media player and cannot be used on any other media player, file or computer.

### 5.3. Security overview

#### 5.3.1. Keys and encryption

The content provider either specifies or generates a public key. A private key is generated using a secret value. The private key is used to encrypt/decrypt the Windows Media File and the public key is used together with the secret value to generate the private key. The secret value must be shared between the content provider and the license issuer. How this is done is not specified in Microsoft's documentation.

Before the license is issued for a file a secure, encrypted session is initiated between the license issuer and the media player. This is to protect the integrity and secrecy of the data exchanged between the license issuer and the media player. Microsoft does not mention much about this secure session except that a session key is used which indicates that a symmetric algorithm is used. How this session key is exchanged between the license issuer and the media player is not mentioned.

Microsoft does not share any detailed information about the encryption used to encrypt the media files. Microsoft admits that the algorithm is based on published ciphers and since there is a public and private key, it must be an asymmetric algorithm.

Windows Media Rights Manager, the server that packages files and issues licenses, encrypts a given media file with a full-strength encryption algorithm. This algorithm is based on published ciphers that have with stood the scrutiny of the cryptographic community. No decryption key is contained in the Windows Media Format file container. Decrypting an isolated Windows Media file would require breaking industrial-strength cryptographic algorithms.

...

Windows Media uses one of the strongest DRM encryption schemes available, which would take days of supercomputer time to decode.

Quote: Microsoft DRM Frequently Asked Questions



### 5.3.2. Security on the user's computer

The license server authenticates the user's media player by using digital certificates with a unique public key to identify the media player. The public key is crosschecked with a list of compromised media players and the media player components are controlled. Licenses are only issued to authenticated media players. The private key in the license is encrypted in such a way that only the target media player can decrypt the key. A digital signature is used to protect the rules in the license.

Microsoft tries to protect the decrypted content through a secure path from the media player to the destination hardware. This is done through a certified Microsoft component that verifies all the components, for example that the sound card drivers are certified. The content is not decrypted if uncertified or if compromised components are detected.

### 5.3.3. Secure Audio Path

To make it impossible for pirates to intercept data at lower application levels, Microsoft has implemented a technology called Secure Audio Path, SAP. The requirement that an audio file must be played only through a secure audio path is specified in the DRM license and automatically enforced by the DRM client components.

If SAP is not applied when the user plays a protected music file, the encrypted content is passed to the DRM client component. The client verifies that the application and the DRM component are valid, decrypts the content and sends it to the application, which sends it to the lower-level audio components. At this point, the decrypted music is available to applications that can intercept the audio bits [24].

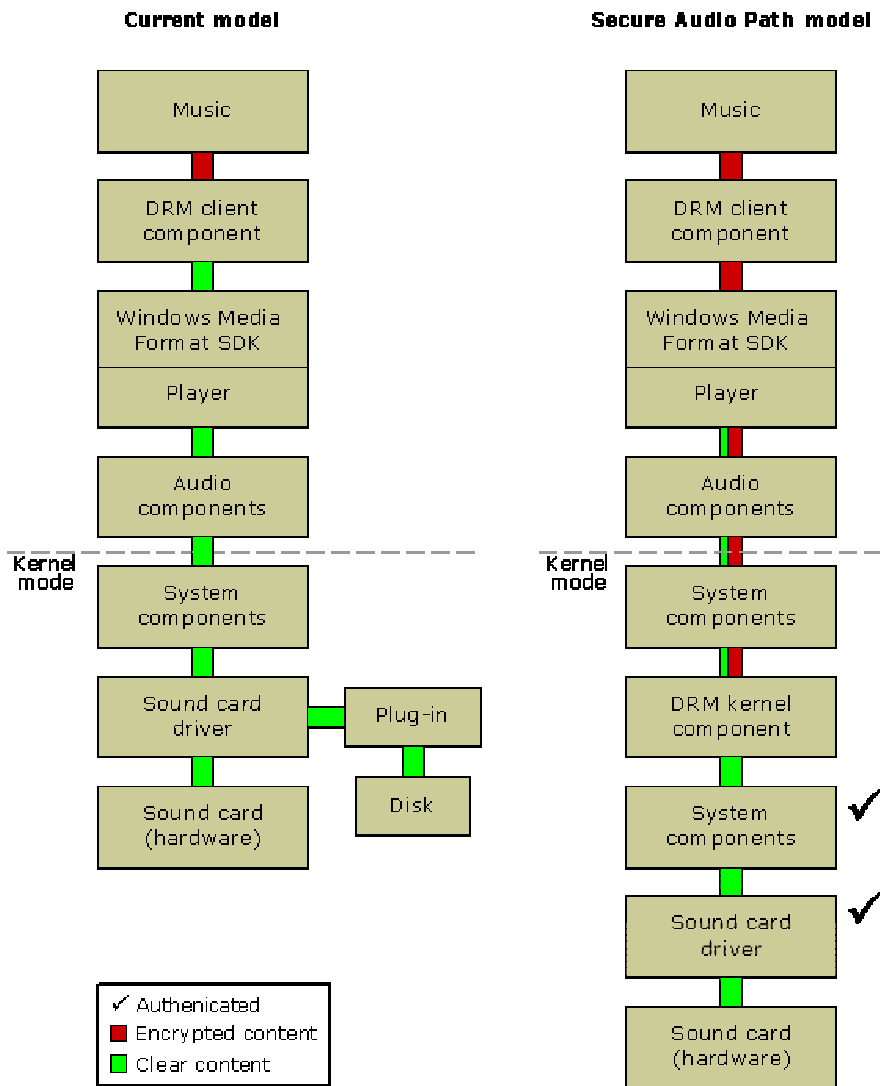
When SAP is used, the content is not decrypted by the application, but passed in an encrypted state to the lower level components. The lower level components have been authenticated by Microsoft and are considered trustworthy because they only make the audio content available to other authenticated components. In this way, the content remains protected all the way to the driver level [24].

