

# Why We May Never Have DRM

Hagai Bar-El  
info@hbarel.com

## Abstract

*Digital Rights Management (DRM) is a concept that receives a lot of attention lately. Content owners are eager to make use of the Internet to distribute their content to larger audiences, with greater ease and with lower costs. However, the digital nature of digital content and the versatility of modern computers allow this content to be copied and otherwise handled in ways the content owner does not approve of. DRM schemes are developed to help content rights owners enforce their policy on content they provide to customers. Yet, these schemes ignore some fundamental properties of the environment their implementations run in which lead to DRM remaining a hopeless battle. This paper describes the fundamental facts that make DRM schemes much harder to implement effectively than it may seem.*

## 1 Introduction

The digital world has discovered the ability to convert almost any content into digital form. Written content is digital by its nature. Printed letters and digits are easily converted into computer files. Other content such as music and video is analog in nature, but can easily be converted into digital form and newly developed compression algorithms have made the digital representation take reasonable amounts of storage space making it completely feasible to store such content on common means for digital storage, such as hard-disks, CD-ROMs, flash memory cards, etc.

When content is digital, it can be handled by computers. It can be stored on computer media, it can be accessed (played and managed) by computer software and it can be sent from one place to another (hence, distributed) using computer communication methods, such as long-distance network connections as well as proximity connections such as USB cables. The ability to handle formerly analog content with the same ease of handling other digital content has made digital distribution of content very appealing. Content owners like the idea of selling songs

and movies online without the cost of burning it on storage media and without the burden of shipping it by physical means. Similarly, end users of content like the ability to store content on their PCs, and to transfer content from one user to another easily, even across continents.

The only problem left unsolved is protecting the rights on the content owners. The ability to copy content freely and distribute it freely causes extreme damage to the business model content owners rely on. By the common business model, content owners get a large part of their total revenue from selling copies of the content. The ability to copy content freely and to send it freely, not just from one user to his friend, but also among groups that span millions of users who have nothing in common other than the will to share the content they possess, cuts the financial branch that the content rights owners sit on.

After realizing the problem, the first thought that comes to mind is to expect technology to solve the problem that technology “caused”. Mechanisms were and are developed to allow the legal owners of rights on content to define and enforce policy regarding the content they own. Of course, the first right that needs to be controlled is the right to copy the content.

Several schemes have been designed to protect content from being copied or otherwise “misused”. Some schemes were already proven non-effective<sup>1</sup> whereas some were not yet adopted in a scale large enough so their strength can be assessed.

This paper will present some fundamental facts of computer science that may make the reader realize that effective DRM schemes are very hard to design; if not impossible.

---

<sup>1</sup> The best example is the CSS mechanism for protecting content stored on DVDs. The scheme was broken shortly after it was introduced. The scheme was broken by a teenager who presumably had no malicious intent.

## 2 Content is Bits

This title is not surprising. By the nature of digital content, it is represented as a set of bits. Bits are information. Bits are not the physical media that stores them, neither are they the wire transferring them. Bits are information, facts of knowledge, and knowledge by its nature can be duplicated (given away without affecting the original) by anyone having it. Anyone who has a set of bits can duplicate them at will and pass this knowledge on.

The statement seems trivial, and it is, but understanding this statement leads to understanding that any way for protecting digital content must always rely on blocking the consumer of the knowledge from actually having that same knowledge. In other words, any DRM system must be based on making the bits of content unknown to the legitimate user consuming the content. This is as opposed to most other security systems in which the user of information who has the right to use it also has complete knowledge (possession) of it. For example: a legitimate reader of an encrypted file can see (know) the decrypted file after decrypting it. Since having information means being able to duplicate it, all DRM schemes must be based on the requirement that the user is prevented from having access to the information he consumes.

The abovementioned limitation has further implications. How can a system prevent a user from possessing information that needs to be passed to him for consumption? The only known way to effectively restrict access to information that is communicated through un-trusted channels is by the use of encryption. Encryption uses keys. Every piece of encrypted information is encrypted using a key and has a similar or matching key for decryption. Since the algorithms are known (or can be reverse-engineered) knowledge of the keys used for decrypting data equals to having that data. These facts lead to the requirement by which the legitimate user of content must not possess the keys that are used to decrypt the content. This is in contrast to most other applications of cryptography where the legitimate owner of data also possesses the key that is used to decrypt it.

The picture should be clear now. The legitimate consumer of content must not be able to access the content he consumes directly and therefore shall have no access to the keys used to decrypt that content. This is in spite of the fact that decryption is performed on his computer (or device) while he consumes the content.

## 3 Control Over the System

After reading chapter 2 it shall be obvious to the reader that a consumer must not be able to access all the components of a DRM system, not even the ones stored on devices he possesses. In particular, the user may not access the keys used for decryption of content, and of course, he may not access the decrypted content other than by consuming (reading, listening or viewing) it.

