THE IMPOSSIBILITY OF TECHNOLOGY-BASED DRM AND A MODEST SUGGESTION

JOHN BLACK[*]

INTRODUCTION

When I was a teenager in the late 1970's, there was no World-Wide Web, no Internet, and no IBM PC. But I, along with a small group of friends, became obsessed with computers: the TRS-80 and the Apple were the targets of our passion. Each time a new computer game was announced, we awaited its release with great anticipation: not because we wanted to kill the dragon or get to level 37, but because we wanted to see how hard it was *this time* to remove the copy protection from the software.

In those early days of personal computing, game manufacturers made perhaps one million dollars per year, and there were only a handful of companies. Few had ever heard of Microsoft, and there were no such things as CD burners or high-speed networks. So trying to control illegal copying (or "pirating" as it was already called back then) was a concern limited to just a few small companies.

Today there are software companies with tens of billions of dollars in gross revenues, each with a strong vested interest in overseeing the legal distribution of their products. Additionally, media companies (in particular, music and film producers and distributors) continue their fight to control illegal distribution of their content, especially now in the presence of the $50 CD burner. To address these problems, media companies have turned to technology such as Digital Rights Management (DRM) to prevent copying and enforce protection of copyright. In this paper I will argue that the media companies' reliance on a technological solution is almost certainly doomed, and that a variety of motives will continue to drive people to circumvent any such technology. The best solution to the problem is not a technological one, but instead one of education.

In Section I of this paper, I will discuss some historical and current examples where the media companies have relied on technology to protect their products and why each has failed. In Section II, I will

[*] Department of Computer Science, University of Colorado at Boulder, jrblack@cs.colorado.edu.

explain why the current dependence on DRM to solve the copyright protection problem has also failed. In Section III, I will look at the current state of legal protections that have been created to assist in the protection of digital content. Finally, I will explain what is missing from each of these approaches.

I. TECHNOLOGY TO THE RESCUE?

Technology will never solve the Digital Rights Management (DRM) problem because of the implicit challenge in attempting to conceal, obfuscate, or make "uncopyable" programs and content. Just as it happened 25 years ago, it happens still today: the harder copyright owners work to protect their content, the harder talented technicians work to circumvent these protections. The challenge of showing that these schemes do not work is irresistible to many people who spend countless hours working to break the "unbreakable." The motivation of such "crackers" varies: some wish to win peer recognition by removing the protection, some are expressing civil disobedience in objection to copyright laws, and some just enjoy solving puzzles.[1]

The various attempts to use technology to control copying (and other rights copyright holders wish to control), have all thus far failed.[2] Embarrassingly, for the software and media providers who have attempted these technological solutions, they have often failed in spectacular ways. I survey just a few examples.

A. Intentional Errors

One way in which copy protection was attempted in the old days (*i.e.*, 1978) was as follows: the game distributor would *intentionally* induce an error on some track of a diskette before distributing it. Then the software that loads the game would first check to ensure that the error was in place before it would load the game. If the defective track was not present, the game would not load. The idea here is simple: if one now attempts to copy the diskette, any self-respecting disk copy program would find the defective track unreadable and therefore make a legitimate track on the copied version. Disk copy programs would *not* reproduce the bad track, and therefore copies made this way were useless. There were two simple ways around this: (1) make a disk copy program which *did* reproduce errors, or (2) find and remove the piece of the software which checked for the bad track. In 1978, method (2) was

[1] STEVEN LEVY, HACKERS (2001).

[2] *See* Ryan Roemer, *Trusted Computing, Digital Rights Management, and the Fight for Copyright Control on Your Computer*, 2003 UCLA J.L. & TECH. 8, *available at* http://www.lawtechjournal.com/articles/2003/08_040223_roemer.php.

the most common technique, but two years later someone did write a program to make copies of software that included the errors, thereby defeating the entire protection scheme and allowing fast and repeated copying of programs.

Some twenty-three years later, Sony used a somewhat similar technique in its Key2Audio technology meant to protect CDs from being loaded on PCs.[3] After all, if you can prevent PCs from reading a CD, you can prevent copying (both the illegal and legal varieties, in fact). Sony's technique leverages the difference between low-end commodity CD players and powerful PC-based software players.[4] Low-end players have limited processing power and almost universally tolerate errors on the first track of the CD, whereas the more powerful players attempt to make sense of the data on the first track and if there is an error, they give up. Sony Key2Audio technology purposely induces errors on the first track to make CDs unplayable (and therefore uncopyable) on personal computers.[5] However, it was quickly discovered that the bogus information preventing PC-based players from loading the CD could be effectively removed using a felt tipped pen on the edge of the CD.[6] Blackening this track then allowed the CD to be loaded, played, and copied by any PC. This was an embarrassingly simple and inexpensive way to defeat a copy-protection scheme