# Digital Rights Management

## Evaluation of existing systems

Anders Burström

Jonas Callander



The Secure Audio Path model [24]

In the SAP model, applications are unable to modify protected music. When an application tries to intercept a music signal, the signal sounds like random noise. Some applications are designed to view a music signal, but not modify it. To make it possible to view the signal, a small part of the music is decrypted and sent in clear form together with the encrypted content. The unprotected signal quality is very poor, but can suffice for applications that are designed to view signals [24].

Another feature in the SAP model is the ability to disable the digital output of the sound card. This lets the content owners or license issuers disable the digital output in order to stop users from making perfect digital copies. The user can still listen to the decrypted music, but is limited to use the analogue output with somewhat lower quality [24].

### 5.4. System upgrades

There is an option in WMP that enables users to make copy protected files. Those files can only be played on the computer they were made on. If an upgrade of the system is made, the protected files can no longer be played on the computer. This also applies to purchased or downloaded files that use copy protection. In order to be able to play the files you need to make a backup of all your licenses before upgrading and restore the licenses after the upgrade is completed. The following text comes from Microsoft's Support site and concerns CPU upgrades:

The Digital Rights Management (DRM) system on a computer may not work if you change the CPU. You may receive the following error message: The license to play the packaged media is invalid.

This issue occurs because the DRM system maintains an internal hardware identifier (ID) that is based on the CPU ID of the CPU in the computer. If the CPU is changed, the hardware ID that DRM maintains does not match the CPU ID of the new CPU. In this case, DRM does not work because this discrepancy causes DRM to determine that there has been an unauthorized attempt to move DRM-protected content to another computer.

Quote: Microsoft support

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;q301082>

To be able to restore a license, the computer must be connected to the Internet in order to reach the Microsoft License Management Service. The user is allowed to restore a license a limited number of times. Specifically, the service does not enable licenses to exist on more than four unique computers, and may require user information after the first restore. Each time a license is restored, the License Management Service tracks it and increments the count for that license by one. If the License Management Service recognizes the computer as the one that made the license backup, the count is not increased. A computer is considered to be different if the operating system is changed or re-installed. If the computer from which the license was backed up is different from the original computer, the License Management Service issues a new license to the new computer. Otherwise, the license that was previously issued to that computer is reissued [23].

In accordance with Microsoft's fraud detection policy, when a license has been restored a certain number of times, the application receives a URL from the DRM components and is responsible for opening a browser and displaying the Web page, which indicates that the license agreement might have been violated. The user must contact the license distributor, who must then determine whether the request is valid.

Quote: Microsoft support

It is up to the content owner to allow or disallow the right to back up and restore the license. For instance, if a record label decides to disallow the right to back up the licenses of the songs they produce, the customer can only play the songs as long as no changes are made to the user's computer. If a hard disk fails, the CPU is changed or the OS is re-installed, the licenses become invalid and the songs must be purchased again.

## 5.5. Testing Microsoft Windows Media Digital Rights Management

We decided to do a simple test of Microsoft Media DRM. We wanted to try to transfer a working license to another computer. We did a fresh install of Windows XP and acquired a public key for our media player. After that, we downloaded a few media files and then tried to retrieve licenses for those files. The files we downloaded were Microsoft's demonstration files of how their DRM works. When we played a file, it wanted to download a license, which we allowed it to do. The problem was that we did not get any license; instead, we got a message that the page could not be found. For three days, we tried to download a license, without any luck. This is a perfect example of one of the weaknesses of Microsoft's implementation of DRM. The license server must be online and reachable at all times.