### 3.1 Control Over Hardware

When playback modules are implemented in hardware (DVD players, MP3 players, CD players, etc.) hiding data-components from the legitimate user is relatively easy. Keys that are stored in cryptographic modules are hard to access for an occasional user. Even against more dedicated violators tamper resistance measures can be employed to protect the hardware module from being probed. However, how reliable can this protection be? Keys stored in cryptographic engines can easily be protected by tamper resistant hardware modules. Still, the decrypted content cannot be consumed while residing in the cryptographic engine. The decrypted content has to leave the engine at some point at which it also leaves the physical area protected by tamper resistance. When the decrypted content is out, it can be probed with ease.

Complete tamper protection for the entire playback device is not always feasible, and even when it is, it usually incurs an extra cost that most consumers will not tolerate.

### 3.2 Control Over Software

Controlling the access of a user to software components installed on her machine is known to be a lost battle. Software copy protection is a field that has progressed very little in terms of real achievements during the decades for which it exists. It is a known fact that today software vendors are aware that there is no effective way to halt users from making illegal copies of software, and therefore find other solutions to assure their revenue, such as selling services and support and fighting copyright offenders after the act.

As long as computers are versatile and flexible and as long as they are controlled (on the lowest layers) by their owners, there is no way to hide secrets (such as keys) within the computers in-

ternals from their owners. Computers do not have secret hiding places. All information that is permanently stored within them is stored either in some sort of non-volatile memory or on the hard-disk. Data can, of course, be encrypted, but encryption must be done using some key that is available within the machine for decryption.

A few initiatives have emerged such as TCPA and Palladium, which attempt to add secure storage and a secure processing environment to common PCs. These, however, are based on hardware components that are tamper resistant (to some extent) and that cannot be accessed by the owner of the computer, practically redefining the term of complete ownership and causing debates concerning privacy and liberty issues.

## 4 Attack Scalability

So far we have seen that hiding bits from their legitimate user poses a hard problem on both hardware-based and software-based implementations, no matter what the exact DRM scheme is. However, it can be reasonably claimed that as long as attacks on schemes are more expensive than the content the schemes are protecting, they do not pose a significant threat. This claim is reasonable and it is commonly raised for many security countermeasures in all fields. Almost every security mechanism can be circumvented by this or that way if enough time, money and efforts are invested in the circumvention. However, as long as the cost of the attack is higher than the gain achieved by circumventing the system, the protection mechanisms are considered effective.

In the DRM context it is obvious that if making an illegal copy of a song requires even the minimal hardware probing, possibly damaging the device, it will simply not be worth the \$5 that can otherwise be paid for purchasing that song legally.

Moreover, if a certain attack on a DRM system is possible and will yield a single skillful and dedicated attacker the ability to play any content forever, the DRM industry still has no interest in preventing this attack. As far as the industry is concerned, he can enjoy the illegal content as much as he likes because modifying the scheme, possibly increasing its total cost, is much more expensive than the damage caused by a single individual not making any legal purchases in his lifetime. This is, of course, assuming that the skill and dedication needed to break the system is such that only a minor part of the population has such skill. Generally, attacks that

result in a single piece, or many pieces, of content stolen by skillful adversaries do not bother the DRM industry.

The attacks that are worth consideration are attacks that cause “real” monetary loss and these are attacks that are easily scalable. When thinking of scalable attacks, four types of attacks come to mind. The first three types are ones in which the attacker easily distributes his knowledge to the public (in some form) and the fourth type is one in which the attacker takes content out of the DRM system.

### 4.1 Distributing the Knowledge

The first type of attacks consists of attacks that can be easily duplicated by cheap hardware modules. If, for example, an attack allows the attacker to produce low-cost cards that, when inserted into a pay-TV or a playback device, allow the user to play content for free, the industry is in problem. The circumvention device will be sold in the black market and the industry is to suffer significant damage. An example of such attacks are PayTV cards and terminals that allow their owner to view TV channels he did not subscribe to (and therefore does not pay for).

The second type of attack is related to the first type and consists of attacks that can result in a software circumvention program. If an attacker finds the location of the secret DRM key on a PC and reads it, he can easily write a short program that does the same thing and post it on the Internet. The damage to the industry in this case is even larger as software is distributed faster and for free. Software *cracks* are the best example. A *crack* is a small executable that, when run, disables the protection mechanism of a given program it was designed to work on. Hacker sites are full of such cracks that disable trial and demo version restrictions on many commercial applications.