A more recent copy-protection scheme by SunnComm underwent extensive testing before it was deployed.[7] The idea was that a special piece of software would be loaded from the SunnComm-enhanced CD into the PC in order to disable copying. Testers used "ripper" programs to attempt to copy CDs protected with their technology and none was successful.[8] The company claimed therefore that their product yielded a "verifiable and commendable level of security."[9] Not long after, it was discovered that simply holding down the "Shift" key while inserting the CD allowed the tracks to be copied.[10]

[3] *See* KEY2AUDIOXS SOLUTION, SONY DADC, *available at* http://www.key2audio.com/solution.asp (last visited Mar. 23 2005).

[4] *Id.*

[5] *Id.*

[6] Brendan I. Koerner, *Can You Violate Copyright Law With a Magic Marker?*, SLATE.COM, June 3, 2002, *at* http://slate.msn.com/id/2066527/.

[7] SUNNCOMM, MEDIAMAX, *at* http://www.sunncomm.com/Brochure/SunncommCover.htm (last visited Mar. 23, 2005).

[8] *Id.*

[9] *Id.*

[10] J. ALEX HALDERMAN, ANALYSIS OF THE MEDIAMAX CD3 COPY-PREVENTION SYSTEM (Princeton University Computer Science Technical Report TR-679-03, Oct. 6, 2003), *available at* http://www.cs.princeton.edu/~jhalderm/cd3/.

II. WHY TECHNOLOGY-BASED DRM IS IMPOSSIBLE

The newest technology that attempts to implement DRM (along with other objectives) is Microsoft's "Trusted Computing" concept, formerly known as "Palladium."[11] The idea behind "trusted computing" is to use secure hardware to boot the Windows operating system to ensure it is a valid version, uncorrupted by viruses or other "illegally added" code.[12] Then when Disney or any other media developer wishes to ensure that this computer has properly licensed some content, it uses a cryptographic protocol (mathematical algorithms to authenticate and encrypt digital content) which is hard to simulate without access to internal information (or "keys") embedded within the secure hardware.[13]

There are three essential technological problems with the "trusted computing" concept. The first problem is that "secure hardware" is never fully secure. In the first implementations of this scheme, there was a special chip called the "Fritz Chip" which was added next to your Pentium CPU.[14] The Fritz chip holds the cryptographic keys, and it was not too hard to extract these keys via reverse-engineering.[15] The Fritz chip will eventually be embedded into the Pentium itself (Intel is part of the Trusted Computing group) and then things will become more difficult. But most hardware experts still predict that it will be feasible to extract the keys from the chip.[16] The problem is that in order to make hardware secure, you have to spend a lot of money: typical "tamper-proof" chips must resist attempts to extract their contents.[17] Sophisticated techniques for reverse engineering include x-raying chips, sampling input-output pairs, and shaving very thin slices from their packaging until their layouts can be viewed with a microscope.[18] To circumvent such attacks, secure chip manufacturers are forced to use various techniques, such as the introduction of chemicals which cause the chip to self-destruct when exposed to air. This adds significant cost to the production process. But if the chips are to be a commodity technology, you have to spare no expense. So manufacturers will err on

[11] MICROSOFT, NEXT-GENERATION SECURE COMPUTING BASE, *at* http://www.microsoft.com/resources/ngscb/default.mspx (last visited Mar. 23, 2005).

[12] *Id.*

[13] *Id.*

[14] ROSS ANDERSON, 'TRUSTED COMPUTING' FREQUENTLY ASKED QUESTIONS (Aug. 2003), *available at* http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html.

[15] *Id.*

[16] *Id.*

[17] SUN MICROSYSTEMS, SMART CARD OVERVIEW, *at* http://java.sun.com/products/javacard/smartcards.html (last visited Mar. 23, 2005).

[18] Gary McGraw, *Smart cards, Java cards and security*, DATAMATION, Jan. 19, 1998, *at* http://itmanagement.earthweb.com/ecom/article.php/601661.

the side of using a limited amount of secure technology in order to save money and keep their products affordable and competitive.[19]

The second problem, which is common to all technological attempts at DRM, is that the computer and its accessories are physically in the presence of the adversary (*i.e.*, you). The only way in which to *guarantee* the security of information is when these companies are able to hide some key piece of information from the attacker. For example, when you log in to a computer system, you often provide a password; this is the leverage you have over an attacker: the attacker does not know your password. But in the DRM setting, the computer knows all; there is no outside authority involved. Any keys or passwords used in unlocking the software or media must be contained within the computer, (whether it be in software or in hardware) and therefore, the attacker has physical access to them. Although using secure hardware does ameliorate this problem to some extent, as discussed above, it means that someone must pay for this secure hardware.

