University of Auckland, Faculty of Science

Department of Computer Science

COMPSCI 725 – Software Security

Term Paper

2003

Hardware-Based Methods for Prevention of Multimedia Piracy: Some Issues

Iain Phillips

Iain Phillips
2498009

8/08/03

Abstract

The advent of digital music and video formats has enabled media piracy on an unprecedented scale. This is a cause for concern to their respective industries. Many methods have been proposed for Digital Rights Management (DRM) in order to combat this problem. Some of the most promising of these are hardware-based methods utilising watermarking or fingerprinting.

This paper outlines several such methods. The phenomenon of 'leakage' is identified as the primary concern. Two possible implementations are presented, and the issues associated with them discussed. This includes the robustness of watermarking schemes, and the feasibility of deploying a hardware-based solution on a large scale. Alternate approaches are identified.

It is concluded that there is some way to come before a complete Digital Rights Management system is achievable.

Iain Phillips
2498009

8/08/03

Originality Declaration

This paper is my own unaided work and was not copied from nor written in collaboration with any other person.

Iain Phillips
8 August 2003

Table of Contents

1. Introduction

Even before the introduction and widespread usage of digital formats for multimedia such as books, music, and video, piracy was a present concern for their creators. Since as early as the 18th Century the debate over copyright, and the technologies which help us to infringe, has raged. Every new technology that is developed brings with it concerns about its uses. Even the invention of the printing press generated much debate as to the future profitability of writing books. Similarly it was thought that the photocopier would forever render paperback publishers out of business [1]. Not so.

Yet no development has generated quite as much concern as the advent of digital multimedia. This is primarily because whereas prior methods of copying would always entail a loss in quality, digital multimedia can be reproduced exactly. It can also be transmitted rapidly around the world at very little cost.

Content providers claim that they are suffering huge losses from illegal copying. Internet music piracy alone is estimated to cost the music industry a billion US dollars a year [2]. Obviously this is very hard to quantify exactly because it cannot be simply assumed that every person who illegally accesses material they didn't pay for would otherwise be a paying customer. Some people claim that piracy is actually beneficial to the industry because it provides greater exposure to potential customers, who will buy an album they like. However for the purposes of this paper it is assumed that piracy is a problem and that potential solutions will benefit both producers and consumers in the long term.

James Burger et al. (2000) [2] state that content publishers have three options for fighting this problem:

1. seek for legal ways to enforce their copyright;
2. change their business model e.g., by collecting revenues through advertisement rather than music sales, and/or;
3. research new technologies that will raise effective barriers for illegitimate use of digital content.

Many forms of these counter-measures to the piracy problem have been tried. None have been particularly successful. For example the makers of the popular Internet file-sharing software

Napster were forced to prevent illegal sharing of music by court order. However this has simply caused the majority of users to switch to other file-sharing programs such as iMesh, which has no centralised server and hence cannot be easily shut down.

Advertising based services have faced considerable consumer resistance and struggled to generate sufficient revenue to survive.

Technological solutions have also had little success, partly due to poor design, and disagreement among different industry players. For example the Secure Digital Music Initiative (SDMI) has recently put its program on hold due lack of "consensus for adoption of any combination of the proposed technologies." [3] It intends to re-assess technological advances at some later date. The Content Scrambling System (CSS) designed for Digital Versatile Disks (DVDs) has been broken by a group of Norwegian hackers. This was due to a weakness in the design, which has only one secret key for each zone. [4]

However there is a lot of research in this third area, and some emerging technologies look very promising. One such solution is the use of watermarking to give every file a unique signature that can prove its ownership. Additionally, some potential solutions propose the use of tamper-resistant hardware and encrypted content. This paper reviews some proposals for such systems. Two of the most promising, by Schneck [5], and Bao [6], are critically considered.

2. Proposed Solutions

Many authors have offered ideas to help combat multimedia piracy. While most traditional approaches have been targeted at preventing the copying of media, it is now widely accepted that such approaches will only work short term, as techniques are inevitably developed to overcome the copy protection. Furthermore, there is no legal reason to prevent the development of such techniques, as it is considered 'fair-use' to make a copy of a work you own for your purposes (under US copyright law at least).

In order to provide an effective measure against piracy long-term, a system is needed that will allow copying but ensure that the users pay the appropriate royalties. Such systems have come to be known as Digital Rights Management (DRM) systems. Ideally, such a system would be simply a technological means of enforcing the rights of artists and consumers, as established by copyright law [7] [8]. For example the authors would be granted a limited monopoly over their work for a set time period, and then it would become freely available. They would receive fair compensation for their efforts during that time.

