BEFORE THE FEDERAL TRADE COMMISSION

IN THE MATTER OF
FTC TOWN HALL TO ADDRESS DIGITAL RIGHTS MANAGEMENT TECHNOLOGIES

Comment of:
J. Alex Halderman
Assistant Professor of Electrical Engineering and Computer Science
--
University of Michigan
CSE Building, Room 4717
2260 Hayward Avenue
Ann Arbor, MI 48109-2121

Represented by:
Blake E. Reid, Clinician and Juris Doctor Candidate
Harry A. Surden, Associate Professor of Law
Paul K. Ohm, Associate Professor of Law
J. Brad Bernthal, Associate Clinical Professor of Law
--
Samuelson-Glushko Technology Law & Policy Clinic
University of Colorado School of Law
105R Wolf Law Building, 401 UCB
Boulder, CO 80309-0401

January 29, 2009

Pursuant to the Proposed Topics for Discussion[1] and the Notice and Request for Public Comment[2] in regard to an FTC Town Hall Meeting to Address Digital Rights Management Technologies, we request that the Commission consider an approach to mitigating the security risks posed to consumers by digital rights management ("DRM") systems. In particular, our request focuses on DRM-protected consumer products that are accessible on personal computers ("PCs"), including video games, audio compact discs, and other works.

The Commission has called for discussion on improving disclosures to consumers regarding limitations of DRM systems. Consumers would benefit greatly from transparent disclosures about the specific security risks posed by many PC-based DRM systems. These risks can include the surreptitious installation of undesired software, the loss of control over critical PC software and hardware, and exposure to cyber-attacks and malware such as viruses, worms, Trojan horses, and spyware, which may lead to the compromise of private personal data.

---

[1] *Available at* http://www.ftc.gov/bcp/workshops/drm/topics.shtml.
[2] *Available at* https://secure.commentworks.com/ftc-DRMtechnologies/.

Unfortunately, the content industry has been largely unable or unwilling to disclose the security risks posed to consumers by these DRM systems prior to the release of products. Content producers have remained largely dismissive of consumer concern over potential security risks, and have responded lethargically, if at all, with fixes to serious security problems. Furthermore, certain industry members have stifled the efforts of independent security researchers, who were acting in good faith to discover and fix these problems, by threatening litigation under the anti-circumvention measures of the Digital Millennium Copyright Act ("DMCA"). This state of affairs leaves many consumers vulnerable to security threats and uninformed of the risks that they face. We believe that this is an untenable situation.

In the ongoing triennial DMCA exemption rulemaking at the Library of Congress, we have requested appropriate exemptions from the DMCA anti-circumvention measures to allow independent security researchers acting in good faith to investigate and correct security problems in DRM on many PC-accessible works *ex post*. However, consumers would surely benefit from more proactive behavior on the part of the content industry to address security problems *ex ante*, before they end up affecting consumers' PCs. While class action lawsuits over security problems[3] may lead to *ad hoc* change by individual companies, it does not appear that a comprehensive, proactive approach to addressing DRM security problems will manifest across the content industry without some form of regulatory intervention.

Accordingly, we ask the Commission to consider pursuing and implementing a two-pronged solution that will require or strongly encourage companies using DRM systems on PC-accessible products to: 1) submit to independent security audits of the DRM systems and 2) provide conspicuous notice to consumers of the products regarding the nature, operation, and limitations of any DRM systems included in the products, as well as the general security risks inherent to most PC-based DRM systems and any known flaws specific to the included DRM systems.

In support of our request, we have attached the following documents for the consideration of the Commission:

- J. Alex Halderman, Blake E. Reid, Paul K. Ohm, Harry A. Surden, and J. Brad Bernthal, *In the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies* (Dec. 2, 2008) (rulemaking filing discussing the current state of PC-based DRM systems and security issues).
- J. Alex Halderman and Edward W. Felten, *Lessons from the Sony CD DRM Episode* (Feb. 14, 2006) (an in-depth, peer-reviewed analysis of the Sony-BMG rootkit saga).

[3] Five class action suits have now been filed against Electronic Arts over potential security problems in the SecuROM DRM software. *See The People vs. SecuROM*, RECLAIM YOUR GAME!, *available at* http://www.reclaimyourgame.com/index.php?option=com_content&view=section&layout=blog&id=17&Itemid=57.

- Edward W. Felten, J. Alex Halderman, Deirdre K. Mulligan, and Aaron Perzanowski, *Comment Re: RM 2005-11 – Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies* (Dec. 1, 2005) (rulemaking filing discussing the Sony rootkit saga)).

We have separately requested that Professor Halderman be considered as a panelist for the Mar. 25, 2009 Town Hall meeting on DRM.

We thank the Commission for its consideration.

Sincerely,

/s/

J. Alex Halderman • Blake E. Reid • Harry Surden • Paul Ohm • J. Brad Bernthal

Enclosures

BEFORE THE COPYRIGHT OFFICE OF THE LIBRARY OF CONGRESS

IN THE MATTER OF
EXEMPTION TO PROHIBITION ON CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS FOR ACCESS CONTROL TECHNOLOGIES

Docket No. RM 2008-8

Comment of:
J. Alex Halderman
Assistant Professor of Electrical Engineering and Computer Science
--
University of Michigan
CSE Building
2260 Hayward Avenue
Ann Arbor, MI 48109-2121

Represented by:
Blake E. Reid, Clinician and Juris Doctor Candidate
Paul K. Ohm, Associate Professor of Law
Harry A. Surden, Associate Professor of Law
J. Brad Bernthal, Associate Clinical Professor of Law
--
Samuelson-Glushko Technology Law & Policy Clinic
University of Colorado School of Law
105R Wolf Law Building, 401 UCB
Boulder, CO 80309-0401

December 2, 2008

Pursuant to the Notice of Inquiry of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies[1] ("NOI") and 17 U.S.C. § 1201(a)(1)(C), we respectfully request that the Librarian of Congress grant an exemption to 17 U.S.C. § 1201(a)(1)(A) for (1) literary works, sound recordings, and audiovisual works accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities, or, in the alternative, for (2) video games accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.

---

[1] 70 Fed. Reg. 73, 58073 (Oct. 6, 2008) [hereinafter *NOI*].

I. Submitting Party

J. Alex Halderman is a noted computer security and privacy researcher and an assistant professor of electric engineering and computer science at the University of Michigan.[2] His research focuses particularly on the threats introduced by access and copy-protection measures. In particular, he published in 2003 an academic paper on SunnComm's MediaMax copy-protection system[3]. In response, SunnComm first threatened a lawsuit under the Digital Millennium Copyright Act ("DMCA")[4], then subsequently retracted the lawsuit, citing the "chilling effect on [computer security] research."[5]

Partially in response, Professor Halderman proposed, as part of the third iteration of this rulemaking process (along with Princeton Professor Edward W. Felten), an exemption to the DMCA anti-circumvention measures to address the chilling effect of the statute on computer security researchers in the context of insecure technological protection measures ("TPMs") on compact discs containing audio recordings and the unfair access limits that the statute placed on consumers.[6] As a result, the Librarian of Congress exempted the following class of works from the anti-circumvention measures (hereinafter "Sound Recordings Exemption"):

> *Sound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.*[7]

---

[2] http://www.cse.umich.edu/~jhalderm/.
[3] J. Alex. Halderman, *Analysis of the MediaMax CD3 Copy-Prevention System*, PRINCETON UNIVERSITY COMPUTER SCIENCE TECHNICAL REPORTS TR-679-03, *available at* http://www.cs.princeton.edu/research/techreps/TR-679-03.
[4] Fred Locklear, *Press "Shift" to Initiate Lawsuit*, ARS TECHNICA (Oct. 9, 2003), *available at* http://arstechnica.com/archive/news/1065755223.html.
[5] Fred Locklear, *SunnComm Shifts Stance, Backs Away from Lawsuit*, ARS TECHNICA (Oct. 10, 2003), *available at* http://arstechnica.com/archive/news/1065816462.html.
[6] Edward W. Felten and J. Alex Halderman, Re: RM 2005-11 – Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (Dec. 1, 2005), *available at* http://www.copyright.gov/1201/2006/comments/mulligan_felten.pdf.
[7] Final Rule of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 227, 68477 [hereinafter "FR"].

II. Proposed Classes of Works

In this rulemaking, we request that the following class of works (hereinafter "Class 1") be exempted from the anti-circumvention measures:

> *Literary works, sound recordings, and audiovisual works accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.*

In the alternative, we request that the following class of works (hereinafter "Class 2") be exempted instead:

> *Video games accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.*

In the proposed classes of works, we have tracked very closely the language adopted by the Librarian during the third rulemaking in granting the Sound Recordings Exemption, merely replacing "[s]ound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format" with "[l]iterary works, sound recordings, and audiovisual works accessible on personal computers" in Class 1, and "[v]ideo games accessible on personal computers" in Class 2, and thereby maintaining the proposed classes of works as limited subsets of the categories of authorship enumerated in 17 U.S.C. § 102(a), further limited to particular uses, as required for an exemption under the NOI.[8]

In particular, the starting points of Class 1 are literary works, sound recordings, and audiovisual works, each a copyrightable category of authorship under 17 U.S.C. § 102(a). Indeed, each category was a starting point of another exemption granted by the Librarian during the third rulemaking.[9]

---

[8] *See NOI*, *supra* note 1 at 58077.

[9] *(1)* ***Audiovisual works*** *included in the educational library of a college or university's film or media studies department, when circumvention is accomplished for the purpose of making compilations of portions of those works for educational use in the classroom by media studies or film professors . . .*
(4) ***Literary works*** *distributed in ebook format when all existing*

The starting point of Class 2 is video games. Video games are a subset of computer programs, which are themselves a subset of literary works under 17 U.S.C. § 102(a)[10]. Video games may further embody literary works, audiovisual works, and sound recordings, all copyrightable categories of authorship under Section 102(a). Accordingly, Class 2 forms a narrow subset of Class 1. Video games were also embraced as part of the class of works of another exemption granted by the Librarian during the third rulemaking.[11]

Furthermore, both proposed classes are limited to works protected by TPMs that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers ("PCs"). Finally, both classes are limited to circumvention "accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities."