The third problem is that, at some point, the content you have purchased must appear. If it is music, sound must eventually emanate from your speakers; if it is a movie, images must appear on your screen in addition to sound. On a typical PC, the sound is generated by a "sound card" and the video by a "video card." These signals are then transferred to your speakers and screen via cables (laptop computers excepted). It is a trivial matter for anyone to attach alligator clips to these cables and record the video and the sound! At this point, the person has successfully copied a song or movie, defeating any sort of DRM anti-copying technology imaginable. If the signals on these cables are analog, there is some degradation in quality, but not much. And more and more the signals these days are digital, where there is zero degradation. This last problem would seem to be the death-knell for DRM technology. But, not to be deterred, purveyors have come up with a "solution" for this problem. The solution is called "watermarking."

A. Watermarking

One problem with cracking copy-protection schemes is that it takes a huge effort, a lot of time, and a fairly sophisticated attacker to defeat some copy-protection schemes.[20] This is good news for the copyright holder because the number of people who are willing to spend the time and money, and who possess the necessary skills is very small. The copyright holder might even be willing to ignore this small minority of lawbreakers, instead hoping that they will be only noise on the revenue

[19] *Id.*

[20] LEVY, *supra* note 1.

sheets. Unfortunately there is a principle known as BORA: Break Once Run Anywhere.[21] This is meant to capture the notion that once *one* person has invested the time to break the copy-protection mechanism, he can then distribute the content in unprotected form to thousands of other users who need only know how to use the Internet and a CD burner.[22] A proposed solution to this problem is known as "watermarking."

Watermarking is a technology intended to enable content distributors to uniquely mark each copy of a song or movie with a unique serial number in such a way that (1) the marking does not adversely affect the quality of the content, (2) the mark can be read efficiently by the copyright holder and its enforcement agencies, (3) the mark is "robust" in that it is preserved in spite of normal degradation or alteration to the content (for example if a song were compressed or if it were converted to analog and then back to digital), and (4) the mark is *hard to remove*.[23] The idea behind watermarking goes to law enforcement of illegal copying and distribution.[24] If watermarking could achieve all of these aims, then any content found in illegal distribution channels could be traced back to the original legitimate purchaser who could then be lawfully prosecuted for illegally distributing it.

The watermarking approach, however, fails in several respects. No one knows any watermarking technology that achieves all four of the properties above, despite several attempts at circumventing it.[25] The most famous instance of a watermarking technology thought to have all four of these properties was one developed by the Recording Industry Association of America (RIAA). The RIAA distributed a song with several watermarks and challenged researchers to remove them without degrading the quality of the music.[26] When a group from Princeton, headed by Edward Felten, succeeded in doing just this,[27] the RIAA threatened suits against Princeton, Professor Felten, and the conference

[21] *See, e.g.*, STEPHEN R. LEWIS, HOW MUCH IS STRONGER DRM WORTH? (2003), *available at* http://www.cl.cam.ac.uk/users/srl32/eis1.pdf.

[22] *Id*.

[23] *See generally* WATERMARKING WORLD, WELCOME TO DIGITAL WATERMARKING WORLD, *at* http://www.watermarkingworld.org/ (last visited Mar. 23, 2005).

[24] *Id*.

[25] *Id*.

[26] Letter from Matthew J. Oppehnheim, Secretary of SDMI foundation, to Edward Felten, Professor, Princeton University (Apr. 9, 2001), *available at* http://www.theregister.co.uk/extra/sdmi-attack.htm.

[27] Secure Internet Programming Group of Princeton University Department of Computer Science, Status of the paper *Reading Between the Lines: Lessons from the SDMI Challenge*, *at* http://www.cs.princeton.edu/sip/sdmi/ (last visited Mar. 23, 2005).

organizers where Felten planned to present his methods.[28] Felten smartly decided to withdraw his paper from the conference.[29]

Perhaps watermarking technology will one day reach a level of sophistication where no one knows how to successfully remove the markings. But, even if a foolproof watermark were developed, there are still legal and ethical problems in attempting to enforce copyright in the manner described above. Suppose, for example, a 15-year-old girl is found to be the source of a leaked Stankonia track. Is the RIAA *really* going to try and recover perceived losses from her in court? Or worse, pursue criminal charges against her? Though the RIAA and DVD Copy Control Association (CCA) have made examples of a few particularly blatant violators, it would seem extremely impractical, not to mention cost-prohibitive, to pursue legal action against every offender.[30] What is to prevent people from claiming that a CD was lost or stolen and that *someone else* released it onto the Internet? Are we going to be asked to sign a contract accepting all liability should our purchased music be found to have been illegally distributed?