The third type of attack consists of attacks in which the circumvention implementation is so trivial that it can be followed by the public if only knowledge is available. The attacker in this case only has to type in the circumvention method as an easy to read text file, and post it for the public to read and follow. The best example for this type of attack involves a technology recently invented to protect audio CDs from being played and “ripped” into MP3 files by PCs. The protection method was based on an unreadable track at the beginning of the CD that causes PCs that read it to not recognize that it

is an audio CD and therefore to not read it properly. Unfortunately, it was soon discovered that this protection method can be circumvented easily by painting a part of the CD with a black marker. Of course, from the day this simple attack was discovered and posted on the web, using the protection technique became useless.

## 4.2 Liberating Content

The forth type of attack contains attacks that result in content being spilled out of the DRM system. DRM is a set of mechanisms that are added to otherwise freely accessible content. If an attack leads to the content being extracted from its DRM protection it can be said that this content is “lost forever” in terms of DRM as it can be freely distributed by the mechanisms available today for distributing digital content.

If an attacker obtains the original bit stream of the content (such as by accessing the original bit-stream after it is decrypted by the DRM module), he can easily store it in plain format and distribute it. If enough content is available freely then the DRM mechanisms can no longer protect the financial model of the content rights owners.

There are mechanisms such as *watermarking* that allow plain content to be recognized even after it is not protected or encrypted. However, these mechanisms merely give indication of stolen content after the fact and do not actually protect the content from being used by non-compliant devices. Compliant devices may refuse to play content that is watermarked and unprotected, but pirated software will still play it gladly.

To summarize this point: the first time content is exposed as raw bits, it is lost in DRM terms. This unprotected content will be circulated by peer-to-peer networks (as all content is today) and will seldom be legally purchased.

## 5 Analog Conversion

So far, all the attacks discussed require the attacker to have some technical skill in tampering with the DRM mechanisms. Every circumvention technique that was covered by the discussion so far required some sort of attack on the system. However, even in the worst case scenario (in terms of the adversary) in which he cannot find a way to get a hold of the decrypted content, there is always the last resort of making

a digital-to-analog-to-digital conversion. This can be easily shown in the digital music case.

Music is stored in a digital format. However, let us remember that it is not yet consumed in a digital format. No matter what DRM mechanism protects a song, this song will always end up being played as analog audio by analog amplifiers connected to analog earphones or speakers. The song can be captured in its audio form, re-sampled and re-digitized into a new plain MP3 music file. Tools for encoding high quality MP3 files out of standard analog audio are freely available and run on common hardware. Once a new music file has been generated, without involving any DRM scheme, the content can be treated as taken out of the DRM system (see chapter 4.2).

One may always claim that the analog conversion degrades quality, which is true. The biggest advantage (or disadvantage?) of digital content over analog content is that it retains its original quality even after an infinite number of recording generations, as opposed to analog content that usually reaches an unacceptable quality after just several recording generations. However, this drawback of analog content might not apply here due to the fact that the content is passed through an analog processing stage only once.

When a piece of music is played and re-digitized, the analog processing is actually performed just once and further duplications of the content are done digitally using the non-protected file that was generated. A single digital-analog-digital conversion will not introduce enough of a degradation to the sound quality to discourage users from using it. A search of peer-to-peer networks will show that most of the MP3 files that are being circulated are not of the highest possible sampling-rates and consumers still download and play them happily. Assuming that DRM-protected purchased content will be of one of the highest possible qualities, the resulting unprotected file, after going through the above-mentioned analog stage, will still be of a quality that is higher than of most files on the net.

As mentioned in chapter 4.2, watermarking can be used to detect stolen content even after it went through such conversion. However, even if the watermarking scheme is never broken and cannot be circumvented, it is still a “know-only” method that has absolutely no significance unless the player of the file cooperates and refuses to play marked content.

## 6 Summary

DRM schemes are an attempt of technology to solve a business problem, ignoring fundamental properties of today's digital world. Had computers not been so versatile the problem would not have risen, but then PCs wouldn't have been so appealing as players and as distribution tools for digital content from the start.

The starting point that all DRM schemes are and will always be based on is that bits of data must and can actually be concealed from the legitimate user who consumes the data. This is a requirement that is very hard to meet. More precisely, this requirement is impossible to follow completely and very hard to follow reasonably. Software will always be reverse-engineered, hardware will always be reverse-engineered, plain data will always have to travel through unprotected pipes at some stage of the playback process, and even if the data cannot be captured in its digital form, it can surely be captured in its analog form and re-digitized.

Software is impossible to protect on multi-purpose computers, and hardware is very hard to protect, especially considering the pricing constraints on such appliances. Hardware tamper-resistant modules are the basis for the best implementations of DRM. Still, when attacks are so scalable that a single broken device can lead to vast amounts of pirated content it is only a matter of time until we return to the point in which most content is circulating on the Internet in an unprotected form.

## Acknowledgements

The author wishes to thank Josh Patt for revising the new version of this document.