As discussed in the following sections, these limitations narrowly focus the proposed classes to remedy the evidence of present and likely harm while preserving protection for copyright holders in other classes as required under the NOI.[12]

> *ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book's read–aloud function or of screen readers that render the text into a specialized format . . . [, or]*
> *(6)* ***Sound recordings****, and* ***audiovisual works*** *associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities."*

FR, *supra* note 7 at 68480 (emphasis added).

[10] *Dun & Bradstreet Software Services, Inc. v. Grace Consulting, Inc.*, 307 F.3d 197, 206 (3d Cir. 2002) (citing *Whelan Assoc. v. Jaslow Dental Lab.*, 797 F.2d 1222, 1234 (3d Cir. 1986)).

[11] > *(2) Computer programs and* ***video games*** *distributed in formats that have become obsolete and that require the original media or hardware as a condition of access, when circumvention is accomplished for the purpose of preservation or archival reproduction of published digital works by a library or archive. A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial marketplace.*

FR, *supra* note 7 at 68480 (emphasis added).

[12] *See NOI*, *supra* note 1 at 58077.

III. Summary of Argument

Beginning in 2005, over *half a million* PCs were afflicted with serious security vulnerabilities as a side effect of copy-protection software, known as a "rootkit," distributed on audio compact discs ("CDs") by Sony.[13] Though the company initially professed ignorance over the rootkit fiasco[14], public outcry and legal advocacy later led to a partial recall of rootkit-equipped CDs[15], abandonment of the rootkit[16], and the aforementioned Sound Recordings Exemption.

Since the third rulemaking, evidence has been uncovered indicating that security flaws in TPMs affecting works *outside* the scope of the Sound Recordings Exemption have created similar security vulnerabilities in many more PCs. A flaw uncovered last year in Macrovision's SafeDisc software[17], one of the most widely used copy-protection systems for PC-accessible video games[18], exposed PCs to attacks similar to but even more dangerous than those enabled by the Sony rootkit.[19] Because SafeDisc shipped preinstalled on nearly every copy of the Microsoft Windows XP and Windows 2003 operating systems, the vulnerability affected nearly *one billion PCs*, two thousand times more than the rootkit.[20]

---

[13] Paul F. Roberts, *Sonys [sic] Rootkit Is on 500,000 Systems, Expert Says*, EWEEK.COM (Nov. 15, 2005), *available at* http://www.eweek.com/c/a/Security/Sonys-Rootkit-Is-on-500000-Systems-Expert-Says/.

[14] Andrew Orlowski, *Sony Digital Boss – Rootkit Ignorance is Bliss*, THE REGISTER (Nov. 9, 2005), *available at* http://www.theregister.co.uk/2005/11/09/sony_drm_who_cares/.

[15] John Borland, *Sony Recalls Risky 'Rootkit' CDs*, CNET (Nov. 15, 2005), *available at* http://news.cnet.com/Sony-recalls-risky-rootkit-CDs/2100-7349_3-5954154.html.

[16] Amy Phillips, *Sony Discontinues Controversial Anti-Piracy Software*, PITCHFORK MEDIA (Nov. 15, 2005), *available at* http://www.pitchforkmedia.com/article/news/35490-sony-discontinues-controversial-anti-piracy-software.

[17] Microsoft, *Security Bulletin MS07-067– Important: Vulnerability in Macrovision Driver Could Allow Local Elevation of Privilege* (Dec. 11, 2007), *available at* http://www.microsoft.com/technet/security/Bulletin/MS07-067.mspx.

[18] *See Macrovision Announces SafeDisc DVD-ROM Copy Protection*, EMEDIALIVE.COM (May 16, 2003), *available at* http://www.emedialive.com/Articles/ReadArticle.aspx?ArticleID=7594.

[19] Both the Sony rootkit and the flawed SafeDisc software are so-called "device drivers." Device drivers have effectively unrestricted access to PC hardware and software, so attackers can often leverage security flaws in the drivers to bypass other security mechanisms on the PC. The flaw in the Sony rootkit grants attackers only the limited power to conceal their own files and programs; the SafeDisc flaw is much more dangerous, allowing attackers to execute unrestricted "kernel-level" code and read or write any area of the hard disk or memory of the PC, thus facilitating the complete compromise of the security of the PC. The flaws in both the rootkit and SafeDisc are exploited by so-called "privilege escalation attacks" and require the attacker to first gain *some* access to the PC.

[20] *See* Joel Hruska, *Windows Install Base to Break One Billion in 2008*, ARS TECHNICA (Jul. 28, 2007), *available at* http://arstechnica.com/journals/microsoft.ars/2007/07/28/windows-install-base-to-break-one-billion-in-2008.

Serving as another prominent example of this kind of TPM is Sony's SecuROM software, utilized by dozens of high-profile video game publishers including Atari, Bethesda Softworks, Capcom, Eidos, Electronic Arts, Konami, LucasArts, Microsoft, Sega, and Ubisoft.[21] PC-accessible video games utilizing SecuROM automatically install copy-protection software, often without the consumer's knowledge. Independent security experts have not yet rigorously studied SecuROM; in the absence of a definitive analysis, anecdotal contentions of harm, speculation about causes, and contradictory assessments of risk have run wild on the Internet. While Sony maintains that the TPM is safe[22], some users report that it disables critical system security functionality including firewalls and antivirus software, opening their PCs to a variety of viruses, spyware, and other malware.[23] Three class action lawsuits have been filed against Electronic Arts on behalf of those allegedly negatively affected by the inclusion of SecuROM in the popular video games *Mass Effect*[24], *Spore*[25], and *Spore Creature Creator*[26].

Whether or not SecuROM causes actual security vulnerabilities, the uncertainty about its risks has created an environment of suspicion where consumers fear the worst.[27] Given the immense stakes that users hold in the security of their PCs – private communications, valuable data, and even financial assets vulnerable to theft and fraud – the presumption that SecuROM is insecure may be a rational decision to err on the side of caution. Yet, consumers who bought SecuROM-encumbered games unaware of the potential risks are now placed between a rock and a hard place, forced to choose between accepting the indeterminate risks posed by SecuROM and abandoning access to their lawfully obtained video games. This is an unacceptable proposition for consumers.

Furthermore, the SafeDisc and SecuROM fiascos showcase the very real chilling effect of the DMCA anti-circumvention measures on security research related to these TPMs. Even though SafeDisc exposed hundreds of millions of PCs to a serious security vulnerability, over six years passed after the release of the TPM until anyone but attackers knew about the vulnerability, which was not publicly documented until a security

---

[21] *Securom [sic] Affected Games*, RECLAIM YOUR GAME! (Nov. 11, 2008), *available at* http://reclaimyourgame.com/index.php?option=com_content&view=article&id=45&Itemid=11.
[22] *See SecuROM™ Frequently Asked Questions*, *available at* http://www.securom.com/support_faq.asp ("SecuROM™ does not damage a computer in any way. Great care has been taken to make sure the SecuROM™ system is sound and compatible.")
[23] *See Thomas v. Electronic Arts, Inc.* fn. 1 (N.D. Cal., Sept. 22, 2008), *available at* http://www.courthousenews.com/2008/09/23/Spore.pdf.
[24] *Gardner v. Electronic Arts, Inc.* (N.D. Cal., Oct. 6, 2008), *available at* http://www.courthousenews.com/2008/10/08/MassEffect.pdf.
[25] *Thomas*, *supra* note 22.
[26] *Eldridge v. Electronic Arts, Inc.* (N.D. Cal., Oct. 14, 2008), *available at* http://docs.justia.com/cases/federal/district-courts/california/candce/3:2008cv04733/208019/1/.
[27] *See* anonymous user "Faceless Clock," *Anti-DRM Revolt Strikes Amazon Reviews*, BLOGCRITICS MAGAZINE (Nov. 12, 2008), *available at* http://blogcritics.org/archives/2008/11/12/183314.php.

researcher observed a piece of malware exploiting it[28]. And the ongoing uncertainty over SecuROM's safety could probably be settled by a single definitive scientific study; instead, a regime of panic, protests, and litigation has taken hold over what may turn out to be nonexistent or easily reparable faults.

Despite the high stakes, security researchers have clearly avoided addressing these problems, and the chilling effect of the DMCA anti-circumvention provisions is at least partially to blame. Security researchers remain the last defense against dangerous security flaws caused by TPMs, and discouraging their intervention is completely undesirable. Accordingly, an exemption to the anti-circumvention measures is needed to allow security researchers to investigate and fix security flaws caused by TPMs on PC-accessible video games, and for consumers to apply those fixes to access their lawfully obtained games.

A growing body of evidence suggests an inherent tension between digital rights management ("DRM") technology embodied by these TPMs and user security[29]. Accordingly, we can confidently predict that the Sony rootkit, SafeDisc, and SecuROM will not be the last TPMs to cause collateral security harm. The exemption of Class 2 from the anti-circumvention measures should be adequate to mitigate the harms caused by TPMs that control access to PC-accessible video games because it will remove the chilling effect of the anti-circumvention measures, thereby encouraging independent researchers to investigate and correct security flaws in these TPMs and allowing users to stay informed and take appropriate measures to protect themselves.

However, potentially dangerous TPMs will likely be used on many other PC-accessible works between now and the next rulemaking procedure in 2012. To wit, TPMs are being used (or are planned for use) on ebooks[30] and digitally distributed multimedia content[31]. The continued use of flawed TPMs in the aftermath of the Sony rootkit fiasco indicates that the risk of harming consumers is unlikely to provide the content industry with sufficient incentive to be diligent about security, and those consumers should not be forced to wait years to gain secure access to their lawfully obtained works. Accordingly, an

---

[28] Elia Florio, *Privilege Escalation Exploit in the Wild*, SYMANTEC FORUMS (October 16, 2007), available at https://forums.symantec.com/syment/blog/article?message.uid=305541.

[29] *See* discussion *infra* Part IV(B).

[30] Adobe plans to establish a de facto industry standard for ebook DRM. Bill McCoy, *Point-Counterpoint: Digital Book DRM, the Least Worst Solution*, O'REILLY TOC (Nov. 24, 2008), *available at* http://toc.oreilly.com/2008/11/an-industry-standard-digital-b.html.