We tried one of Microsoft Media DRM partners, [www.DMDSecure.com](http://www.DMDSecure.com). They had their own demonstration files, and a license server that was online and working. We downloaded their files and licenses making sure that they worked the way they were suppose to work. We then extracted the hard drive from the computer with Windows XP, media player and the demonstration files and installed it in another computer. The computer we installed the hard drive in had similar, but not identical hardware. We tried to play one of the demonstration files, but the media player immediately asked for a security update (public key). After that, the files could not be played unless we downloaded a new license. It is obvious that Microsoft Media DRM really does check the hardware for changes. If this check is too sensitive, it might annoy customers who will lose their licenses when they make changes to their computer hardware or their drivers.

## 5.6. Cracking Windows Media Audio

This chapter deals with the two attempts to crack Windows Media Audio that have been successful so far. It also contains some experiments made with both programs on .wma-files with different versions of Windows Media. The first program, named "Unfuck.exe" (sic) is a work-around and the second; "FreeMe.exe" actually cracks the encryption of the audio files.

### 5.6.1. "UnFuck.exe"

On the same day Microsoft launched its Windows Media Version 4 in 1999, some crackers released a program called UnFuck.exe. The application intercepted the audio data at driver level on its way to the sound card. That way it could save the data stream from a protected .wma-file as an uncompressed .wav-file and later rebuild it as an unprotected .wma-file.

# Digital Rights Management

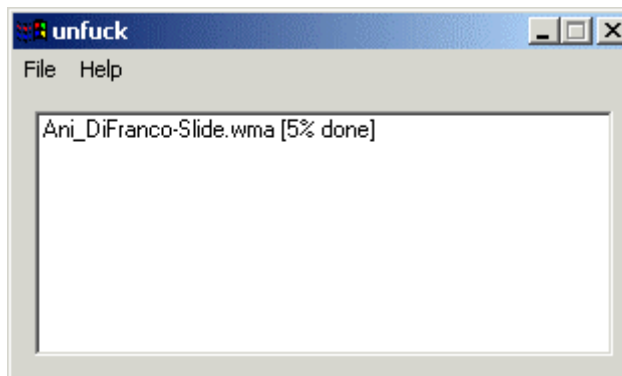
## Evaluation of existing systems

Anders Burström

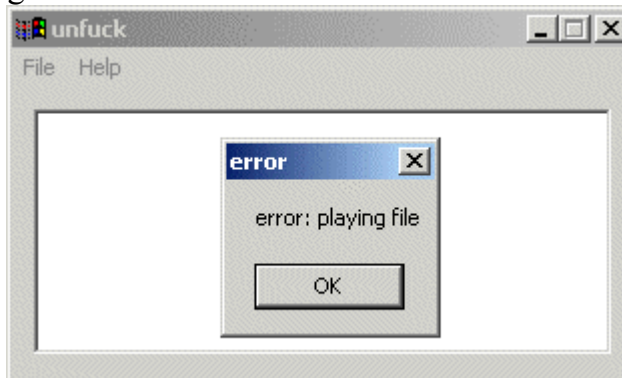
Jonas Callander

To determine if this “old” program still works, we downloaded some .wma-files made with different Windows Media versions and with different licenses. The first three .wma-files were made with Windows Media version 8 and the other three with Windows Media version 9.

The WM8 files have a license that expires after 30 days and they have different restrictions when it comes to copying. To remove the protection you simply load the file in the program (Unfuck.exe) and it automatically starts to convert the file.



All WM8 files that we downloaded from <http://gohastings.neuroticmedia.net> were successfully cracked with “Unfuck.exe.” When we tried the WM9 files downloaded from <http://entertainment.msn.com/download/Default.aspx> the program generated this message:

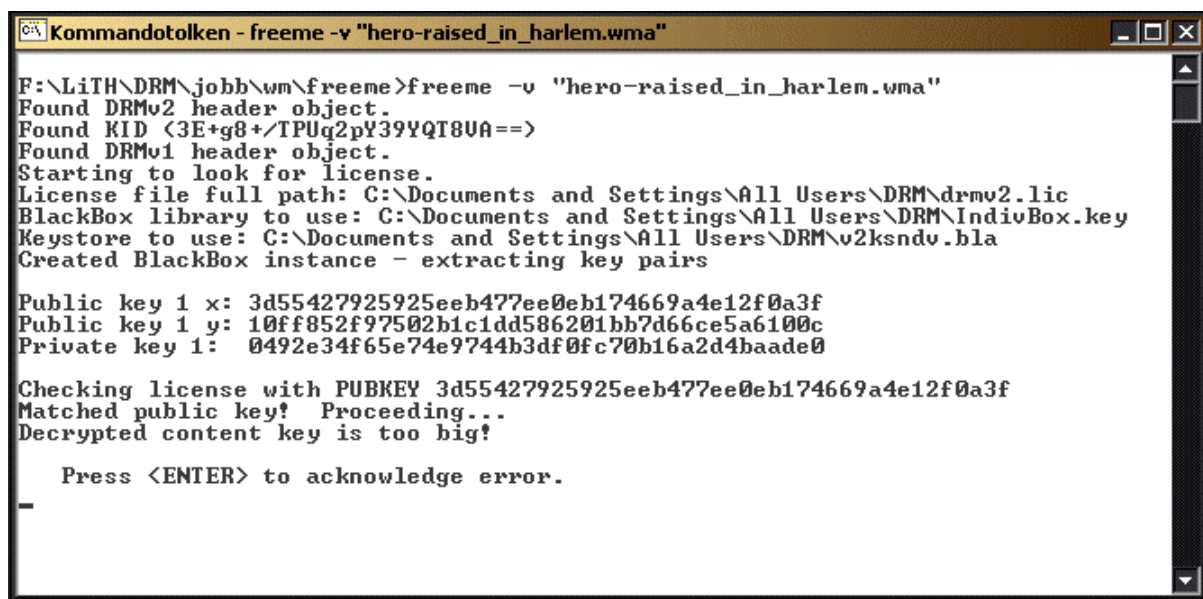


A browser window was opened (<http://windowsmedia.com/wmrm/wmrm.asp>) and we were asked to upgrade to WMRM (Windows Media Rights Manager) version 7. The program probably emulates the Windows Media Player and intercepts the data stream at driver level. This fails when we try to crack the newer WM9 files, since “Unfuck.exe” is not a WMRM7 compatible player. However, some WM9 files can still be converted. When we tried to make our own copy protected file with WMP9, the file was effectively converted with “UnFuck”.

### 5.6.2. "FreeMe.exe"

On October 18 2001, a user called "Beale Screamer" posted a message on the newsgroup sci.crypt. It contained a technical description of Microsoft's Digital Rights Management Scheme as applied to .wma-files, together with a program called "FreeMe.exe" and the source code of that program. The FreeMe program removes the protection of the .wma-files by removing the encryption. This is much more effective than to capture the data streams en-route to the sound card.

We tried FreeMe on all of the .wma-files mentioned earlier and none of them became unprotected. This is what happens when you try to run FreeMe:



```
Kommandotolken - freeme -v "hero-raised_in_harlem.wma"

F:\LiTH\DRM\jobb\wm\freeme>freeme -v "hero-raised_in_harlem.wma"
Found DRMv2 header object.
Found KID (3E+g8+/TPUq2pY39YQT8UA==)
Found DRMv1 header object.
Starting to look for license.
License file full path: C:\Documents and Settings\All Users\DRM\drm2.lic
BlackBox library to use: C:\Documents and Settings\All Users\DRM\IndivBox.key
Keystore to use: C:\Documents and Settings\All Users\DRM\v2ksndv.bla
Created BlackBox instance - extracting key pairs

Public key 1 x: 3d55427925925eeb477ee0eb174669a4e12f0a3f
Public key 1 y: 10ff852f97502b1c1dd586201bb7d66ce5a6100c
Private key 1: 0492e34f65e74e9744b3df0fc70b16a2d4baade0

Checking license with PUBKEY 3d55427925925eeb477ee0eb174669a4e12f0a3f
Matched public key! Proceeding...
Decrypted content key is too big!

Press <ENTER> to acknowledge error.
-
```

FreeMe.exe

Microsoft has effectively plugged the security leak and this program will not work with newer .wma-files. As the screenshot shows, the two public keys and the private key are displayed, but the content key, which unlocks the media, is too big. Microsoft has altered one or more of the encryptions used in their DRM solution. It is therefore possible that the public and private keys seized by FreeMe also are wrong.

