

2.8 If Piracy Is the Problem, Is DRM the Answer?⁵⁶⁶

*Stuart Haber, Bill Horne, Joe Pato, Tomas Sander*⁵⁶⁷,
*Robert Endre Tarjan*⁵⁶⁸

I 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 chapter of this book entitled: *The Darknet and the Future of Content Protection* (page 344). 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.

II 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.

⁵⁶⁶ The opinions expressed in this article reflect solely the view of the authors and are not necessarily the view of HP.

⁵⁶⁷ Stuart Haber, Bill Horne, Joe Pato, Tomas Sander: Hewlett-Packard Laboratories.

⁵⁶⁸ Department of Computer Science, Princeton University, and Office of Strategy and Technology, Hewlett-Packard.

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 friend⁵⁶⁹.
- *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.

III DRM Technologies

The goal of a DRM system is to enforce licenses⁵⁷⁰ 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*.⁵⁷¹ 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 unlimited ways. In particular, they can

⁵⁶⁹ 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.

⁵⁷⁰ Also known as *policies* or *digital rights*.

⁵⁷¹ 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.