[31] Netflix is using Microsoft Silverlight digital rights management (DRM) technology to protect its video streams. Joshua Topolsky, *Netflix Finally Brings 'Watch Instantly' to Macs Via Silverlight*, ENGADGET (Oct. 26, 2008), *available at* http://www.engadget.com/2008/10/26/netflix-finally-brings-watch-instantly-to-macs-via-silverlight/. YouTube and Hulu use Adobe Flash technology, which is now capable of encrypting video streams, thus bringing security research thereof under the purview of the DMCA. Kevin Towes, *Encryption and Streaming Media Protection to Adobe Flash*, FLASH MEDIA BLOG (Sept. 28, 2008), *available at* http://blogs.adobe.com/ktowes/2008/09/encryption_and_streaming_media_1.html.

exemption of Class 1 from the anti-circumvention measures is needed to prospectively allow security researches to discover and fix security flaws in other PC-accessible works before attackers find and exploit these flaws against consumers.

IV. Nature and Operation of the Access-Controlling Technological Measures

This section describes the technological measures that control access to the proposed classes of works and the manner of operation of the measures.

A. PC-accessible Video Games (Class 2)

Over the history of PC video games, publishers have relied extensively on the use of access controls to prevent unauthorized copying. Early video games contained simple serial numbers in the packaging that needed to be entered in order to install the games; many contained gameplay-based puzzles unsolvable without information in the included user manual[32]. With the rise of the Internet and the growth of sophisticated hacking techniques, these controls were considered no longer sufficient to control access to the games; serial numbers and information from user manuals could simply be distributed over the network, or internal protection measures could simply be bypassed. Publishers responded with video games that "phoned home," checking with a server operated by the publisher to ensure that the software was licensed, as well as controls to prevent discs from being copied. These controls were quickly and widely circumvented as well.

Frustrated by these technological changes, the video game industry has followed Sony's rootkit lead, responding with new, more aggressive TPMs to control access to their games. These TPMs, of which SafeDisc and SecuROM are well-known examples, tend to operate approximately as follows: When a user attempts to install a video game, a hidden computer program is surreptitiously installed along with the game.[33] The program is installed with elevated privileges, giving it unfettered access to the rest of the PC[34] to carry out DRM tasks such as authenticating discs, enforcing access policies, and taking countermeasures against circumvention tools.

TPMs like these may prevent users from accessing their games in ways that are unquestionably legal under (and largely unregulated by) the Copyright Act.[35] Even worse, these TPMs may cause problems with other subsystems of the user's PC. For example, SecuROM reportedly may interfere with the operation of a PC's CD and DVD burners and

---

[32] A famous example is found in *The Secret of Monkey Island*, the seminal 1990 LucasArts adventure game that halts the adventures of the winsome pirate Guybrush Threepwood until the user enters the correct code from the enclosed "*Dial-A-Pirate"* code wheel included in the game box. *See The Secret of Monkey Island*, THE MONKEY ISLAND SCUMM BAR, *available at* http://www.scummbar.com/games/index.php?game=1&sub=media&todo=7; *see also* image *infra* at Ex. A, Fig. 1.

[33] *See Eldridge* at 10 ¶ 13.

[34] *Id.* at 10 ¶ 14.

[35] *See infra* Part V(A)(2).

several software programs[36]; some users even claim that SecuROM can even interfere with virus and firewall protection software[37], opening a serious hole in the defenses of the PC.

Unfortunately, the video game publishers using these TPMs profess ignorance about the security risks posed by the TPMs.[38] Ironically mimicking a Sony officer's initial comments about the rootkit fiasco[39], Electronic Arts CEO John Riccitiello confidently claimed that "99.8% percent of users *wouldn't notice* [the TPMs]," [40] a statement that, if true, *highlights* the need for independent security researchers to act quickly to inform and protect innocent, unknowing, and at-risk consumers, most of whom are ill-equipped to defend against the security risks posed by the TPMs. Even when acknowledging problems with the TPMs, video game publishers have merely loosened usability restrictions[41] and failed to address security risks.

While it is impossible to predict what vulnerabilities will be discovered next in PC video games, the continued adoption of TPMs like SafeDisc and SecuROM makes it inevitable that new vulnerabilities *will* be discovered over the present rulemaking period[42]. Less certain is who will discover these vulnerabilities first. Without the exemption of either of the proposed classes, it is likely to be malicious attackers unconcerned with potential suit under the DMCA, and not legitimate security researchers chilled by the anti-circumvention measures. Accordingly, the proposed exemption of Class 2 is the bare minimum necessary to both cure present, ongoing problems and prevent future harms with video games, as required by the NOI.[43] However, the proposed exemption of Class 1, described in the following subsection, would better enable the noninfringing uses described hereinafter.

---

[36] *See Eldridge* at 13-15 ¶¶ 20-22.
[37] *See Thomas* fn. 1.
[38] *See SecuROM™ Frequently Asked Questions*, *available at* http://www.securom.com/support_faq.asp ("SecuROM™ does not damage a computer in any way. Great care has been taken to make sure the SecuROM™ system is sound and compatible.") (hereinafter "SecuROM FAQ").
[39] Then-Sony BMG Global Digital Business Division President Thomas Hesse pondered, "Most people, I think, don't even know what a rootkit is, so why should they care about it?" Orlowski, *supra* note 14.
[40] David Kaplan, *EA's Ricciteliello: Last Year for 'Offline-Only' Games*, YAHOO! FINANCE (Oct. 14, 2008), *available at* http://biz.yahoo.com/paidcontent/081014/1_328572_id.html?.v=1
[41] *E.g.*, Eric Caoili, *EA Loosens Spore's DRM, Account Restrictions*, GAMASUTRA (Sept. 19, 2008), *available at http://www.gamasutra.com/php-bin/news_index.php?story=20322*.
[42] For example, Blizzard, the creator of the popular *World of Warcraft* series, intends to use SecuROM-esque measures in several upcoming games. *See* Earnest Cavalli, *Q&A: Blizzard CEO Mike Morhaime on DRM, WoW and the Next MMO,* WIRED BLOG NETWORK (October 16, 2008), *available at* http://blog.wired.com/games/2008/10/qa-blizzard-ceo.html.
[43] *See NOI*, *supra* note 1 at 58077.

B. PC-accessible Literary Works, Sound Recordings, and Audiovisual Works (Class 1)

As detailed in the previous subsection and in the initial comment preceding the Sound Recordings Exemption[44], TPMs such as the Sony rootkit and SafeDisc have caused extensive security risks to consumers, and the content industry seems to show little hesitation toward the continued adoption of DRM technologies[45] embodied by these TPMs. However, many security researchers now believe that the Sony rootkit and SafeDisc fiascos are just the tip of the iceberg, merely highlighting security issues that are endemic to all DRM technology.

Researchers have already begun to document the fact that DRM inherently tends to give rise to security vulnerabilities. According to noted security expert Bruce Schneier, "[t]here is an inherent insecurity to technologies that try to own people's computers: [t]hey allow individuals other than the computers' legitimate owners to enforce policy on those machines. These systems invite attackers to assume the role of the third party and turn a user's device against him."[46] This is neither a tentative nor uncertain conclusion in the security field; for example, Schneier's academic colleagues Joan Feigenbaum, Michael Freedman, Tomas Sander, and Adam Shostack pointed out that, "[a]t the risk of stating the obvious, . . . there can be inherent tension between the copyright-enforcement goals of owners and distributors who deploy DRM systems and the privacy goals of users."[47]

The security problems surrounding DRM technology stem from its inherent complexity. Computer scientist Steve Bellovin notes that while "DRM may not be evil[, i]t is, however, very, very complex, and, historically, complexity has led to insecurity."[48] Risky software engineering practices behind DRM technology are also to blame. Programmer Ken Johnson states that "[m]ost DRM technologies tend to use unsupported and/or 'fringe' techniques to make themselves difficult to understand and debug. However, more often than not, the DRM authors often get little things wrong with their anti-debug/anti-hack implementations, and when you're running in a privileged space, 'little things wrong' can translate into a security vulnerability. . ."[49]

---

[44] Edward W. Felten and J. Alex Halderman, *Comment Re: RM 2005-11* (Dec. 1, 2005), *available at* http://www.copyright.gov/1201/2006/comments/mulligan_felten.pdf [hereinafter *Sony Rootkit Comment*].

[45] *See infra* note 23.

[46] *Everyone Wants to 'Own' Your PC*, WIRED (May 4, 2006), *available at* http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70802.

[47] *Privacy Engineering for Digital Rights Management Systems* (2001), *available at* http://www.cs.yale.edu/homes/jf/FFSS.pdf.

[48] *DRM, Complexity, and Correctness*, IEEE SECURITY AND PRIVACY 80 (Feb. 2007), *available at* http://www.cs.columbia.edu/~smb/papers/04085601.pdf.

[49] *Invasive DRM Systems are Dangerous from a Security Perspective*, NYNAEVE: ADVENTURES IN WINDOWS DEBUGGING AND REVERSE ENGINEERING (Nov. 6, 2007), *available at* http://www.nynaeve.net/?p=193. Johnson concludes that "This is one of the reasons why I personally am extremely wary of playing games that require administrative privileges or install administrative 'helper services' for non-administrative users, because games have a

The inherent connection between DRM and security vulnerabilities is a centerpiece of Professor Halderman's research, and indeed, is one of the most significant themes developed in his dissertation. For example, his investigation into the Sony rootkit fiasco led him to conclude that "[b]y looking carefully at CD copy-protection as a technical problem, we can see why DRM designers are drawn to spyware tactics as their best hope of halting copying. . . . From a nontechnical viewpoint, Sony-BMG's experience has much to teach the music industry. The most important lesson is that DRM can have serious side effects, especially relating to security and privacy."[50] In another paper, Professor Halderman noted that "there can be an inverse relation between the efficacy of DRM and the user's ability to defend her computer from unrelated security and privacy risks. The user's best defense is rooted in understanding and controlling which software is installed, but many DRM systems rely on undermining this understanding and control."[51]

Despite the inherent connection between DRM and security vulnerabilities, we are quite sensitive to the rights of copyright owners under the DMCA to protect their copyrighted works with TPMs, and respect the Librarian's necessarily narrow interpretation of his rulemaking authority. Accordingly, and although we would prefer to see a blanket security research exemption to the DMCA,[52] we have limited Class 1 to focus narrowly on the circumstances in which the connections between DRM and security vulnerabilities are best documented.