There are limited contexts in which watermarking makes sense and in which it might afford the protections desired. One example is for "screeners" who acquire high-quality copies of pre-release movies in order to view them for the *Academy Awards* (these screeners are thought to often be a source of leaks).[31] In this case the screeners are adults, are made to sign a contract, and are small in number. Another example is downloaded software where you are often required to identify yourself (via credit card and other personal information), but watermarking technology has not yet been targeted at software.[32] In any event, one can hardly imagine the watermarking solution working on a global scale, if even the technology can be realized in the first place

[28] *See* ELECTRONIC FREEDOM FOUNDATION, FELTEN, ET AL., V. RIAA, ET AL., *at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/ (last visited Mar. 23, 2005).

[29] Felton later sued the RIAA but dropped the case when the RIAA assured Felton that it would not pursue the matter. *See* Media Release, Electronic Frontier Foundation, Security Researchers Drop Scientific Censorship Case (Feb. 6, 2002), *available at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/20020206_eff_felten_pr.html (the RIAA further encouraged Felton to publish his findings, "because everyone benefits from research into the vulnerabilities of security mechanisms.").

[30] *See generally* DVD COPY CONTROL ASSOCIATION, FREQUENTLY ASKED QUESTIONS, *at* http://www.dvdcca.org/faq.html (last visited Mar. 23, 2005).

[31] Aliya Sternstein, *Disney's Pirate Fight*, FORBES.COM (Sept. 29, 2003), *at* http://www.forbes.com/2003/09/29/cz_as_0929dis.html.

[32] CHRISTIAN COLLBERG & CLARK THOMBORSON, SOFTWARE WATERMARKING: MODELS AND DYNAMIC EMBEDDINGS (1999), *available at* http://citeseer.ist.psu.edu/cache/papers/cs/3565/http:zSzzSzwww.cs.auckland.ac.nzzSz~collbergzSzResearchzSzPublicationszSzCollbergThomborson99azSzA4.pdf/collberg99software.pdf.

III. Legal Approaches

Copyright law is known for its complexity, but its basic tenets are understood by most laypersons: copyrighted materials may be copied for your own "fair-use," but you may not make copies for distribution to others.[33] Though some people may have understood these rules, it does not necessarily follow that they have obeyed them. The music industry has long suffered significant losses in revenue due to music sharing, but until the Internet Age it was small enough to be tolerable.[34] By 2001, with more than 100 million computers on the Internet, illegal distribution had become all too easy, and new laws were needed.[35]

The Digital Millennium Copyright Act (DMCA), passed in 1998, was designed to augment protections for copyright holders in the age of the Internet.[36] The law attempts to compensate for the lack of any workable technology for DRM by outlawing the methods used to defeat that technology.[37] In particular, the law states that it is illegal to reverse engineer a product, be it hardware or software, for the purposes of circumventing copyright.[38]

The law provoked an immediate outcry on many fronts. Academics claimed the law rescinded their basic right to evaluate and analyze technology, a practice long established by researchers.[39] Professor Felten, mentioned above, said the law rescinded our fundamental "freedom to tinker" with the products we purchase.[40] Some claimed the law was in conflict with fair-use.[41] But now, six years later, the law remains in effect and people continue to be prosecuted under its provisions. I believe that law is the proper vehicle for enforcing the rights of copyright holders, though I also believe the DMCA is fundamentally the wrong law to do it. Academic freedom and the broad

[33] *See, e.g.*, Démodé, Copyright and Common Sense, *at* http://www.demode.tweedlebop.com/copyright.htm*l* (last revised Aug. 27, 2004).

[34] Vangie Aurora Beal, When Is Downloading Music on the Internet Illegal?, Webopedia.com (Dec. 22, 2004), *at* http://www.webopedia.com/DidYouKnow/Internet/2004/music_downloading.asp.

[35] See *Internet Hosts Reach 100 Million Worldwide*, Information Superhighways Newsletter, June 2001, *available at* http://www.findarticles.com/p/articles/mi_m0IGM/is_6_8/ai_76701365.

[36] Digital Millennium Copyright Act § 103(a), 17 U.S.C. § 1201(a)(2) (2004).

[37] *Id*.

[38] *Id*.

[39] *Tinkerer's Champion*, The Economist, Jun. 20, 2002, *available at* http://www.economist.com/science/tq/displayStory.cfm?story_id=1176171.