Arguably, no currently deployed system achieves this ideal. Designs for complete DRM systems take many forms, utilising a wide range of technologies. Almost all involve a change in the way we think about using digital content.

For example Timothy Budd (2001) [1] proposed a scheme in which the use of digital media is controlled by a hardware device known as a ‘Digital Battery’. This battery is analogous to a real battery in that it has a limited lifetime and is essential to the operation of the device. The idea is that a user would purchase a digital battery from a convenience store for a small price, and this battery would enable them to playback/view encrypted digital content. Furthermore, the battery would store a record of what content has been accessed, and when it is returned for recharging the royalties from the sale of the battery could be distributed appropriately.

Budd’s proposal introduces a major paradigm change for consumers. No longer would it be possible to buy an album or ‘own’ a book written by someone else. Instead users would pay a small fee every time that they listened to a song, or read a book. Budd does not examine the feasibility of such a major paradigm change, which may not be rapidly adopted by consumers. However, such a scheme could be successful if cleverly marketed. Importantly, the paradigm shift required resembles the modern view artistic works as Intellectual Property, which certainly cannot be owned by anyone other than the author (although the rights to it may be sold).

The paper does not give much detail as to the specific technologies that could be used to implement the digital battery, but a possible approach is suggested by Rivest and Shamir (2001) [9]. Their ‘PayWord’ and ‘MicroMint’ schemes are a practical smart-card implementation of a pay-as-you-access system. However their schemes are primarily targeted at content that has a short lifetime, such as daily newspapers, and does not address the problem of users retransmitting decrypted content. This is a major oversight, as all it takes is one user to post an unprotected copy of a file on the Internet for it to render all protected versions of the file worthless.

This problem is known as leakage, and is the main reason that DRM systems have had little success to date. The difficulty with media (as opposed to software) is that at some point it must be decrypted and available to the user. If the user has little concern for the publishers of the content, there is nothing to prevent them sharing the decrypted content with whomever they wish.

There exist at least two potential ways of controlling leakage; watermarking and fingerprinting. These terms are often used interchangeably, but may be defined as follows. Watermarking is the imperceptible embedding of information into an image or song that can prove its authorship. For example a unique string could be embedded using an authors private key and only be revealed by using their public key. It should not be possible to remove or alter the watermark without also destroying the content. Fingerprinting on the other hand embeds information about the intended recipient of the file, so that leaked content can be traced back to the person who leaked it. This requires every user to have a uniquely fingerprinted copy.

The following sections examine two proposed DRM systems. The first, by Dr Paul Schneck, uses watermarking to address leakage. The other, by Feng Bao, uses fingerprinting.

2.1. A Watermark Based DRM System

In his paper *Persistent Access Control to Prevent Piracy of Digital Information*, [5] Schneck proposes a DRM system based on tamperproof hardware and watermarking techniques.

This system manages leakage by ensuring that media can only be accessed by approved hardware, which will not allow the user to retransmit it. The output is in the form of an analogue waveform (for music), which can theoretically be re-recorded and distributed, but will entail the same loss of quality as current analogue copying. Schneck points out that this is similar to the strategy used by pay television services, where the set-top box is tamperproof and will cease to function if any attempt is made to open it and get at the secret key or a digital signal.

Figure 2-1 illustrates the functionality of this system. It relies heavily on the hardware device being tamperproof. Schneck clearly defines such devices, which include a tamper-detecting enclosure, protected storage, and encrypted I/O. Any physical attack on the device will destroy the private key and render it useless, and there is no way to discover the private key from external analysis. Such devices have been used successfully for at least a decade.