### 5.7. Xbox

Xbox is Microsoft's first gaming console, built with technology closely related to a PC. It is so closely related to a PC that some parts are interchangeable between the Xbox and the PC. The Xbox is capable of online communication through "Xbox Live", a Microsoft subscription service. What makes the Xbox interesting from a Digital Rights management view is that Microsoft has tried to create a secure platform. It is possible to pay for and download music, movies and so on. The rights

to use the copyrighted material are controlled by a practically identical DRM system as on the PC, with the added security that each Xbox has a unique serial number. The Xbox is designed to only run code signed by Microsoft and unpirated game, movie and music CDs/DVDs. The Xbox is only able to play DVDs from the correct region [20].

### 5.7.1. Xbox security

Xbox was released in November 2001 and immediately people began to look for flaws in the Xbox security, some people with specific goals, such as to change the operating system to Linux and some to enable pirated games to run on the Xbox. Other people looked for security flaws out of curiosity or for the challenge.

In less than seven months after the launch of the Xbox, a MIT student released a paper about the Xbox security<sup>3</sup>. This paper goes in-depth and reveals details of the Xbox hardware cryptosystem and physical protection [4].

Not long after that, Xbox Linux Project<sup>4</sup> released a press release revealing that they had managed to change a hardware modified Xbox operating system to Linux. This modified Xbox could run any software, signed or unsigned by Microsoft [28].

The past year a small industry has emerged manufacturing and selling Xbox modification kits, enabling the Xbox owner to play pirated games and execute unsigned code. The option to execute unsigned code has made it possible for Xbox owners to execute the “Xbox media player” that enable users to play virtually any digital media, original or pirated [29]. While it is not possible to use “Xbox Live” with a modified Xbox, these kits often include a switch to disable the modification [28].

---

<sup>3</sup> Jason Brown, Xbox System Software Overview

<sup>4</sup> <http://xbox-linux.sourceforge.net>

## 6. Privacy and DRM

### 6.1. Who can we trust?

Computer security during the last decades has been focused on malicious code, such as viruses and trojans, and to keep unauthorized users from accessing systems. The security model for DRM is somewhat different from the typical Internet security model. In general, system components are deployed in a trusted environment, for example a company's web server with restricted physical access. In DRM, content providers must deliver their content to users across a network, which they have no control over. Furthermore, they cannot assume that the user or the user's software can be trusted. Content providers must also assume that the user has an unlimited amount of time and resources to attack and bypass the content protection mechanisms. This is a key challenge in DRM; how do you trust people who cannot be trusted [26]?

### 6.2. Possible solutions

One possible solution is to create a trusted hardware platform that cannot be tampered with. There are several examples of such systems; smart cards for satellite TV and Microsoft's gaming console Xbox to name a few. It has been shown that trusted hardware platforms can be hacked and bypassed and this will probably be the case for future platforms as well. Most trusted hardware platforms are BOBE-weak (Break Once, Break Everywhere). This means that if a hardware modification can be made on one type of platform, it will probably work on all platforms of the same type. Microsoft's X-box is a typical example of this. A secure hardware solution for DRM is not likely to be implemented. It would be too costly, considering both time and money, to equip all users with the hardware required. The difficulty to upgrade if the hardware security is compromised is also a factor that makes trusted hardware platforms not suitable for DRM solutions.

### 6.3. Consumer privacy

Traditionally, individuals have been able to anonymously consume ideas that have been presented in books, newspapers, music and movies. With the introduction of DRM, this could change. All existing DRM technologies are able to monitor and register the individual user's consumption. Many, if not all, DRM systems require the user to identify and authenticate a right of access to the content. The most common method of gathering user information in today's DRM systems is to track the user via downloads or subscription. This is done by giving the customer a unique ID and to gather information on the customer's usage history of the products he or she



downloads. This results in a collection of an individual's interests and usage patterns. When the customer is linked to the content, the company can build records for target marketing [12]. This can result in something called "price discrimination". This is when a company sells items at different costs to different consumers [6]. To be able to use price discrimination, the company must have an idea of how much the individual customers are willing to pay for the content. Suppose Alice is willing to pay 12€ for a CD and Bob is willing to pay 17€ for the same CD. If the company knows this information, it will be tempting to sell Bob a CD for a higher price than Alice.

There are legitimate reasons for DRM to monitor and collect data from its users. These include quality of service enhancement and traffic modeling for infrastructure planning; untargeted marketing and advertising; risk management; backup and archiving; counting and statistical sampling, which often is used for payment to artists. However the same data that is collected for these legitimate reasons can also be used in illegitimate, or perhaps annoying and distasteful ways. Through this information it could be possible to guess everything from a user's political opinion to sexual preferences. Even though our current transactions with electronic money already allow for some collection of similar data it is even more obvious and organized in DRM.