[40] *See* Edward Felten, Weblog, *at* http://www.freedom-to-tinker.com/about.html (last updated Mar. 23, 2005).

[41] Mark Lemley & Anthony Reece, Stopping Digital Copyright Infringement Without Stopping Innovation (TPRC Program Paper No. 210, 2003), *available at* http://tprc.org/papers/2003/210/Stopping_Copyright_Infringement_Without_Stopping_Innovation.htm.

protections accorded by fair-use are deeply jeopardized by this law. There are several researchers who have purposely steered clear of analyses of protected software or media for fear that it might land them in jail.[42] If anything, the DMCA has spurred civil disobedience and cultivated scorn by those who dislike its restrictions. As an example, the Content Scrambling System (CSS) was invented by the Motion Picture Association of America to protect DVDs.[43] CSS is a simple encryption system which prevents reading the DVD unless the machine knows the corresponding decryption algorithm.[44] However, since software to play DVDs is available for PCs, it was a fairly straightforward matter to reverse engineer the player and figure out how to decrypt CCS-protected content. The resulting program is called DeCSS[45] and is available on hundreds of websites around the world, despite its possibly prohibited status under the DMCA. Furthermore, you can purchase t-shirts, sweatshirts, and coffee mugs with the DeCSS code printed on them. I have one such t-shirt, it gives the DeCSS code along with the relevant portions of the DMCA stating "I am a circumvention device forbidden by 17 USC 1201(a)(2). Do not manufacture me, import me, offer me to the public, provide me, or traffic in me or in any part of me. You have been warned." I believe a more sensible law, respecting citizens' "right to tinker" and their continued access to fair-use of purchased content, would likely be more successful in curbing piracy. It would likely evoke far less backlash and disobedience among those who would ordinarily respect the law.

IV. THE MISSING PIECE?

Most of what I have written above is familiar to those who specialize in DRM. There are those who might disagree with some of it, but it is all familiar. However, I have never seen anyone make the following simple argument: why not attempt to curb illegal copying by simply explaining to people that it is *wrong*. It is a laughably simple suggestion. People surely *know* that distributing copyrighted material is illegal, and people surely know that it is wrong to break the law. So explaining the transitivity of these two statements should not make a difference. I disagree.

[42] *See* NIELS FERGUSON, CENSORSHIP IN ACTION: WHY I DON'T PUBLISH MY HDCP RESULTS (Aug. 15, 2001), *available at* http://macfergus.com/niels/dmca/cia.html.

[43] *See* WIKIPEDIA, CONTENT SCRAMBLING SYSTEM, *at* http://en.wikipedia.org/wiki/Content-scrambling_system (last modified Mar. 19, 2005).

[44] *Id*.

[45] *See* LEMURIA.ORG, DECSS CENTRAL, *at* http://www.lemuria.org/ DeCSS/main.html (last visited Mar. 23, 2005).

The vast majority of illegal song sharing on the Internet is done by young people.[46] I recently spoke with a small number of high school students and asked them a few simple questions about illegal sharing of content. The results were enlightening: although these students knew that sharing copyrighted songs was illegal, they thought it "wasn't a big deal." Their perception was, generally that copying bits floating over wires could not be considered "real theft" because there was no physical object being stolen. I asked them if they would ever consider walking into Wal-Mart and slipping a DVD inside their coats. None of them would consider this: it was *clearly wrong*.

Although part of this difference stems from the different levels of risk involved, *i.e.*, in the bricks-and-mortar context, there is a higher risk of getting caught, there is a more fundamental distinction. The high school students had the perception that stealing a physical object is somehow more significant than stealing digital content. These students believed that the value in a CD lay in the medium, the jewel case, and the labeling, *not* in the content. Anyone in the recording industry will tell you that exactly the reverse is true. I modestly suggest that copyright holders should spend less effort suing violators of the DMCA and those running illegal content distribution servers, and spend more effort educating young people that downloading a movie, a song, or software is *absolutely equivalent* to walking into a store and slipping that same movie, song, or program into their coats. This viewpoint could be aired through the usual channels to reach its target: television commercials, movie trailers, inserts included with CDs and DVDs. The cost would likely be sizeable, but if the losses to content providers are as staggering as they claim, surely any significant gains against piracy would be worthwhile.

In the 21st century we have a new model for content distribution—we need a new moral doctrine to match. And those best suited to educate us are those who stand to lose the most by neglecting to do so: the copyright owners.

[46] Frank Ahrens, *RIAA's Lawsuits Meet Surprised Targets; Single Mother in Cali.; 12-Year-Old Girl in N.Y. Among Defendants*, WASH. POST, Sept. 10, 2003, at E1.