If Piracy is the Problem, Is DRM the Answer?

Stuart Haber, Bill Horne, Joe Pato, Tomas Sander,
Robert Endre Tarjan
Trusted Systems Laboratory
HP Laboratories Cambridge
HPL-2003-110
May 27th , 2003*

security, content protection, digital rights management, trust, privacy, piracy

Piracy of digital content is considered a serious problem by content companies. Digital Rights Management is considered a potential solution to this problem. In this paper we study to what degree DRM can live up to this expectation. We conclude that given the current and foreseeable state of technology the content protection features of DRM are not effective at combating piracy. The key problem is that even if only a small fraction of users are able to get content from a protected form into an unprotected form, then illegitimate distribution networks are likely to make that content available ubiquitously. One possible technological solution to the problem is what we call "draconian DRM," which involves deploying devices that only process managed content. However, we find that such systems face significant, if not insurmountable, obstacles to deployment and we believe that the real solution to the piracy problem is largely non-technical. The most effective way for interested parties to defeat piracy may be to compete with it.

* Internal Accession Date Only Approved for External Publication
To be published as a chapter in Digital Rights Management: Technological, Economic, Legal and Political Aspects, ed. Eberhard Becker, Willms Buhse, Dirk Günnewig, Niels Rump, Springer-Verlag, 2003

If Piracy is the Problem, Is DRM the Answer? [1]

Stuart Haber, Bill Horne, Joe Pato, Tomas Sander, Robert Endre Tarjan

Hewlett-Packard Company

1 Summary

Piracy of digital content is considered a serious problem by content companies. Digital Rights Management is considered a potential solution to this problem. In this paper we study to what degree DRM can live up to this expectation. We conclude that given the current and foreseeable state of technology the content protection features of DRM are not effective at combating piracy.

The key problem is that if even a small fraction of users are able to transform content from a protected to an unprotected form, then illegitimate distribution networks are likely to make that content available ubiquitously.

One possible technological solution to the problem is what we call "draconian DRM", which involves deploying devices that only process managed content. However, we find that such systems face significant, if not insurmountable, obstacles to deployment and we believe that the real solution to the piracy problem is largely non-technical. The most effective way for interested parties to defeat piracy may be to compete with it.

Our paper is closely related to the recent paper by Biddle, et al., "The Darknet and the Future of Content Protection" [2]. Instead of focusing on the distribution network, however, we describe in more depth how DRM systems attempt to deal with various aspects of piracy, and how they fail.

2 Piracy

Piracy is the unauthorized use or reproduction of music, movies, books, and other types of content that are granted protection under copyright law. This kind of protection typically gives the owner of the content the exclusive right to perform certain actions on the content or to authorize others to do so. We recognize that determining whether an action is authorized or unauthorized may require protracted and subtle debate and that reasonable people may differ in their assessment of a given situation. For the purposes of this paper, however, we do not further address these subtleties for no matter how broadly or narrowly we construe piracy, we reach the same conclusion with regard to the effectiveness of DRM technologies in combating its effect.

---

[1] This article will appear as a chapter in *Digital Rights Management: Technological, Economic, Legal and Political Aspects*, ed. Eberhard Becker, Willms Buhse, Dirk Günnewig, Niels Rump (Springer-Verlag, 2003). The opinions expressed in this article reflect solely the view of the authors and are not necessarily the view of HP.

There are many kinds of content that do not qualify for copyright protection because they do not contain any original authorship and are common public property. Even content that does qualify receives protection only for a limited time, after which that work becomes public property. We refer to these types of content, which are not granted copyright protection, as *public content*.

There are generally two ways in which piracy can occur:

- *Unauthorized acquisition*. The form of piracy with which most people are familiar occurs when a consumer obtains copyrighted content illegitimately, for example by unauthorized downloading of content from a peer-to-peer file sharing service such as Napster or Gnutella, or by obtaining illegitimate CDs or DVDs from a street vendor or friend[2].
- *Unauthorized use*. This form of piracy occurs when a consumer obtains a piece of copyrighted content legitimately and then attempts to use it in an unauthorized way.