The one thing that concerns the Internet users the most, according to several surveys, is the monitoring of their habits. It is strange that the manufacturers of DRM systems totally ignore that fact and continue to monitor and register the user's behaviours. This is one of the factors that make DRM a less attractive option compared to other forms of media distribution.

According to the famous 1993 Pat Steiner cartoon in The New Yorker, "On the Internet, nobody knows you're a dog." But in practice, there are many who not only know you are a dog, but are familiar with your age, breed, illnesses, and tastes in dog food. The Internet offers not only the possibility of unprecedented privacy, but also of unprecedented loss of privacy, and so far privacy has been losing.
--

Quote: Privacy, Economics, and Price Discrimination on the Internet, Andrew Odlyzko, 2003

### 6.3.1. Privacy according to Microsoft

When a user is restoring the license, information is sent to Microsoft that uniquely identifies the user's machine. The information is stored in a database, located in the US, which keeps track of the number of times the user attempts to restore the licenses. When the user tries to restore the licenses, he or she may be asked to provide some personally identifiable information [23]. According to Microsoft, this is done to "prevent fraudulent restores and piracy of protected content".

# Digital Rights Management

## Evaluation of existing systems

Anders Burström

Jonas Callander

The personally identifiable information that you provide will not be used for any other purpose. It will be securely stored in a dedicated database located in the United States of America, and will be kept separate from information you may have provided to Microsoft in other contexts. This information will not be shared with any other services either internal or external to Microsoft.

Quote: Microsoft Windows Media Rights Manager Privacy Statement

<http://drm7.smdisp.net/0009/policy.htm>

Backing up and restoring licenses is not the only time the user has to provide Microsoft with a unique identification of the machine. This also applies to upgrades of the security level (individualization) of the Media Player. Microsoft keeps track of the number of times the user attempts to upgrade the security level of the Media Player and which security updates that is downloaded to the user's machine. This is done to "help Microsoft prevent security breaches that could affect legitimate users". However, Microsoft also states the following in another section of their DRM documentation:

Individualization (also referred to as a "security upgrade") is a process that makes one instance of player unique from all other instances of the software by modifying the protected content module on a consumer's computer. As a result, if an individualized player installation's DRM functionality is compromised, only that installation of the software is affected. Individualization eliminates global hacks to the software; otherwise, an entire application would need to be revoked, which would affect many consumers rather than one.

Quote: Microsoft Windows Media Rights Manager Privacy Statement

So on one hand Microsoft claims that breaching security on one computer will not result in a global hack, but on the other hand they track every single security upgrade that is made in order to prevent security breaches that could affect all users.

## 7. The state of DRM today

In the introduction we mentioned some criteria that had to be fulfilled in order for a DRM system to be successful. Which of these criteria are met in the present DRM systems?

Present DRM systems offer the following to a consumer:

### **Reliability**

- We believe that this criterion is fulfilled. The reliability of the DRM system is better or equally good as the reliability of the user's Internet Service Provider. No computer system works flawlessly, and the DRM systems are no worse than anything else connected to computers.

### **Value**

- The pricing of the media is somewhat mixed. The ability to offer other forms of benefits to the consumer is generally neglected.

### **Privacy**

- The privacy issues are numerous and practically ignored by the present DRM systems. There is no space for privacy the way DRM is implemented today, as mentioned in chapter 6.3 and 6.3.1.

### **Availability**

- Although we had trouble obtaining licences for Microsoft's own demonstration files, it really is up to each distributor to keep licence servers available to the consumer at all times. The service is available whenever the consumer wants but does not carry the same variety of products as other means of distribution. The services are often not available on different platforms. It is not likely that a DRM system will be available for open source platforms, such as Linux, since this would make the source code available to all users.

### **Common format**

- There is no common format today.

### **Fair use**

- The copyright owner's demands and the consumer's needs are always contradicting each other. Current DRM systems are unable to determine if a consumer is making copies for personal use or for illegal purposes, as stated in chapter 2.2 and 2.3.

# Digital Rights Management

## Evaluation of existing systems

Anders Burström

Jonas Callander

Present DRM systems offers the following to a copyright owner:

### **Piracy prevention**

- We believe that the media protection offered by present DRM systems is satisfying from the copyright owners point of view. We were unable to bypass the copy protection of newer media files as mentioned in chapter 5.5 and 5.6.

### **Security**

- Even though DRM does not work on a secure platform, the security must be considered high. Microsoft has effectively taken care of the few attempts to circumvent the security so far, as shown in chapter 5.6. It is up to the copyright owners to update their media files to keep them secured.

### **Payment**

- The copyright owners are being paid with DRM. With the right pricing and by making DRM more attractive, they would probably make even more money compared to traditional means of distribution.