We have narrowed the scope of Class 1 in two critical ways. First, Class 1 includes only works accessible on personal computers. By personal computers, we mean *general purpose* personal computers, and exclude dedicated and specialized hardware like stand-alone video game playing machines, dedicated eBook readers, and non-PC CD and DVD players, as security vulnerabilities are worst when they infect general-purpose, generative machines like PCs[53].

Second, Class 1 is restricted to three specific categories of copyrighted works: literary works, sound recordings, and audiovisual works. Thus, the proposed exemption

---

high incidence of including low quality anti-cheat/anti-hack/anti-copying system nowadays. I simply don't trust the people behind these systems to get their code right enough to be comfortable with it running with full privileges on my box." *Id.*

[50] Edward W. Felten and J. Alex Halderman, *Digital Rights Management, Spyware, and Security*, IEEE SECURITY AND PRIVACY 21-22 (Feb. 2006), *available at* http://www.cse.umich.edu/~jhalderm/pub/papers/drm-sp06.pdf.

[51] J. Alex Halderman and Edward W. Felten, *Lessons from the Sony CD DRM Episode* (2006), *available at* http://www.cse.umich.edu/~jhalderm/pub/papers/rootkit-sec06.pdf.

[52] Of course, 17 U.S.C. § 1201(j) provides a security exemption of questionable applicability, as discussed extensively during the third rulemaking. For the reasons articulated during those discussions, 1201(j) may provide insufficient protection for security researchers.

[53] *See generally* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT (2008) (defining and discussing generativity).

would not apply to TPMs that restrict access solely to choreographic works[54], pictorial, graphic, and sculptural works[55], or architectural works[56], for example.[57] This reflects the fact that the past evidence of harm has been encountered with TPMs regulating access to literary works (such as computer programs), audiovisual works (video games[58]), and sound recordings (audio CDs).

While it is again impossible, as with PC video games, to predict what vulnerabilities will be discovered next in PC-accessible literary works, sound recordings, and audiovisual works, it is inevitable that new vulnerabilities *will* be discovered over the present rulemaking period, and certain that the DMCA will chill security researchers from discovering them without the exemption of Class 1. Accordingly, and although the proposed exemption of Class 2 would be welcomed and appreciated, the proposed exemption of Class 1 is necessary to both cure present, ongoing problems and prevent future harms with the aforementioned PC-accessible works, as required by the NOI.[59]

V. Legal Arguments in Support of the Requested Exemption

This section first describes the noninfringing uses at issue, then analyzes the proposed classes in the context of the statutory considerations enumerated in 17 U.S.C. § 1201(a)(1)(C).

A. The Prevented Noninfringing Activities

In the third rulemaking, the Register of Copyrights refined her approach to defining acceptable classes of works. Inspired by a proposal narrowly tailored to film and media studies professors, the Register recommended, and the Librarian ruled, that classes of works may be tailored to "particular uses or users."[60] We agree that this rule is sound, in particular because it ensures that proposed exemptions do not swallow the DMCA or exceed the Librarian's rulemaking authority. For this reason, we have narrowed our proposed classes precisely as the Register did in the last round with respect to sound recordings, limiting them to circumvention "accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities."

Accordingly, we enumerate in this section two noninfringing uses of the proposed classes of works adversely affected by the previously described TPMs: (1) engaging in good

---

[54] 17 U.S.C. § 102(a)(4).
[55] 17 U.S.C. § 102(a)(5).
[56] 17 U.S.C. § 102(a)(8).
[57] Class 1 would, however, apply to TPMs restricting access to literary works, audiovisual works, and sound recordings that also embody other works (such as choreographic works, pictorial, graphic, and sculptural works, or architectural works).
[58] As previously mentioned, video games may also embody literary works, audiovisual works, and sound recordings.
[59] *See NOI*, *supra* note 1 at 58077.
[60] *FR*, *supra* note 7 at 68474.

faith computer security research, and (2) installing and utilizing the works. Furthermore, each use requires the access-protected copy of the work, an essential element for an exemption under the NOI[61], because alternative, unprotected formats are either unavailable, insufficiently functional to serve as substitutes, or inherently incapable of facilitating the use. These uses are the same or substantially similar for both proposed classes of works, except as noted otherwise.

1. Engaging in Good Faith Computer Security Research

The chilling effects of the DMCA prevent legitimate security researchers from circumventing the TPMs placed on PC-accessible literary works (including video games), sound recordings, and audiovisual works to discover, document, and fix security flaws in good faith. This increases the likelihood that attackers will find flaws first and leaves consumer protection to anonymous researchers who are forced to release their work under the digital cover of darkness, depriving many consumers of the full value of the fixes and preventing legitimate academic publication and discussion of the flaws. This is not merely a concern for academic researchers, as an entire industry of professional security researchers, including those who work for antivirus and anti-spyware firms and specialize in finding and correcting vulnerabilities, is similarly chilled from investigating these TPMs.

Engaging in security research on the proposed classes of works is a noninfringing use under copyright law. Much of the research involves the same activities required to install and use the works, which, as discussed below, do not implicate any of the copyright holder's reproduction or adaptation rights of copyright holders under 17 U.S.C. 106(1)-(2) and, alternatively, are licensed by the game publishers and also explicitly allowed under 17 U.S.C. § 117(a)(1).

Even when unlicensed, this type of security research is almost certain to constitute a legal fair use under 17 U.S.C. § 107. Section 107 enumerates four nonexclusive factors for determining whether a particular use is fair: (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.

a. PURPOSE AND CHARACTER OF THE USE

The purposes of the intended use in question are research, scholarship, and teaching, all listed as model fair uses in the preamble to Section 107.[62] Furthermore, the discovery and disclosure of security vulnerabilities is closely analogous to criticism and commentary, two other model fair uses listed in the preamble. The listing of a use in the

[61] *See NOI*, *supra* note 1 at 58077.
[62] The Supreme Court noted that a fair use analysis "may be guided by the examples given in the preamble of § 107. . . ." *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 578 (1994).

preamble to Section 107 weighs the first factor heavily in favor of a determination of fair use.[63]

b. NATURE OF THE WORKS

The nature of the works in question runs the gamut from purely factual (e.g., nonfictional ebooks) to purely creative (e.g., video games); thus, a generalized analysis under the second factor is impossible to perform.[64] However, several courts have held computer programs and video games to be entitled to a lower degree of protection than more traditional literary works because they generally "contain unprotected aspects that cannot be examined without copying."[65] Therefore, the second factor is likely weighted toward a determination of fair use.

c. AMOUNT AND SUBSTANTIALITY OF THE USE

Although security researchers often must install the works in question in their entirety in order to test them for vulnerabilities, such installation is usually licensed and therefore irrelevant to the third factor. More relevant is the amount and substantiality of the copyrighted work *used* by the security researcher which, in most cases, is little to none. Security researchers generally focus their attention on the TPM, not the underlying protected work. In other words, researchers dissect, scrutinize, and manipulate the lock, not what is protected by the lock. Accordingly, the third factor is likely weighted toward a determination of fair use.

d. MARKET EFFECT OF THE USE

As discussed further below[66], successful security research is likely to *increase* market demand for a work by ameliorating consumer uncertainty surrounding the security of the work. Likewise, the detection and responsible mitigation of a security vulnerability in a work will likely give consumers an ongoing confidence in the publisher of the work, further enhancing the market attractiveness of the work. The revelation of security flaws research may have a negative effect on the market for the work if the publisher refuses to fix the flaws. However, this market effect of security research is directly analogous to that of a vicious parody or successful criticism and thus irrelevant to the fourth factor.[67]

---

[63] *See, e.g.*, *Marcus v. Rowley*, 695 F.2d 1171, 1175 (9th Cir. 1983).
[64] The Supreme Court has held that, "[i]n general, fair use is more likely to be found in factual works than in fictional works." *Stewart v. Abend*, 495 U.S. 207, 237 (1990).
[65] *E.g., Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596, 603 (9th Cir. 2000); *Sega Enters. v. Accolade, Inc.*, 977 F.2d 1510, 1526 (9th Cir. 1992).
[66] *See* discussion *infra* Part V(B)(4).
[67] *See Campbell*, 510 U.S. at 591-92 ("[W]hen a lethal parody, like a scathing theater review, kills demand for the original, it does not produce a harm cognizable under the Copyright Act. . . . 'Parody may quite legitimately aim at garroting the original, destroying it commercially as well as artistically . . . .'" (quoting BENJAMIN KAPLAN, AN UNHURRIED VIEW OF COPYRIGHT 69 (1967)).

Because each of the factors enumerated under Section 107 is weighted in favor of fair use, a determination of fair use is almost certain.

Finally, security research inherently requires the use of the access-controlled works, as any security flaws in the access-controlled works may not be present on any alternate formats, if any such formats even exist. Accordingly, no alternate means exists to engage in this noninfringing use.

2. Installation and Utilization

In the present-day security ecosystem, the publishers of PC-accessible works cannot, practically speaking, eliminate all exploitable security flaws from their products. Thus, PC users must rely on academic and industrial security researchers to root out, publicize, and fix security vulnerabilities. However, research on an entire class of vulnerabilities (those associated with TPMs that effectively control access to copyrighted works) has been rendered much riskier and more difficult by the DMCA. With researchers turning their attention elsewhere, the ecosystem has broken down, leaving PCs less reliable and less secure.

As the content industry continues to embrace TPMs laden with security vulnerabilities, and as researchers continue to be chilled from investigating them, consumers have begun to trust content less. In the extreme, a consumer will choose not to install (if necessary) and use a lawfully obtained, TPM-protected work on her PC because of security risks (whether actual or potential). Thus, the TPM will indirectly interfere with her right to install and utilize the content.

There is ample proof that this has already happened in the context of the SafeDisc and Sony rootkit[68] fiascos, and that it is happening now with SecuROM[69]. Without the proposed exemptions, PC users will continue to be stuck with the unpalatable decision of either risking the security of their PCs or being denied access to use their lawfully obtained content.

Furthermore, the installation and ordinary use of lawfully obtained PC-accessible literary works (including video games), sound recordings, and audiovisual works constitute a noninfringing use of the works under copyright law. Copying files and code underlying a work to a user's random-access memory ("RAM") and hard drive as necessary to install and utilize the work does not implicate any of the copyright holder's reproduction or adaptation rights under 17 U.S.C. § 106(1)-(2), and even assuming *arguendo* that it does,

---

[68] *See generally Sony Rootkit Comment*, *supra* note 43.