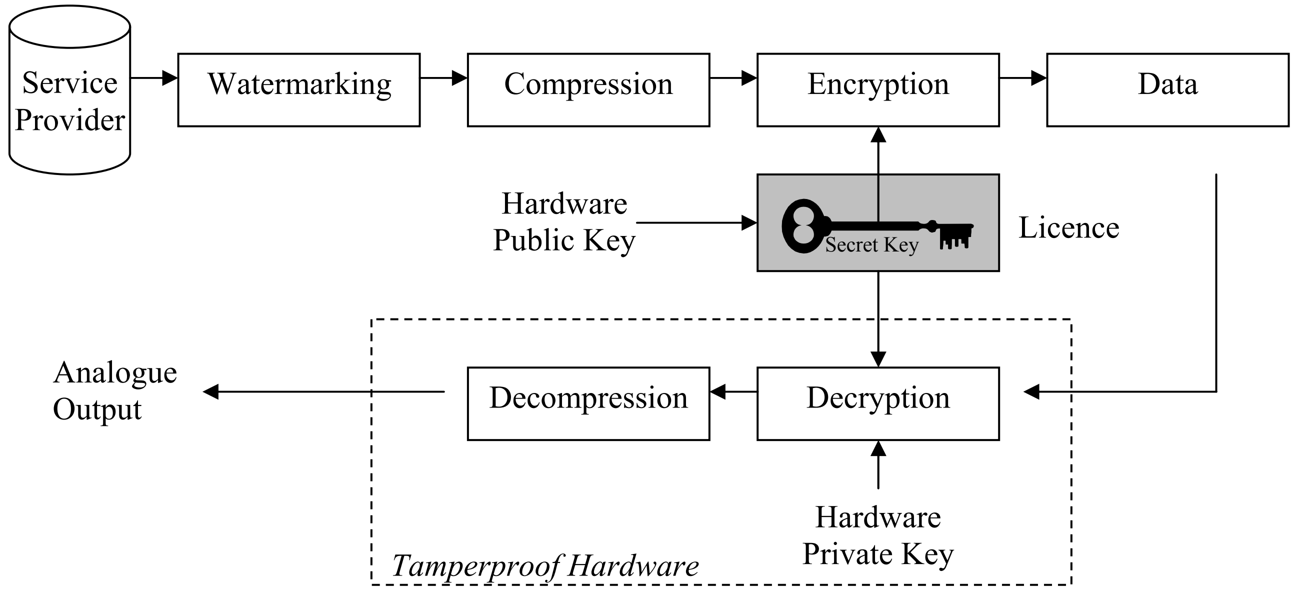

Figure 2-1 A block diagram of Schneck's DRM System. Redrawn from 'Fig. 1. Analog waveform data delivery' in his paper [5].

An important aspect of this system is that data can be freely distributed by any means. For example music could be sold on a CD, downloaded from the Internet, shared between friends, etc. As it is encrypted this is not a problem. It can only be listened to or viewed on trusted hardware with the appropriate licence. A licence to access a particular file would be obtained from the producer. This could be purchased over the Internet, or sold with the CD. The licence contains the secret key needed to decode the file, but is also encrypted using the public key of the hardware device it is intended for, so a licence can only be used for a specific hardware device.

Since each individual song, picture, or page is encrypted with a different secret key, it is not susceptible to a brute force attack. Any key that is broken will only compromise one file.

The importance of watermarking here is to provide proof of authorship. Since an author will receive their income from selling licences to their content, it is important to ensure that someone cannot profit from selling licences for cheap imitations. The use of a watermark enables the consumer to be sure that their money is going to the true author.

Since the system uses special hardware, it can support many other features. For example licences could specify the exact permissions a user has, e.g. to print or copy the file. They could also specify a set number of accesses, or expire after a set time. Interestingly, this method could work with

Budd's idea of a pay-as-you-access system, although obtaining a new licence every time you wanted to access a file would be cumbersome.

Another interesting aspect of this system is that it could be made to comply with the limited monopoly provided by copyright law. When the copyright period has expired the authorities could simply publish the secret key of the file concerned, and it would immediately become freely available to anyone.

Multimedia content is only one of the many applications Schneck suggests for his scheme. He claims it could also be used for software, databases, and generic computer files, although it is unclear how watermarking could be used with data which has such a low tolerance for error.

2.2. A Fingerprint Based DRM System

Feng Bao [6] proposes a system specific to multimedia content. It is similar in many ways to that proposed by Schneck, but has some distinct advantages.

The main difference is that instead of relying on an analogue output from trusted hardware to prevent leakage, fingerprinting is used to deter users from sharing their files. This is illustrated in Figure 2-2 below.