Present DRM systems offer the following to a distributor:

### **Payment**

- A successful DRM system will generate money for the distributor, but so far, DRM as a solution has not been as successful as other types of media distribution.

### **Satisfaction**

- The copyright owners are probably satisfied with the present DRM solutions, but the consumers are not yet convinced of the benefits of DRM, since the consumer demands stated above are not fulfilled.

## 8. Conclusion

The present DRM systems are successful from both the copyright owner and the distributor's point of view. From a consumer perspective, the systems seem to be less rewarding than other forms of media distribution. There are not enough benefits for consumers that would give the technology the edge over competing distribution channels. Since the customers do not gain enough benefits by using the DRM systems, they will still buy their CD's and movies elsewhere. Without consumers the whole DRM idea will fail. Piracy will continue to thrive as long as copy protection or secure platforms do not provide the security they claim to provide. DRM media need to compete more with price and availability without sacrificing quality to attract customers.

DRM needs to be redesigned to take into account the consumer's privacy, or distributors need to convince consumers that their information is not used, and will never be used in any way to compromise their privacy. It is not likely that DRM distributors are able to convince people that their information is safe with them, since they do not appear to be as reliable as a bank.

The prices for downloaded songs are still high compared to songs on a CD. In addition, you have to burn the CD yourself and you do not get a cover leaflet. The ability to make copies for personal use is often limited through DRM restrictions. To be able to transfer the music to a portable device, the device must support the types of DRM protection used. The loss of a DRM license can render the media useless and the consumer will have to buy the media again. Needless to say, this would not affect the popularity of the DRM system in a positive way.

The present DRM systems have to compete with file sharing programs that make the media available for free. Until the piracy problem is solved, DRM will not be attractive to most consumers. It is not likely that piracy will ever be completely removed. For every high wall, there is a taller ladder.

We do not believe it is possible to design a DRM system that consumers, copyright owners and distributors are satisfied with. It is not possible to combine the demands of copyright owners and the users' claims of fair use.

## 9. References

### 9.1. Books and documents

1. Biddle, P., England, P., Peinado, M. and Willman, B. (2002). The Darknet and the future of content distribution. Retrieved August 21 2003.
2. Bloom, J. A. et al. (1999). Copy protection for DVD video. Proceedings of the IEEE 1999.
3. Cisco Systems. (2002). Introduction to Secure Sockets Layer.
4. Huang, A. (2002). Keeping Secrets in Hardware: The Microsoft XBox Case Study. Retrieved August 21 2003.
5. Menezes, A., van Oorschot, P. and Vanstone, S. (1996). Handbook of Applied Cryptography. CRC Press.
6. Odlyzko, A. (2003). Privacy, Economics, and Price Discrimination on the Internet. Retrieved August 21 2003.
7. Stevenson, F.A. (1999). Cryptanalysis of Contents Scrambling System. Retrieved August 21 2003.
8. Taylor, J. (2000). DVD demystified. Second edition. McGraw-Hill.

### 9.2. Internet resources

9. Accurite Technologies, Floppy Disk Drive Primer (2001)  
URL: <http://www.accurite.com/FloppyPrimer.html> (2003-08-21)
10. Benjamin Soans, Of Protectors and Pirates (May 1, 2001)  
URL: <http://www.pcquest.com/content/mac/100050126.asp> (2003-08-21)
11. CD Media World, CD/DVD Protections (Unknown)  
URL: [http://www.cdmediaworld.com/hardware/cdrom/cd\\_protections.shtml](http://www.cdmediaworld.com/hardware/cdrom/cd_protections.shtml) (2003-08-21)
12. Chris Hoofnagle, Jason Young, Nicole Anastasopoulos, In the Matter of Digital Entertainment and Rights Management (Jul 17, 2002)  
URL: <http://www.epic.org/privacy/drm/tadrmcomments7.17.02.html> (2003-08-21)
13. Copyright Law of the United States of America (1999)  
URL: <http://www.copyright.gov/title17/92chap1.html#107> (2003-08-21)
14. Electronic Frontier Foundation, Fair Use Frequently Asked Questions (and Answers) (Mar, 21 2002)  
URL: [http://www.eff.org/IP/eff\\_fair\\_use\\_faq.php](http://www.eff.org/IP/eff_fair_use_faq.php) (2003-08-21)
15. European Parliament, Directive 2001/29/EC (Jun 22, 2001)  
URL: [http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexplus!prod!CELEXnumdoc&numdoc=301L0029&lg=EN](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&numdoc=301L0029&lg=EN) (2003-08-21)
16. Fraunhofer-Gesellschaft, History, Audio & Multimedia MPEG Audio Layer-3 (Unknown)  
URL: <http://www.iis.fraunhofer.de/amm/techinf/layer3/> (2003-08-21)