A fundamental flaw in the debate around DRM is that it is often assumed that a solution to the second problem will solve the first as well. In this paper we explore how various DRM technologies attempt to address these two problems, and to what extent they might succeed.

3 DRM Technologies

The goal of a DRM system is to enforce licenses[3] between a content provider (the licensor) and a consumer (the licensee) that define rules about authorized use of managed content. There are only a limited number of technologies that can be employed to build DRM systems to achieve this goal. These technologies can be broadly categorized as follows.

First, there must be a piece of software or hardware somewhere within the system that evaluates the license against a requested action, determines if that action conforms to the terms of the license, and either allows or blocks that action from occurring.

Second, there must be an *authentication* component to identify the licensee. The licensee could be a human user or a piece of hardware or software.

Third, we need a way to associate licenses with content. When content is associated with a license using some technological means, we say that the content is *managed.*[4] If content does not have a license associated with it, we say it is *unmanaged*. If users can somehow convert a managed piece of content into an unmanaged form, then they can use it in

[2] In these situations it is usually the person doing the distribution that is called the "pirate". Since the number of illegitimate distributions must equal the number of illegitimate consumptions, we focus on the consumer side of piracy.

[3] Also known as *policies* or *digital rights*.

[4] We could have used the term *protected* in this context, but *managed* fits more cleanly as we are making no claims as to the strength of the technological mechanism for linking content with its license.

unlimited ways. In particular, they can share it with other unauthorized users. We call such illegitimately transformed content *dissociated content*.

3.1 General Vulnerabilities

Typically the license-evaluating engine executes on a computing platform that is under the control of the licensee, as opposed to the licensor. Since the licensee can potentially be an adversary, we must rely on the security of the platform to ensure that the content is used in accordance with its associated license. To buttress the security of this platform we may employ tamper-resistant hardware or software components. However, there is no widely deployed trusted platform technology that has sufficient security guarantees, and it is widely accepted within the security community that such platforms can and will be broken by determined adversaries[5].

Without authentication, an attacker could attempt to deceive the license evaluation engine into thinking that a different, authorized user is attempting to use the content. While authentication systems are well understood, they are not infallible, and thus provide another target for circumventing the system. In general, the adversary may attempt to spoof other characteristics that the license evaluation engine uses to make its decision.

In the rest of this section, we discuss how various DRM technologies attempt to bind licenses to content, how those bindings can be broken, and how these technologies attempt to deal with the problem of unauthorized acquisition. The binding can be achieved externally, by cryptographic means, using what may be called "secure container methods"; or internally, as part of the content itself, either by employing watermarking methods as discussed in Section 3.3, or by using an intrinsic property of each piece of content, as with the "fuzzy hashing" technique discussed below.

3.2 Secure Container Methods

Many DRM systems work by distributing and storing content in an encrypted form and protecting it indirectly by managing the keys used to decrypt the content [10]. The license can be associated with the protected content in a variety of ways, for example as a header to the encrypted file. There is typically some attempt to "hide" the decryption keys from the user with tamper-resistant software or hardware methods. We call DRM systems based on this kind of technique *secure container methods.*

[5] Recently much debate has arisen about the role of trusted computing platforms with regard to DRM. Much of this discussion has focused on systems such as those exemplified by the Trusted Computing Group [6] or Microsoft's Palladium architecture, now known as *Next-Generation Secure Computing Base for Windows* (NGSCB) [5]. While these technologies can be used to strengthen the delivery of ordinary DRM capabilities, we do not believe that they are effective in combating piracy. As is argued in section 4 below, even a small number of motivated attackers is sufficient to enable widespread dissemination of content. Both TCPA and NGSCB are designed to be robust against software attacks on the platform, but with a focus on low costs these systems are not designed to withstand motivated physical attacks on the hardware. As a result, content manipulated on these systems can be assumed to be vulnerable to the determined pirate.

Secure container methods have a limited ability to address the piracy problem since they have no mechanisms to prevent unauthorized acquisition. They must rely on some other method to address this aspect of piracy.