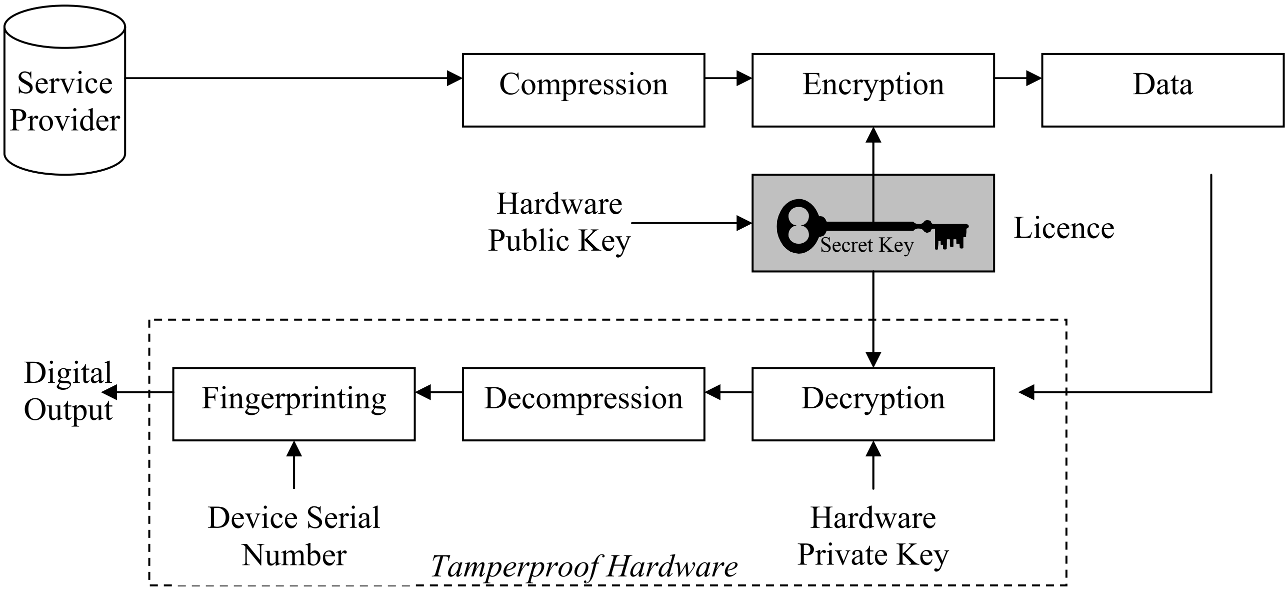

Figure 2-2 An interpretation of Bao's DRM System; drawn to illustrate the similarities to Schneck.

Every file that a user accesses will be fingerprinted with the serial number of their device. If they share the file with other users they risk their hardware being identified as the source. The licensing authority will then refuse to sell them any further licences. This may not prevent small scale sharing of files between friends, but will put a definite end to large scale anonymous trading of files via the Internet.

Bao suggests that a separate licensing authority be established, rather than content publishers selling licences directly. This is because of the importance of checking that each public key used to request a licence belongs to a valid hardware device. Failure to do this could result in a user requesting a licence with a public key that they know the private key for, and using this to obtain the secret key. In addition, the licensing authority would actively search for leaked files and maintain a hardware revocation list. In exchange for this service they would take a cut of the profit from licence sales.

Bao's proposal does not address the proof of authorship problem which Schneck tackles with his use of watermarking. It may be possible to combine these proposals to create an ever better system. However the use of both watermarking and fingerprinting may be difficult, as one may effect the other, and there is a limit as to how much information can be hidden in a single file.

3. Issues

Both of the solutions covered in the previous section are well thought out and have many merits. They present two interesting responses to the difficult problem of leakage. However they both depend on the robustness of fingerprinting/watermarking technologies, and the issuing of licences. These areas may present some problems. Furthermore, since they depend on the use of unique hardware, they are completely incompatible with any existing systems.

3.1. Watermark / Fingerprint Robustness

Neither author discusses this in much detail, assuming that such technologies will soon be sufficiently developed. This may be valid, however no one technique has yet emerged (three years later) as a clear leader in the field.

The difficulty arises because watermarking generally makes use of inaudible parts of sound waveforms, so as not to distort quality. However, advanced compression technologies such as mp3 discard these same areas, destroying the watermark. Progress has been made, however, and groups such as Blue Spike [10] claim to have working watermarking systems. Unfortunately they do not provide details as to what kinds of compression and format conversion the watermark can withstand.

In the absence of a robust fingerprinting scheme, Schneck's proposal is the most practical, as destruction of a watermark will not provide any gain for the attacker, provided they cannot masquerade as the author of stolen content.

3.2. Licence Mobility

Both Schneck and Bao use asymmetric encryption to encrypt a licence so that only one specific hardware device can use it. This assumes that each user will only have one device they wish to use. However, must customers will have a living room stereo, a car CD player, a computer, and possibly a Walkman. No provision is made for the ability to use one licence on multiple devices, and yet without it consumers are very unlikely to adopt the technology.

A possible solution is to put the complete tamperproof hardware system onto a smart-card. This would contain the private key, and could be used with any device, but only one at a time. Licences would be stored in the memory of the smart-card so that they are also portable from one device to another. However this introduces another problem with Schneck's proposal. Since the smart-card would also have to contain an analog-to-digital converter, the sound quality of the system would be a function of the smart-card, not the sound system. This would be unacceptable to users of high quality equipment.