[69] *See* Staci D. Kramer, *EA Admits Spore Launched Botched by DRM; Still, Financial Damage Already Done*, THE WASHINGTON POST VIA PAIDCONTENT.ORG (September 19, 2008), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/09/19/AR2008091900129.html ("Buyers worry that [Spore's] SecuROM software is actually installing spyware on their machines.").

making of new copies or adaptations of the works as necessary to install and utilize them is usually licensed by their publishers and also explicitly permitted under 17 U.S.C. § 117(a)(1). Furthermore, no other exclusive rights under section 106 are implicated: in particular, no other copies are made or disturbed; no other derivative works are prepared; and no works are publicly performed, displayed, or transmitted.

The access-protected copies of the works provide the only way for most consumers to engage in the installation and utilization of the works. Many works protected with technological measures such as SecuROM are distributed solely in a format exclusively compatible with the Microsoft Windows operating system. While some works may be available in alternate formats, such as those compatible with other PC operating systems, cellular telephones, or television video game systems, these alternate formats tend to vary widely from the original format in terms of functionality and reliability[70], and may force the consumer to invest hundreds or even thousands of dollars in a new PC, operating system, or video game system and compatible television simply to install and use a comparatively inexpensive work. Accordingly, an alternate means of engaging in this noninfringing use either does not exist or is an insufficient substitute for accomplishing the use due to lack of functionality or prohibitive expense, depending on the particular work.

B. Statutory Considerations

17 U.S.C. § 1201(a)(C) requires the Librarian to consider 1) the availability for use of copyrighted works; 2) the availability for use of works for nonprofit archival, preservation, and educational purposes; 3) the impact that the prohibition has on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research; 4) the effect of circumvention of technological measures on the market for or value of copyrighted works; and 5) such other factors as the Librarian considers important. In this section, we address each factor in turn as applied to the proposed classes. Except where noted, the factors apply in the same or substantially similar ways to both proposed classes; while examples are given primarily in the context of Class 2, we believe it is clear that, based on the aforementioned trend toward the broad adoption of TPMs with security flaws, similar examples will arise in the wider context of Class 1.

1. Availability for Use of Copyrighted Works

The proposed exemption will likely have a positive effect on the availability of the copyrighted works at issue. Despite critical acclaim for the works at issue[71], a significant

---

[70] *See, e.g.*, David Clayman, *Head-to-Head: Fallout 3*, IMAGINE GAMES NETWORK (Nov. 3, 2008), *available at* http://xbox360.ign.com/articles/926/926646p1.html (in *seven* pages, detailing the differences between the four versions of Fallout 3, a Bethesda Softworks game, the PC version of which is encumbered with SecuROM).

[71] See Spore; METACRITIC.COM, available at http://www.metacritic.com/games/platforms/pc/spore?q=spore ("84[/100]," "Generally favorable reviews"); Mass Effect, METACRITIC.COM, available

number of consumers have been dissuaded from purchasing the works because of the aforementioned security risks[72]. In other words, the technological measure has the effect of lowering legitimate sales, as opposed to its intended effect of lowering piracy.[73]

If the proposed exemption is passed, security researchers are likely to devote considerable time and resources toward investigating SecuROM and similar TPMs, identifying security flaws and devising solutions as they did for the Sony rootkit. Careful study of TPM security flaws may reveal causative or contributory factors common to all TPMs that could help their designers eliminate future problems. Moreover, the transparent environment would incentivize content publishers to fund the creation of TPMs that respect the security interests of consumers while protecting copyright interests. Eventually, researchers could certify the security of TPMs, thus helping to convince consumers of the safety of those works encumbered with TPMs and thereby increasing the potential for legitimate sales.

2. Availability for Use of Works for Non-Profit Archival, Preservation, and Educational Purposes

After a TPM-encumbered, PC-accessible work is released, security risks are likely to increase over time as new problems are found. Unfortunately, the motivation of the publisher of the work to mitigate the risks is based primarily on the economic return of selling more copies of the work. As soon as the cost of fixing security flaws exceeds the potential profits of increased sales, the publisher is likely to stop releasing fixes. Alternatively, the publisher could simply go out of business. However, the unfixed security flaws leave consumers still using the work vulnerable to attack. Thus, using such a work safely in the long run will require some unofficial method of correcting security flaws. Without an exemption to the DMCA to allow security researchers to continue to investigate works that are no longer supported by their publishers yet still prevalent in the wild, the use of older works will become increasingly fraught with security risks.

---

athttp://www.metacritic.com/games/platforms/pc/masseffect?q=mass%20effect ("89[/100]," "Generally favorable reviews").

[72] One estimate puts Electronic Arts' lost sales revenue on Spore due to SecuROM as high as $25 million, which equates to approximately 500,000 users. *See* Kramer, *supra* note 68.

[73] Some commentators argue that TPMs like SecuROM actually *increases* piracy. *How EA and Spore Are Causing Piracy, the DasmX86Dll Issues, Removing SecuROM and Some Great DRM Free [sic] Alternatives*, ARSGEEK (Sept. 9, 2008), *available at* http://www.arsgeek.com/2008/09/09/how-to-remove-securom-spore-dasmx86dll-issues-and-some-great-drm-free-alternatives/. To wit, some DRM-free games appear to suffer from slightly lower piracy rates than their encumbered bretheren. *See* Seán Byrne, *DRM-free Games No Worse Off With Piracy*, CDFREAKS.COM (Nov. 18, 2008), *available at* http://www.cdfreaks.com/news/15216-DRM-free-games-no-worse-off-with-piracy.html.

3. Impact That the Prohibition Has on the Circumvention of Technological Measures Applied to Copyrighted Works Has On Criticism, Comment, News Reporting, Teaching, Scholarship, or Research

Research directed towards exposing security flaws created by TPMs like SafeDisc, SecuROM, and the Sony rootkit often involves activities that could expose the researchers to the threat of suit under the DMCA. This potential exposure has a chilling effect on the pace and scope of research in this field, without which the identification and mitigation of security risks and related debate, discussion, and scholarship will not occur.

Professor Halderman experienced first hand knowledge of this chilling effect on research and criticism when the manufacturer of insecure technological measures threatened him with a lawsuit prior to the third rulemaking. As was discussed extensively during the hearing, it is unclear that existing statutory preventions[74] provide the legal cover needed by security researchers to perform necessary research without the threat of suit. The time of security researchers would be better spent discovering and fixing security flaws than discussing potential DMCA liability issues with their lawyers.

The prohibition on the circumvention of TPMs on PC-accessible works (including video games) has also adversely impacted teaching. Many university computer science departments offer or are considering offering security courses covering DRM design and operation. Ideally, these courses could train future software engineers to build safer TPMs through immersive, hands-on laboratory components working with TPMs and traditional techniques used by attackers. However, the use of real-world examples of TPMs could give rise to lawsuits or threats thereof under the DMCA. The chilling effect on this important type of teaching and learning is precisely the kind of effect that Congress intended the present rulemaking to alleviate.

4. The Effect of Circumvention of the Technological Measures on the Market For or Value of Copyrighted Works

As under the availability factor, the circumvention of TPMs such as SecuROM is likely to have a *positive* effect on the value of the copyrighted works. For example, much of the criticism of *Spore* was directed not at the artistic merit of the game, but toward SecuROM.[75] In other words, the security risks caused by the TPMs (and the uncertainty about the magnitude of those risks) are likely to have a negative effect on the market for and value of the works. Accordingly, legalizing the good faith investigation and mitigation of those risks is likely to lead to better-informed consumers, fewer TPMs with security flaws, and, accordingly, a positive effect on the market for and value of the works.

Although some copyright owners may believe that TPMs such as SafeDisc, SecuROM, and the Sony rootkit are necessary to profitably distribute PC-accessible works, TPMs

[74] *See* 17 U.S.C. § 1201(i)-(j).
[75] *See, e.g.*, Kris Pigna, *Amazon Users Lash Out Against Spore DRM*, 1UP.COM (Sept. 8, 2008), *available at* http://www.1up.com/do/newsStory?cId=3169804.

laden with security flaws are likely to devalue both the TPMs themselves and the protected works by shaking consumer confidence in the security of the works, particularly when attacks that exploit the flaws are publicized. Because the proposed exemption will increase information about and fixes for security flaws in the TPMs, discourage further use of TPMs with security flaws, and decrease uncertainty about all PC-accessible works, whether or not they are plagued by TPM-enabled security vulnerabilities, the exemption is likely to positively affect the market for and value of video games by restoring consumer confidence in the security of those works.

5. Factors the Librarian May Consider Appropriate

TPMs that protect PC-accessible works pose serious threats to the PCs of consumers. While consumers have been warned for years about the dangers of downloading strange files from the Internet, they did not, until now, have particular reason to fear that content from established publishers could subvert the security of their PCs. Yet, the DMCA casts doubt on the legality of the good faith attempts of security researchers and consumers to rectify the situation. Surely Congress cannot have intended such a result. The DMCA was passed to help protect *legitimate* interests of copyright holders, not to hold security researchers and consumers hostage to security risks. Because of SecuROM and similar TPMs, informed consumers must either forsake access to their lawfully purchased works or face an uncertain level of security risk; uninformed consumers may unknowingly sacrifice security to gain access. This is an untenable predicament.

VI. Conclusion

The proposed classes would allow security researchers and consumers to collectively undertake the necessary measures to maintain both access and security. During the third rulemaking, the Department of Homeland Security laid out a strict edict to the music industry:

> *"It's very important to remember that it's your intellectual property – it's not your computer. And in the pursuit of protection of intellectual property, it's important not to defeat or undermine the security measures that people need to adopt in these days."*[76]

It is essential for the content industry to hear the same call – and to allow independent security researchers to ensure that its teachings are respected by the industry. Thus, we respectfully request that that the Register recommend and the Librarian grant an exemption for Class 1, or, in the alternative, Class 2, from the DMCA anti-circumvention measures.

---

[76] Michael Geist, *Sony's Long-term Rootkit CD Woes*, BBC NEWS (Nov. 21, 2005), *available at* http://news.bbc.co.uk/2/hi/technology/4456970.stm (quoting Stewart Baker, then-assistant secretary of policy for the U.S. Department of Homeland Security).