Encrypting the content solves some useful problems. In particular, it allows the system to target content towards a specific device or user and prevents eavesdropping by an unauthorized party during transmission. But ultimately, we have only deferred a solution to the primary problem of preventing unauthorized use of content to that of preventing unauthorized use of the key. Consequently, we need some mechanism to manage the key in the sense above of associating it with a license.

Clearly, the licensee must eventually obtain the key to use the content. Once the key is obtained, the security of the system relies entirely on the security of the trusted platform to maintain the binding of key to content. This binding can be broken either by finding the hidden key or by modifying the license evaluation engine to release the content in an unprotected form.

Even without compromising the security of the trusted platform, there is an almost trivial approach to convert managed content to dissociated content. Content must eventually be released in an unprotected form in order for it to be consumed. Music and movies must be converted to sound waves and photons for us to enjoy it. Content can be sampled at those points in the control flow where it is no longer directly associated with a license. This problem is commonly known as *the analog hole*, because these capture points usually occur after the content has been converted from digital to analog form. But the term "analog hole" is overly restrictive, since the problem exists even while the content is still in digital form. For practical purposes, the content is often in an unprotected form in device drivers, memory, or storage long before its digital-to-analog conversion, and so can be easily captured at these points as well. Once again, we must rely on the security of the trusted platform to protect the content at as many of these points as best as we can. But ultimately there are points at which the content can no longer be protected.

3.3 Watermarking

In watermarking a signal is embedded directly into the content; the signal is imperceptible to humans, but can be detected by machines. For the purposes of this discussion, the signal represents the license associated with the content (even though, in many cases where watermarking has been proposed, the "license" is an especially simple one or is a reference to an external license specification).

We do not address here the subject of *fingerprinting*, in which the watermark represents the identity of the licensee and is typically used for forensic purposes.

Watermarking deals with the problem of unauthorized use by detecting watermarks in content and deciding whether or not the content can be used according to the license specified by the watermark. Watermarking deals with unauthorized acquisition by assuming that watermark detectors are ubiquitously embedded into all of the critical points at which content might be used.

To break the binding between the license and the content involves either removing the watermark or making the watermark undetectable. This is typically accomplished by applying basic data transformations to the content; for example, for images these transformations include scaling, cropping, and compression. The very ubiquity of the watermark detectors considerably eases the task of removing a watermark from a piece of content: an attacker can use the detector as part of an algorithm to remove the watermark [7]. The goal of watermarking is to make it difficult to allow these transformations to succeed without causing unacceptable perceptual distortions in the content. In fact, watermarking schemes are usually designed so that the watermarks will survive the conversion from digital to analog form. A scheme that achieved this goal would be useful in facing certain attacks via the analog hole.

Unfortunately, we cannot provide a strong security assessment of watermarking technologies. A fundamental problem with watermarking is that we only have partial theories of human perception (and we are unlikely to find one in the near future as this is an extremely difficult artificial intelligence problem). This is a double edged sword. On the one hand, it is this lack of understanding that gives us the ability to insert watermarks into content in the first place. If we did understand perception we could in principle compress all perceptually equivalent signals to the same value, leaving no bandwidth for watermarks. On the other hand, this lack of understanding means that we can give no strong security guarantees about watermarking because, at best, we must rely on empirical evidence to say that removing a watermark necessarily results in a perceptually degraded signal.

Moreover, it is not clear that any existing watermarking techniques achieve their stated goal. Most of the techniques described in the academic literature just address specific aspects of the watermarking problem, or they have later been shown to be vulnerable to attack [8]. Proprietary algorithms from technology vendors have failed to show robustness in public challenges [3] or have not been widely enough deployed to evaluate their strength.

We believe that, given this state of affairs, we have to make the assumption that watermarking will not provide any significant security in the near future. Although a number of claims for the effectiveness of watermarking have been made so far the technical reality has turned out to be disappointing.