3.3. Hardware Deployment

A further issue is that both schemes utilise tamperproof hardware devices. In order for consumers to access files protected with either system, they will have to own the appropriate device. This entails an enormous roll-out of hardware, and produces a chicken or egg problem: consumers will not buy devices there are no content for, but producers will not produce content there is no market for. In order to successfully implement such a solution, the devices must be 'backwards compatible' with existing media formats, and offer sufficient features for consumers to buy them on merit. This requires considerable collaboration between the music industry and the hardware manufacturers, which has traditionally been poor.

4. Alternate Approaches

Given the issues identified in the previous section, it may be some time before a suitable Digital Rights Management system is deployed. In the mean time, there are some possible ways of minimising the impact of multimedia piracy.

The primary way to achieve this is to enhance the media in ways that cannot be easily reproduced. This will encourage consumers to purchase a legitimate copy, in order to access the enhanced features. For example music could be sold on DVD and include music videos and extended footage of the band. DVD recorders are still very expensive and sparse, so illegal copying would be dramatically reduced.

Another idea is to create a service that produces customised CDs cheaply and more easily than customers could by themselves. A client could select from a wide range of songs, pay the appropriate royalties, and receive a CD burnt professionally, along with artwork and lyrics from the original albums. This provides additional value over a homemade compilation CD, avoids paying download fees, and provides a sense of legitimacy.

These approaches do not in any way prevent piracy in its current form. They do however provide incentives for users to buy original content. In the long term, a DRM system should still be pursued.

5. Conclusion

In the digital era, multimedia piracy has become a problem of enormous scale. Much effort has been put into developing ways to deal with this problem. This includes legal methods, changing the business model, and technological approaches known as Digital Rights Management systems.

The biggest challenge with technological methods is preventing 'leakage', or illegal redistribution of unencrypted music. Many proposals have used watermarking and fingerprinting techniques to combat this. The schemes presented by Schneck and Budd are promising examples.

Both of these schemes use tamperproof hardware. Content is distributed in encrypted form and users must obtain a license in order to view or play it on their hardware. Leakage is controlled by either providing an analogue output only, or by fingerprinting the output with the serial number of the hardware used to play it.

Despite many good features of the schemes, there are some serious issues. These include the robustness of current techniques for watermarking/fingerprinting, and the difficulty of deploying hardware based solutions on a large scale. Portability of licences is also a potential issue, however this may be resolved if the entire hardware unit can be made to fit on a smart-card.

These issues make it unlikely that any DRM system will be deployed until the supporting technologies are further advanced. To slow the growth of piracy in the interim, alternate approaches must be examined. These include the possibility of enhancing the content to discourage reproduction, and providing value-added services, making it easier not to pirate.

Many authors have stated that no matter what technologies are developed, piracy will be an ongoing battle. This is no doubt true. However hopefully the development of a robust DRM system will someday help to reverse the tide of piracy brought on by the digital revolution.

References

[1] Budd, T. “Protecting and Managing Electronic Content with a Digital Battery” *IEEE Computer* pp2-8, August 2001

[2] Burger, J.M. et al “Multimedia Copyright Enforcement on the Internet” *Proceedings of the eighth ACM international conference on Multimedia* pp347-349, 2000, California, United States

[3] “The Secure Digital Music Initiative: Current Status” Available: http://www.sdmi.org 31/5/03

[4] Yu, H., Kundur, D., and Lin, C. “Spies, Thieves, and Lies: The Battle for Multimedia in the Digital Era” *IEEE Multimedia*, v8 i3 pp8-12, Jul-Sep 2001

[5] Schneck, P.B. “Persistent Access Control to Prevent Piracy of Digital Information” *Proceedings of the IEEE*, v87 i7, pp1239-1250, Jul 1999

[6] Bao, F. “Multimedia Content Protection by Cryptography and Watermarking in Tamper-Resistant Hardware” *Proceedings of the 2000 ACM workshops on Multimedia* pp139-142, 2000, California, United States

[7] Samuelson, P. “DRM {and, or, vs.} the Law” *Communications of the ACM* v46 n4, pp41-45, 2003

[8] Davis, R. “The Digital Dilemma” *Communications of the ACM*, v44 n2, pp77-83, 2001

[9] Rivest, R. and Shamir, A. “PayWord and MicroMint: Two Simple Micropayment Schemes” *Technical Report*, MIT Laboratory for Computer Science, April 2001

[10] “Giovanni Digital Watermarking Suite” Available: http://www.bluespike.com/giovanni.html 2/6/03