Sincerely,

/s/

J. Alex Halderman • Blake E. Reid • Paul Ohm • Harry Surden • J. Brad Bernthal

Exhibit A

Fig. 1 – The Secret of Monkey Island "Dial-A-Pirate" Code Wheel[77]

[77] *Available at* http://www.scummbar.com/imageviewer/imageviewer.php?useimage=/games/media/mi12/mi1codewheel.jpg.

Lessons from the Sony CD DRM Episode

J. Alex Halderman and Edward W. Felten
Center for Information Technology Policy
Department of Computer Science
Princeton University

Abstract

In the fall of 2005, problems discovered in two Sony-BMG compact disc copy protection systems, XCP and MediaMax, triggered a public uproar that ultimately led to class-action litigation and the recall of millions of discs. We present an in-depth analysis of these technologies, including their design, implementation, and deployment. The systems are surprisingly complex and suffer from a diverse array of flaws that weaken their content protection and expose users to serious security and privacy risks. Their complexity, and their failure, makes them an interesting case study of digital rights management that carries valuable lessons for content companies, DRM vendors, policymakers, end users, and the security community.

1 Introduction

This paper is a case study of the design, implementation, and deployment of anti-copying technologies. We present a detailed technical analysis of the security and privacy implications of two systems, XCP and MediaMax, which were developed by separate companies (First4Internet and SunnComm, respectively) and shipped on millions of music compact discs by Sony-BMG, the world's second largest record company. We consider the design choices the companies faced, examine the choices they made, and weigh the consequences of those choices. The lessons that emerge are valuable not only for compact disc copy protection, but for copy protection systems in general.

The security and privacy implications of Sony-BMG's CD digital rights management (DRM) technologies first reached the public eye on October 31, 2005, in a blog post by Mark Russinovich [21]. While testing a rootkit detector he had co-written, Russinovich was surprised to find an apparent rootkit (software designed to hide an intruder's presence [13]) on one of his systems. Investigating, he found that the rootkit was part of a CD DRM system called XCP that had been installed when he inserted a Sony-BMG music CD into his computer's CD drive.

News of Russinovich's discovery circulated rapidly on the Internet, and further revelations soon followed, from us,[1] from Russinovich, and from others. It was discovered that the XCP rootkit makes users' systems more vulnerable to attacks, that both CD DRM schemes install risky software components without obtaining informed consent from users, that both systems covertly transmit usage information back to the vendor or the music label, and that none of the protected discs include tools for uninstalling the software. (For these reasons, both XCP and MediaMax seem to meet the consensus definition of spyware.) These and other findings outraged many users.

As the story was picked up by the popular press and public pressure built, Sony-BMG agreed to recall XCP discs from stores and to issue uninstallers for both XCP and MediaMax, but we discovered that both uninstallers created serious security holes on users' systems. Class action lawsuits were filed soon after, and government investigations were launched, as Sony-BMG worked to repair relations with its customers.

While Sony-BMG and its DRM vendors were at the center of this incident, its implications go beyond Sony-BMG and beyond compact discs. Viewed in context, it is a case study in the deployment of DRM into a mature market for recorded media. Many of the lessons of CD DRM apply to other DRM markets as well.

Several themes emerge from this case study: similarities between DRM and malicious software such as spyware, the temptation of DRM vendors to adopt malware tactics, the tendency of DRM to erode privacy, the strategic use of access control to control markets, the failure of ad hoc designs, and the force of differing incentives in shaping behavior and causing conflict.

Outline The remainder of the paper is structured as follows. Section 2 discusses the business incentives of

record labels and DRM vendors, which drive their technology decisions. Section 3 gives a high-level technical summary of the systems' design. Sections 4–9 each cover one aspect of the design in more detail, discussing the design choices made in XCP and MediaMax and considering alternative designs. We discuss weaknesses in the copy protection schemes themselves, as well as vulnerabilities they introduce in users' systems. We cover installation issues in Section 4, recognition of protected discs in Section 5, player software in Section 6, deactivation attacks in Section 7, uninstallation issues in Section 8, and compatibility and upgrading issues in Section 9. Section 10 explores the outrage users expressed in response to the DRM problems. Section 11 concludes and draws lessons for other systems.

2 Goals and Incentives

The goals of a CD DRM system are purely economic: the system is designed to protect and enable the business models of the record label and the DRM vendor. Accordingly, any discussion of goals and incentives must begin and end by talking about business models. The record label and the DRM vendor are separate actors whose interests are not always aligned. Incentive gaps between the label and the DRM vendor can be important in explaining the design and deployment of CD DRM systems.

2.1 Record Label Goals

We first examine the record label's goals. Though the label would like to keep the music from the CD from being made available on peer-to-peer (P2P) file sharing networks, this goal is not feasible [4]. If even one user can rip an unprotected copy of the music and put it on a P2P network, it will be available to the whole world. In practice, every commercially valuable song appears on P2P networks immediately upon release, if not sooner. No CD DRM system can hope to stop this. Real systems do not appear designed to stop P2P sharing, but seem aimed at other goals.[2]

The record label's goal must therefore be to retard disc-to-disc copying and other local copying and use of the music. Stopping local copying might increase sales of the music—if Alice cannot copy a CD to give to Bob, Bob might buy the CD himself.

Control over local uses can translate into more revenue for the record label. For example, if the label can control Alice's ability to download music from a CD into her iPod, the label might be able to charge Alice an extra fee for iPod downloads. Charging for iPod downloads creates new revenue, but it also reduces the value to users of the original CD and therefore reduces revenue from CD sales. Whether the new revenue will outweigh the loss of CD revenue is a complex economic question that depends on detailed assumptions about users' preferences; generally, increasing the label's control over uses of the music will tend to increase the label's profit.

Whether the label would find it more profitable to control a use, as opposed to granting it for free to CD purchasers, is a separate question from whether copyright law gives the label the right to file lawsuits relating to that use. Using DRM to enforce copyright law exactly as written is almost certainly not the record label's profit-maximizing strategy.

Besides controlling use of the music, CD DRM can make money for the record label because it puts software onto users' computers, and the label can monetize this installed platform. For example, each CD DRM album includes a special application for listening to the protected music. This application can show advertisements or create other promotional value for the label; or the platform can gather information about the user's activities, which can be exploited for some business purpose. If taken too far, these become spyware tactics; but they may be pursued more moderately, even over user objections, if the label believes the benefits outweigh the costs.

2.2 DRM Vendor Goals

The CD DRM vendor's primary goal is to create value for the record label in order to maximize the price the label will pay for the DRM technology. In this respect, the vendor's and label's incentives are aligned.

However, the vendor's incentives diverge from the label's in at least two ways. First, the vendor has a higher risk tolerance than the label, because the label is a large, established business with a valuable brand name, while the vendor (at least in the cases at issue here) is a start-up company with few assets and not much brand equity. Start-ups face many risks already and are therefore less averse to taking on one more risk. The record label, on the other hand, has much more capital and brand equity to lose if something goes horribly wrong. Accordingly, we can expect the vendor to be much more willing to accept security risks than the label.

The second incentive difference is that the vendor can monetize the installed platform in ways the record label cannot. For example, once the vendor's DRM software is installed on a user's system, the software can control use of other labels' CDs, so a larger installed base makes the vendor's technology more attractive to other labels. This extra incentive to build the installed base will make the vendor more aggressive about pushing the software onto users' computers than the label would be.

In short, incentive differences make the vendor more likely than the label to (a) cut corners and accept security risks, and (b) push DRM software onto more users'

computers. If the label had perfect knowledge about the vendor's technology, this incentive gap would not be an issue—the label would simply insist that the vendor protect the label's interests. But if, as seems likely in practice, the label has imperfect knowledge of the technology, then the vendor will sometimes act against the label's interests. (For a discussion of differing incentives in another content protection context, see [9].)

2.3 DRM and Market Power

DRM affects more than just the relationships among the label, the vendor, and the user. It also impacts the label's and vendor's positions in their industries, in ways that will shape the companies' DRM strategies.

For example, DRM vendors are in a kind of standards war—a company that controls DRM standards has power to shape the online music business. DRM vendors fight this battle by spreading their platforms widely. Record labels want to play DRM vendors off against each other and prevent any one vendor from achieving dominance.

Major record companies such as Sony-BMG are parts of larger, diversified companies, and can be expected to help bolster the competitive position of their corporate siblings. For example, parts of Sony sell portable music players in competition with Apple, so Sony-BMG has an incentive to take steps to weaken Apple's market power.

Having examined the goals and motivations of the record labels and DRM vendors, we now turn to a description of the technologies they deployed.

3 CD DRM Systems

CD DRM systems must meet difficult requirements. Copy protected discs must be reasonably compliant with the CD Digital Audio standard so that they can play in ordinary CD players. They must be unreadable by almost all computer programs in order to prevent copying, yet the DRM vendor's own software must be able to read them in order to give the user some access to the music.

Most CD DRM systems use both passive and active anti-copying measures. Passive measures change the disc's contents in the hope of confusing most computer drives and software, without confusing most audio CD players. Active measures, in contrast, rely on software on the computer that actively intervenes to block access to the music by programs other than the DRM vendor's own software.

Active protection software must be installed on the computer somehow. XCP and MediaMax use Windows autorun, which (when enabled) automatically loads and runs software from a disc when the disc is inserted into the computer's drive. Autorun lets the DRM vendor's software run or install immediately.

Once the DRM software is installed, every time a new CD is inserted the software runs a recognition algorithm to determine whether the disc is associated with the DRM scheme. If it is, the active protection software will interfere with accesses to the disc, except those originating from the vendor's own music player application. This proprietary player application, which is shipped on the disc, gives the user limited access to the music.

As we will discuss further, all parts of this design are subject to attack by a user who wants to copy the music illegally or who wants to make uses allowed by copyright law but blocked by the DRM. The user can defeat the passive protection, stop the DRM software from installing itself, trick the recognition algorithm, defeat the active protection software's blocking, capture the music from the DRM vendor's player, or uninstall the protection software.

The complexity of today's CD DRM software offers many avenues of attack. On the whole, today's systems are no more resistant to attack than were simpler early CD DRM systems [10, 11]. When there are fundamental limits to security, extra complexity does not mean extra security.