3.4 Fuzzy Hashing

A relatively new alternative to secure containers and watermarking is “fuzzy hashing,” such as the Fraunhofer’s AudioID technology that has been developed recently for audio content[1]. In principle, this kind of technique could be applied to other forms of content such as video. Instead of inserting a signal into the content, as is done with watermarking, the goal of fuzzy hashing is to recognize the content directly. Unlike cryptographic hashing, where the hashes of two different pieces of data are wildly different even if the data differ by only a single bit, fuzzy hashing attempts to compute an identical hash for two pieces of content if they are perceptually equivalent. The hash

value can then be used as a key to query a database for the licensing information associated with a piece of content.

There are two choices for a system architecture using fuzzy hashing. Either the hashes are stored locally with the license evaluation engine, or they are stored remotely on a centralized server. If the hashes are stored locally, the list needs to be continuously updated as new content is created. The storage requirements of such a system could be potentially massive, and the cost of the device might be significant. If the hashes are stored remotely, then it is not clear how to deal with devices that are off-line.

As with watermarking, fuzzy hashing deals with unauthorized acquisition by assuming that fuzzy hash detectors are ubiquitously embedded into all of the critical points at which content might be used.

Fuzzy hashing is also heavily dependent on our understanding of human perception. To break the binding between the license and the content requires modifying the content in some way so that the hash no longer matches the hash stored in the database. Clearly, if we had complete understanding of human perception, this kind of attack would be impossible as we would design the hash functions to account for all perceptually equivalent versions of the content.

The robustness of these technologies is unknown. Public testing is needed to determine whether the algorithms can easily be fooled. Furthermore, a number of systems issues need to be resolved for a reliable infrastructure. Lastly, this technology needs to be very precise, yielding (almost) no false positives, to ensure that personal or business users would not find themselves in the situation that legitimate (public) content is not rendered. Thus, while fuzzy hashing is an interesting technical approach, there are too many unknowns at this time to justify significant hope for a solution in the near future.

4 Ordinary vs. Draconian DRM

We've seen that there are a variety of DRM solutions to deal with the problem of unauthorized use. None of these technologies is perfect, but one might imagine that they could be made secure enough to deter all but the most determined adversaries.

Furthermore, we have seen that watermarking and fuzzy hashing are the only technologies that deal with unauthorized acquisition.[6] They must be deployed ubiquitously in order to be effective. One might imagine that the various stakeholders could come to some agreement on such technology, standardize it, and deploy it so that the vast majority of devices that deal with copyrighted content would implement those technologies.

Would these two steps be enough to stop the problem of piracy? We claim that even given the optimistic hypothesis that the above conditions held, this would have little

[6] Recall the "analog hole". Only watermarking and fuzzy hashing techniques that survive analog rendering and subsequent digital recapture can be effective. Secure container systems render their content in the clear, thereby losing subsequent control of the content.

effect on piracy. The real problem with piracy is that it takes only a small fraction of users who are capable of dissociating licenses from content to make managed content available to a significant fraction of users in unmanaged form.

The key is that even if each user only shares his or her content with a small set of other users, the content can spread throughout the distribution network rather efficiently. Moreover skilled adversaries can turn their attack into a widely distributed tool that others who are less technically sophisticated can use, further increasing the efficiency of illegitimate content dissemination. Either way, once content is dissociated from its license, it can become widely available to all who want it.

This is why the attempts by the media and entertainment industry to shut down illegal file trading systems like Napster and Gnutella are such an important component of the industry's strategy to battle piracy. However, as is well articulated in the Darknet paper, there are a number of technical reasons why this strategy is unlikely to succeed [2].

One of the reasons for this failure is that DRM, as it is ordinarily conceived, requires that devices handle both managed and unmanaged content simultaneously. We call systems built according to this principle *ordinary DRM*.

The only logical alternative is what we call *draconian DRM,* in which devices that handle managed content do not handle unmanaged content at all. Specifically, technology is embedded ubiquitously at key points in the content distribution chain, most notably in rendering devices, so that content cannot be used unless it has an associated license. We assume that licenses are issued by a trusted authority and are hard to forge. This solves the unauthorized acquisition problem since dissociated content will not be played, by definition.

However there are serious problems with draconian DRM. The first major hurdle is that this solution would require a complete replacement of the existing device infrastructure with DRM enabled end devices. For the sake of argument, let us assume that such a system could be agreed upon and built.