# Digital Rights Management

## Evaluation of existing systems

Anders Burström

Jonas Callander

17. Gord Larose, Why DRM sucks (Unknown)  
URL: [http://www.info-mech.com/drm\\_flaws.html](http://www.info-mech.com/drm_flaws.html) (2003-08-21)
18. Gregory B. Newby Dr., Taking the High Road: CSS Issues (2000)  
URL: <http://www.ils.unc.edu/gbnewby/DVD/highroad.html> (2003-08-21)
19. The history of MP3 and how did it all begin (Unknown)  
URL: [http://www.mp3-mac.com/Pages/History\\_of\\_MP3.html](http://www.mp3-mac.com/Pages/History_of_MP3.html) (2003-08-21)
20. Jason Brown, Xbox System Software Overview (Unknown)  
URL: <http://www.xbox365.com/stories/xdkcomplete.shtml> (2003-08-21)
21. Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk (Apr 1, 2000)  
URL: <http://www.notisum.se/rnp/sls/lag/19600729.HTM> (2003-08-21)
22. Microsoft, Windows Media 9 Series Software Development Kit Documentation (Unknown)  
URL: <http://www.microsoft.com/windows/windowsmedia/9series/sdk.aspx> (2003-08-21)
23. Microsoft, Media Rights Manager Restore and Security Upgrade Privacy Statement (Unknown)  
URL: <http://drm7.smdisp.net/0009/policy.htm> (2003-08-21)
24. Understanding the Secure Audio Path Model (Unknown)  
URL: <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmmr/htm/understandingthesecureaudiopathmodel.asp> (2003-08-25)
25. Murdoch Mactaggart, Introduction to cryptography (Mar, 2001)  
URL: <http://www.mjidor.com/introcrypt1.shtml> (2003-08-21)
26. Spencer Cheng, Paul Litva, Alec Main, Trusting DRM Software (Jan 2001)  
URL: <http://www.w3.org/2000/12/drm-ws/pp/cloakware.html> (2003-08-21)
27. U.S. Copyright Office, Copyright Basics (Sep, 2000)  
URL: <http://www.copyright.gov/circs/circ1.html> (2003-08-21)
28. Xbox Linux Project. (2003)  
URL: <http://xbox-linux.sourceforge.net> (2003-08-21)
29. Xbox Media Player. (Unknown)  
URL: [http://www.xboxmediaplayer.de/newweb/info\\_project.htm](http://www.xboxmediaplayer.de/newweb/info_project.htm) (2003-08-21)

## På svenska

Detta dokument hålls tillgängligt på Internet – eller dess framtida ersättare – under en längre tid från publiceringsdatum under förutsättning att inga extra-ordinära omständigheter uppstår.

Tillgång till dokumentet innebär tillstånd för var och en att läsa, ladda ner, skriva ut enstaka kopior för enskilt bruk och att använda det oförändrat för ickekommersiell forskning och för undervisning. Överföring av upphovsrätten vid en senare tidpunkt kan inte upphäva detta tillstånd. All annan användning av dokumentet kräver upphovsmannens medgivande. För att garantera äktheten, säkerheten och tillgängligheten finns det lösningar av teknisk och administrativ art.

Upphovsmannens ideella rätt innefattar rätt att bli nämnd som upphovsman i den omfattning som god sed kräver vid användning av dokumentet på ovan beskrivna sätt samt skydd mot att dokumentet ändras eller presenteras i sådan form eller i sådant sammanhang som är kränkande för upphovsmannens litterära eller konstnärliga anseende eller egenart.

För ytterligare information om Linköping University Electronic Press se förlagets hemsida <http://www.ep.liu.se/>

## In English

The publishers will keep this document online on the Internet - or its possible replacement - for a considerable time from the date of publication barring exceptional circumstances.

The online availability of the document implies a permanent permission for anyone to read, to download, to print out single copies for your own use and to use it unchanged for any non-commercial research and educational purpose. Subsequent transfers of copyright cannot revoke this permission. All other uses of the document are conditional on the consent of the copyright owner. The publisher has taken technical and administrative measures to assure authenticity, security and accessibility.

According to intellectual property law the author has the right to be mentioned when his/her work is accessed as described above and to be protected against infringement.

For additional information about the Linköping University Electronic Press and its procedures for publication and for assurance of document integrity, please refer to its WWW home page: <http://www.ep.liu.se/>