Discs Studied Sony deployed XCP on 52 titles (representing more than 4.7 million CDs) [1]. We examined three of them in detail: Acceptance, *Phantoms* (2005); Susie Suh, *Susie Suh* (2005); and Switchfoot, *Nothing is Sound* (2005). MediaMax was deployed on 37 Sony titles (over 20 million CDs) as well as dozens of titles from other labels [1]. We studied three albums that used MediaMax version 3—Velvet Revolver, *Contraband* (BMG, 2004); Dave Matthews Band, *Stand Up* (Sony, 2005); and Anthony Hamilton, *Comin' from Where I'm From* (Arista/Sony 2005)—and three albums that used MediaMax version 5—Peter Cetera, *You Just Gotta Love Christmas* (Viastar, 2004); Babyface, *Grown and Sexy* (Arista/Sony, 2005); and My Morning Jacket, *Z* (ATO/Sony, 2005). Unless otherwise noted, statements about MediaMax apply to both version 3 and version 5.

4 Installation

Active protection measures cannot begin to operate until the DRM software is installed on the user's system. In this section we consider attacks that either prevent installation of the DRM software, or capture music files from the disc in the interval after the disc has been inserted but before the DRM software is installed on the computer.

4.1 Autorun

Both XCP and MediaMax rely on the autorun feature of Windows. Whenever removable media, such as a floppy

disc or CD, is inserted into a Windows PC (and autorun is enabled), Windows looks on the disc for a file called `autorun.inf` and executes commands contained in it. Autorun is commonly used to pop up a splash screen or simple menu (for example) to offer to install software found on the disc. However, the autorun mechanism will run any program that the disc specifies.

Other popular operating systems, including MacOS X and Linux, do not have an autorun feature, so this mechanism does not work on those systems. XCP ships only Windows code and so has no effect on other operating systems. MediaMax ships with both Windows and MacOS code, but only the Windows code can autorun. The MacOS code relies on the user to double-click an installer, which few users will do. For this reason, we will not discuss the MacOS version of MediaMax further.

Current versions of Windows ship with autorun enabled by default, but the user can choose to disable it. Many security experts advise users to disable autorun to protect against disc-borne malware. If autorun is disabled, the XCP or MediaMax active protection software will not load or run. Even if autorun is enabled, the user can block autorun for a particular disc by holding down the Shift key while inserting the disc [11]. This will prevent the active protection software from running.

Even without disabling autorun, a user can prevent the active protection software from loading by covering up the portion of the disc on which it is stored. Both XCP and MediaMax discs contain two sessions, with the first session containing the music files and the second session containing DRM content, including the active protection software and the autorun command file. The first session begins at the center of the disc and extends outward; the second session is near the outer edge of the disc. By covering the outer edge of the disc, the user can prevent the drive from reading the second session's files, effectively converting the disc back to an ordinary single-session audio CD. The edge of the disc can be covered with non-transparent material such as masking tape, or by writing over it with a felt-tip marker [19]. Exactly how much of the disc to cover can be determined by iteratively covering more and more until the disc's behavior changes, or by visually inspecting the disc to look for a difference in appearance of the disc's surface which is often visible at the boundary between the two sessions.

4.2 Temporary Protection

Even if the copy protection software is allowed to autorun, there is a period of time, between when a protected disc is inserted and when the active protection software is installed, when the music is vulnerable to copying. It would be possible to have the discs immediately and automatically install the active protection software, minimizing this window of vulnerability, but legal and ethical requirements should preclude this option. Installing software without first obtaining the user's consent appears to be illegal in the U.S. under the Computer Fraud and Abuse Act (CFAA) as well as various state anti-spyware laws [2, 3].

Software vendors conventionally obtain user consent to the installation of their software by displaying an End User License Agreement (EULA) and asking the user to accept it. Only after the user agrees to the EULA is the software installed. The EULA informs the user, in theory at least, of the general scope and purpose of the software being installed, and the user has the option to withhold consent by declining the EULA, in which case no software is installed. As we will see below, the DRM vendors do not always follow this procedure.

If the discs didn't use any other protection measures, the music would be vulnerable to copying while the installer waited for the user to accept or reject the EULA. Users could just ignore the installer's EULA window and switch tasks to a CD ripping or copying application. Both XCP and MediaMax employ temporary protection mechanisms to protect the music during this time.

4.2.1 XCP Temporary Protection

The first time an XCP-protected disc is inserted into a Windows machine, the Windows autorun feature launches the XCP installer, the file `go.exe` located in the `contents` folder on the CD. The installer displays a license agreement and prompts the user to accept or decline it. If the user accepts the agreement, the installer installs the XCP active protection software onto the machine; if the user declines, the installer exits after ejecting the CD, preventing other applications from ripping or copying it.

While the EULA is being displayed, the XCP installer continuously monitors the list of processes running on the system. It compares the image name of each process to a blacklist of nearly 200 ripping and copying applications hard coded into the `go.exe` program. If one or more blacklisted applications are running, the installer replaces the EULA display with a warning indicating that the applications need to be closed in order for the installation to continue. It also initiates a 30-second countdown timer; if any of the applications are still running when the countdown reaches zero, the installer ejects the CD and quits.[3]

This technique might prevent some unsophisticated users from copying the disc while the installer is running, but it can be bypassed with a number of widely known techniques. For instance, users might kill the installer process (using the Windows Task Manager) before it can eject the CD, or they might use a ripping or copying ap-

plication that locks the CD tray, preventing the installer from ejecting the disc.

The greatest limitation of the XCP temporary protection system is the blacklist. Users might find ripping or copying applications that are not on the list, or they might use a blacklisted application but rename its executable file to prevent the installer from recognizing it. Since there is no mechanism for updating the blacklist on existing CDs, they will gradually become easier to rip and copy as new applications not on the blacklist come into widespread use. Application developers may also adapt their software to the blacklisting technique by randomizing their process image names or taking other measures to avoid detection.[4]

4.2.2 MediaMax Temporary Protection

MediaMax employs a different—and highly controversial—temporary protection measure. It defends the music while the installer is running by installing, and at least temporarily activating, the active protection software *before* displaying the EULA. The software is installed without obtaining consent, and it remains installed (and in some cases, permanently active) even if the user explicitly denies consent by declining the license agreement.

MediaMax discs install the active protection driver by copying a file called `sbcphid.sys` to the Windows drivers directory, configuring it as a service in the registry, and launching it. Initially, the driver's startup type is set to "Manual," so it will not re-launch the next time the computer boots; however, it remains running until the computer is shut down, and it remains installed permanently [11]. Albums that use MediaMax version 5 additionally install components of the MediaMax player software before displaying a license agreement. These files are not removed if the EULA is declined.

Even more troublingly, under some common circumstances—for example, if the user inserts a MediaMax version 5 CD and declines the EULA and later inserts a MediaMax CD again—the MediaMax installer will permanently activate the active protection software (by setting its startup type to "Auto," which causes it to be launched every time the computer boots). This behavior is related to a mechanism in the installer apparently intended to upgrade the active protection software if an older version is already installed.

We can think of two possible explanations for this behavior. Perhaps the vendor, SunnComm, did not test these scenarios to determine what their software did, and so did not realize that they were activating the software without consent. Or perhaps they did know what would happen in these cases and deliberately chose these behaviors. Either possibility is troubling, indicating either a deficient design and testing procedure or a deliberate decision to install software after the user denied permission to do so.

Even if poor testing is the explanation for *activating* the software without consent, it is clear that SunnComm deliberately chose to *install* the MediaMax software on the user's system even if the user did not consent. These decisions are difficult to reconcile with the ethical and legal requirements on software companies. But they are easy to reconcile with the vendor's platform building strategy, which rewards the vendor for placing its software on as many computers as possible.

Even if no software is *installed* without consent, the temporary *activation* of DRM software, by both XCP and MediaMax, before the user consents to anything raises troubling ethical questions. It is hard to argue that the user has consented to loading running software merely by the act of inserting the disc. Most users do not expect the insertion of a music CD to load software, and although many (but not all) of the affected discs did contain a statement about protection software being on the discs, the statements generally were confusingly worded, were written in tiny print, and did not say explicitly that software would install or run immediately upon insertion of the disc. Some in the record industry argue that the industry's desire to block potential infringement justifies the short-term execution of the temporary protection software on every user's computer. We think this issue deserves more ethical and legal debate.

4.3 Passive Protection

Another way to prevent copying before active protection software is installed is to use passive protection measures. Passive protection exploits subtle differences between the way computers read CDs and the way ordinary CD players do. By changing the layout of data on the CD, it is sometimes possible to confuse computers without affecting ordinary players. In practice, the distinction between computers and CD players is imprecise. Older generations of CD copy protection, which relied entirely on passive protection, proved easy to copy in some computers and impossible to play on some CD players [10]. Furthermore, computer hardware and software has tended to get better at reading the passive protected CDs over time as it has become more robust to all manner of damaged or poorly formatted discs. For these reasons, more recent CD DRM schemes rely mainly on active protection.

XCP uses a mild variety of passive protection as an added layer of security against ripping and copying. This form of passive protection exploits a quirk in the way Windows handles multisession CDs. When CD burners came to market in the early 1990s, the multisession CD format was introduced to allow data to be appended to

partially recorded discs. (This was especially desirable at a time when recordable CD media cost tens of dollars per disc.) Each time data is added to the disc, it is written as an independent series of tracks called a session. Multisession compatible CD drives see all the sessions, but ordinary CD players, which generally do not support the multisession format, recognize only the first session.

Some commercial discs use a variant of the multisession format to combine CD audio and computer accessible files on a single CD. These discs adhere to the Blue Book or "stamped multisession" format. According to the Blue Book specification, stamped multisession discs must contain two sessions: a first session with 1–99 CD audio tracks, and a second session with one data track. The Windows CD audio driver contains special support for Blue Book discs. It presents the CD to player and ripper applications as if it were a normal audio CD. Windows treats other multisession discs as data-only CDs.

XCP discs deviate from the Blue Book format by adding a second data track in the second session. This causes Windows to treat the disc as a regular multisession data CD, so the primary data track is mounted as a file system, but the audio tracks are invisible to player and ripper applications that use the Windows audio CD driver. This includes Windows Media Player, iTunes, and most other widely used CD applications. We developed a procedure for creating discs with this passive protection using only standard CD burning hardware and software.