A more fundamental problem is how such a system would handle public content. And there is also the problem of how to deal with individually generated content, such as home videos, business correspondence and other such material.

There are two solutions, each with its own set of problems.

- There could be two parallel infrastructures: one that handles managed content and one that handles all other content.
- We could require that all content, whether managed or not, come with a license.

The problem with the first approach is that the parallel infrastructure could, and probably would, be used to support dissociated content. Therefore, the managed infrastructure must offer some value to the consumer that the other infrastructure does not. This may actually be feasible, for example, if the managed infrastructure had better features or

lower cost than the other infrastructure. On the other hand it is not clear that consumers would not want and that infrastructure providers would not enable those same features for unmanaged content as well.

For the second solution, the primary problem is who would issue the licenses to public or individually created content. In one scenario, this could be a centralized institution, or small set of institutions, that are globally trusted by all users. However this raises a number of issues. What should be done with content that is confidential or private? Clearly any such proposal raises a number of fundamental privacy issues. Alternatively, any content capturing device can be certified by a manufacturer and the license for content produced by the device could be certified by the device itself. However, unless playback is limited to that single device, this only delays the problem by one step. How does the recording device reliably distinguish between copyrighted and public or individually created content?

5 Competing with Piracy

Ordinary DRM will not prevent piracy and it is questionable whether or not draconian DRM can be effective either. Legal attacks will probably never make the Darknet completely go away. One might be tempted to toss up one's hands and give up.

But perhaps we should not be so hasty. It is entirely feasible that DRM could at least partially affect piracy. The software industry is currently experiencing a 40% software piracy rate. Nevertheless, the software industry by all accounts appears to be thriving. Media and entertainment companies may face a similar challenge. If piracy could be decreased by just a few percentage points using DRM, then this might translate into millions of dollars of otherwise unrealized revenue.

But DRM does not come without a price. First there is the cost of building, deploying and maintaining a DRM infrastructure, which will eat into whatever unrealized revenues are recovered. Second, as pointed out in [2], DRM protected content is economically less valuable than unprotected content. So deploying DRM will result in fewer sales of legitimate content, which also might offset some of the revenues gained by decreasing piracy. The question is whether or not the benefits of DRM outweigh its costs.

Regardless of whether or not DRM can be effectively used as a risk management component, we believe that content producers must regard themselves as being in competition with the pirates. As expressed by Shapiro and Varian, "The important thing is to *maximize the value* of your intellectual property, not to protect it for the sake of protection" [9].

A historical perspective on adjusting to new technologies is useful. Many content producers reacted with alarm at the emergence of home video recording capabilities, but today video distribution is a significant vehicle for the content distribution industry. This is not an isolated case, in fact, the growth of circulating libraries and of book publishing

in England and the United States in the 18th and 19th centuries is analogous to the case of the video industry [11].

The assertion that content producers might do better by structuring their offerings as subscriptions (or a variation on that model) than according to a pay-per-view model has some backing from an economic analysis by Fishburn, Odlyzko, and Siders [4]. Modeling the situation of competing producers of mass-market information goods, and surveying the history of consumer preferences in several industries, they found that producers could achieve higher revenues through bundling, and that consumers' strong preference for flat rates could stimulate usage.

There are several different ways in which the content and IT industries might extend their offerings to compete with piracy.

- Content management:
  - *Recommendation*: A music-service tool that would offer users recommendations for songs they might enjoy, based on the history of what they have already played, would be a considerable improvement over most current offerings, in which the only way to search for a piece of music that is completely new to you is to browse by genre. Naturally, this would be useful in other media as well as music.
  - *Organization*: Very soon, users are likely to have large personal "libraries" of content that they have accessed. New tools are needed that enable users to organize and manage their content; without such tools, their libraries will be as unwieldy as a disorganized directory of email folders. These tools would be enormously useful for all kinds of content, no matter how the users access the content and no matter where the content itself is stored (locally on a portable device, on a server, etc.).
- Content delivery:
  - *Quality of distribution*: Legitimate content distributors are typically able to offer a higher quality of service than is available in an illegitimate distribution network.
  - *Quality of content*: Content in peer-to-peer networks is often poorly sampled, and there is an emerging threat of viruses and spam. Legitimate content can be authenticated in various ways so that consumers would be assured that they only receive official versions of the content on offer.
  - *Infrastructure*: Content distributors might arrange new partnerships with infrastructure providers, e.g. with mobile phone providers, to ensure cheap and easy access to content. It would be considerably more difficult for pirates to offer such services.
- Business models:
  - As suggested above, there is evidence that producers can profit by introducing alternate methods of charging for access to content, including

subscriptions, bundling techniques, and price-discrimination schemes for access to a piece of content at different times or in different formats.[7]

- In addition to bundling different sorts of offerings of their digital content, providers can link digital content to concert tickets, clothing, club memberships, and other kinds of value-added merchandising.

6 Conclusion

We pointed out that unauthorized use and unauthorized acquisition are two aspects of piracy. A key concept is how licenses are bound to content. We saw that various kinds of DRM technology address these issues in very different ways, but that all of them have some kind of flaw that make it highly unlikely that they will be able to solve the problem of piracy. The real problem with piracy is that it takes only a small fraction of users who are capable of dissociating licenses from content to make managed content available to a significant fraction of users in unmanaged form.

We explored the concept of draconian DRM in which devices that handle managed content do not handle unmanaged content at all. Draconian DRM could potentially be effective at eliminating piracy if it were ubiquitously adopted, but introduces a new problem of how to handle public content.

Our conclusion is that currently proposed technical measures will not be able to completely stop the illegitimate distribution of pirated content. We believe that content producers must take steps to compete with the piracy as an alternative.

References

[1] E. Allamanche, J. Herre, B. Froba, and M. Cremer, "AudioID: Towards Content-Based Identification of Audio Material". In Proc. 110th AES Convention, Amsterdam, NL, 2001.

[2] P. Biddle, P. England, M. Peinado, and B. Willman, "The Darknet and the Future of Content Protection". In *Digital Rights Management: Technological, Economic, Legal and Political Aspects*, ed. Erberhard Becker, Willms Buhse, Dirk Günnewig, Niels Rump (Springer-Verlag, 2003).

[3] S.A. Craver, M. Wu, B. Liu, A. Stubblefield, B. Swartzlander, D.S. Wallach, D. Dean, E. Felton, "Reading between the lines: lessons from the SDMI challenge," Proceedings of the 10th USENIX Security Symposium, Washington, D.C., August, 2001.

[4] P. C. Fishburn, A. M. Odlyzko, and R. C. Siders, "Fixed fee versus unit pricing for information goods: competition, equilibria, and price wars," *First Monday* 2(7), July 1997. Available at http://firstmonday.org/. Definitive version on pp.

[7] The pricing of different parts of a sophisticated new offering along these lines might well take into account the risk-management aspects of handling pirates' competing offerings for different pieces of content.

167-189 in *Internet Publishing and Beyond: The Economics of Digital Information and Intellectual Property*, B. Kahin and H. R. Varian, eds., MIT Press, 2000.

[5] http://www.microsoft.com/presspass/features/2002/jul02/0724palladiumwp.asp

[6] http://www.trustedcomputinggroup.org

[7] T. Kalker, J.P.M.G. Linnartz, M. van Dijk, "Watermark Estimation through Detector Analysis," Int. Conf. on Image Processing, ICIP, October 1998, Chicago IL.

[8] F.A.P. Petitcolas. "Watermarking schemes evaluation" IEEE Signal Processing, vol. 17, no. 5, pp. 58–64, September 2000.

[9] C. Shapiro and H. Varian, *Information Rules*, Harvard Business School Press, 1999.

[10] O. Sibert, D. Bernstein and D. Van Wie. "Digibox: A self-protecting container for information commerce," Proceedings of the 1st USENIX Workshop on Electronic Commerce. New York, New York, July 1995.

[11] H. Varian and R. Roehl, "Circulating Libraries and Video Rental Stores," *First Monday*, 6(5), May 2001. Available at http://firstmonday.org/.