This variety of passive protection provides only limited resistance to ripping and copying. There are a number of well-known methods for defeating it:

- *Advanced ripping and copying applications* avoid the Windows CD audio driver altogether and issue commands directly to the drive. This allows programs such as Nero and Exact Audio Copy to recognize and read all the audio tracks.
- *Non-Windows platforms*, including MacOS and Linux, read multisession CDs more robustly and do not suffer from the limitation that causes ripping problems on Windows.
- The *felt-tip marker trick*, described above, can also defeat this kind of passive protection. When the second session is obscured by the marker, CD drives see only the first session and treat the disc as a regular audio CD, which can be ripped or copied.

5 Disc Recognition

The active protection mechanisms employed by XCP and MediaMax regulate access to raw CD audio, blocking access to the audio tracks on albums protected with a particular scheme while allowing access to all other titles.

To accomplish this, the schemes install a background process that interposes itself between applications and the original CD driver. In MediaMax, this process is a kernel-mode driver called `sbcphid.sys`. XCP uses a pair of filter drivers called `crater.sys` and `cor.sys` that attach to the CD-ROM and IDE devices [21]. In both schemes, the active protection drivers examine each disc that is inserted into the computer to see whether access to it should be restricted. If the disc is recognized as copy protected, the drivers monitor for attempts to read the audio tracks, as would occur during a playback, rip, or disc copy operation, and corrupt the audio returned by the drive to degrade the listening experience. MediaMax introduces a large amount of random jitter, making the disc sound like it has been badly scratched or damaged; XCP replaces the audio with random noise.

Each scheme's active protection software interferes with attempts to rip or copy any disc that is protected by the same scheme, not merely the disc from which the software was installed. This requires some mechanism for identifying discs that are to be protected. In this section we discuss the security requirements for such a recognition system, and describe the design and limitations of the actual recognition mechanism employed by the MediaMax scheme.

5.1 Recognition Requirements

Any disc recognition system detects some distinctive feature of discs protected by a particular copy protection scheme. Ideally such a feature would satisfy four requirements: it would *uniquely* identify protected discs without accidentally triggering the copy protection on other titles; it would be *detectable* quickly after reading a limited amount of audio from the disc; it would be *indelible* enough that an attacker could not remove it without significantly degrading the quality of the audio; and it would be *unforgeable*, so that it could not be applied to an unprotected album without the cooperation of the protection vendor, even if the adversary had access to protected discs.

This last requirement stems from the DRM vendor's platform building strategy, which tries to put the DRM software on to as many computers as possible and to have the software control access to all marked discs. If the vendor's identifying mark is forgeable, then a record label could mark its discs without the vendor's permission, thereby taking advantage of the vendor's platform without paying.[5]

5.2 MediaMax Disc Recognition

To find out how well the disc recognition mechanisms employed by CD DRM systems meet the ideal re-

quirements, we examined the recognition system built into MediaMax. This system drew our attention because MediaMax's creators have touted their advanced disc identification capabilities, including the ability to identify individual tracks within a compilation as protected [16]. XCP appears to use a less sophisticated disc recognition system based on a marker stored in the data track of protected discs; we did not include it in this study.

We determined how MediaMax identifies protected albums by tracing the commands sent to the CD drive with and without the active protection software running. These experiments took place on a Windows XP VMWare virtual machine running on top of a Fedora Linux host system, which we modified by patching the kernel IDE-SCSI driver to log all CD device activity.

With this setup we observed that the MediaMax software executes a disc recognition procedure immediately upon the insertion of a CD. The MediaMax driver reads two sectors of audio at a specific offset from the beginning of audio tracks—approximately 365 and 366 frames in (a CD frame stores $1/75$ second of sound). On unprotected discs, the software scans through every track in this way, but on MediaMax-protected albums, it stops after the first three tracks, apparently having detected an identifying feature. The software decides whether or not to block read access to the audio solely on the basis of information in this region, so we inferred that the identifying mechanism takes the form of an inaudible watermark embedded in this part of the audio stream.[6]

Locating the watermark amid megabytes of audio might have been difficult, but we had the advantage of a virtual Rosetta Stone. The actual Rosetta Stone—a 1500 lb. granite slab, unearthed in Rosetta, Egypt, in 1799—is inscribed with the same text written in three languages: ancient hieroglyphics, demotic (simplified) hieroglyphics, and Greek. Comparing these inscriptions provided the key to deciphering Egyptian hieroglyphic texts. Our Rosetta Stone was a single album, Velvet Revolver's *Contraband*, released in three different versions: a U.S. release protected by MediaMax, a European release protected by a passive scheme developed by Macrovision, and a Japanese release with no copy protection. We decoded the MediaMax watermark by examining the differences between the audio on these three discs. Binary comparison revealed no differences between the releases from Europe and Japan; however, the MediaMax-protected U.S. release differed slightly from the other two in certain parts of the recording. By carefully analyzing these differences—and repeatedly attempting to create new watermarked discs using the MediaMax active protection software as an oracle—we were able to deduce the structure of the watermark.

The MediaMax watermark is embedded in the audio of each track in 30 *clusters* of modified audio samples. Each cluster is made up of 288 marked 16-bit audio samples followed by 104 unaltered samples. Three mark clusters exactly fit into one 2352-byte CD audio frame. The watermark is centered at approximately frame 365 of the track; though the detection routine in the software only reads two frames, the mark extends several frames to either side of the designated read target to allow for imprecise seeking in the audio portion of the disc (a typical shortcoming of inexpensive CD drives). The MediaMax driver detects the watermark if at least one mark cluster is present in the region read by the detector.

A sequence of 288 bits that we call the *raw watermark* is embedded into the 288 marked audio samples of each mark cluster. A single bit of the raw watermark is embedded into an unmarked audio sample by setting one of the three least significant bits to the new bit value (as shown in bold below) and then setting the two other bits according to this table:[7]

Original bits	Marked bits					
	0__	_**0**_	__**0**	**1**__	_**1**_	__**1**
----------111	**0**11	1**0**1	11**0**	**1**11	1**1**1	11**1**
----------110	**0**11	1**0**1	11**0**	**1**10	1**1**0	11**1**
----------101	**0**11	1**0**1	10**0**	**1**01	1**1**0	10**1**
----------100	**0**11	1**0**0	10**0**	**1**00	1**1**0	10**1**
----------011	**0**11	0**0**1	01**0**	**1**00	0**1**1	01**1**
----------010	**0**10	0**0**1	01**0**	**1**00	0**1**0	01**1**
----------001	**0**01	0**0**1	00**0**	**1**00	0**1**0	00**1**
----------000	**0**00	0**0**0	00**0**	**1**00	0**1**0	00**1**

The position of the embedded bit in each sample follows a fixed sequence for every mark cluster. Each of the 288 bits is embedded in the first-, second-, or third-least-significant bit position of the sample according to this sequence:

```
2,3,1,1,2,2,3,3,2,3,3,3,1,3,2,3,2,1,3,2,2,3,2,2,
 2,1,3,3,2,1,2,3,3,1,2,2,3,1,2,3,3,1,1,2,2,1,1,3,
3,1,2,3,1,2,3,3,1,3,3,2,1,1,2,3,2,2,3,3,3,1,1,3,
 1,2,1,2,3,3,2,2,3,2,1,2,2,1,3,1,3,2,1,1,2,1,1,1,
2,3,2,1,1,2,3,2,1,3,2,2,2,3,1,2,1,3,3,3,3,1,1,1,
 2,1,1,2,2,2,2,3,1,2,3,2,1,3,1,2,2,3,1,1,3,1,1,1,
1,2,2,3,2,3,2,3,2,1,2,3,1,3,1,3,3,3,1,1,2,1,1,2,
 1,3,3,2,3,3,2,2,1,1,1,2,2,1,3,3,3,3,3,1,3,1,1,3,
2,2,3,1,2,1,2,3,3,2,1,1,3,2,1,1,2,2,1,3,3,2,2,3,
 1,3,2,2,2,3,1,1,1,1,3,2,1,3,1,1,2,2,3,2,3,1,1,2,
1,3,2,3,3,1,1,3,2,1,3,1,2,2,3,1,1,3,2,1,2,2,2,1,
3,3,1,2,3,3,3,1,2,2,3,1,2,3,1,1,3,2,2,1,3,2,1,3
```

The active protection software reads the raw watermark by reading the first, second, or third bit from each sample according to the sequence above. It determines whether the resulting 288-bit sequence is a valid watermark by checking certain properties of the sequence (represented below). It requires 96 positions in the sequence to have a fixed value, either 0 or 1. Another 192 positions are divided into 32 groups of linked values (denoted a–z

and α–ζ below). In each group, three positions share the same value and three share the complement value. This allows the scheme to encode a 32-bit value (value A), though in the discs we studied it appears to take a different random value in each mark cluster of each protected title. The final 32 bits of the raw watermark may have arbitrary values (denoted by _ below) and encode a second 32-bit value (value B). MediaMax version 5 uses this value to distinguish between original discs and backup copies burned through it proprietary player application.

$$0, a, b, c, d, e, 0, 0, f, 0, g, 0, h, 0, i, d, j, \bar{j}, k, 0, l, m, 0, n,$$
$$o, p, \bar{e}, q, \bar{e}, r, 0, \bar{p}, s, d, \bar{m}, t, u, v, w, t, \bar{l}, a, x, c, u, 0, \bar{r}, l,$$
$$f, \bar{d}, v, 0, m, 0, \bar{q}, 0, y, c, z, 0, j, \bar{i}, \bar{g}, \alpha, \bar{s}, \bar{w}, \bar{h}, v, y, n, 0, 0,$$
$$\bar{h}, \bar{j}, \bar{u}, a, \beta, 0, \bar{v}, g, j, 0, 0, \bar{\beta}, \bar{i}, e, \bar{z}, 0, r, \gamma, \bar{a}, \delta, \bar{d}, \bar{z}, 0, \bar{v},$$
$$\epsilon, 0, x, s, \bar{g}, \bar{r}, 0, \bar{b}, o, b, r, 0, y, \bar{\beta}, \bar{m}, h, 0, \bar{a}, n, \bar{f}, \bar{t}, 0, \bar{o}, 0,$$
$$\bar{\gamma}, \bar{e}, \bar{e}, 0, 0, \bar{k}, \bar{c}, \bar{x}, 0, \bar{f}, p, z, \bar{x}, i, 0, 0, \alpha, \bar{g}, 0, 1, w, \bar{t}, \bar{n}, \bar{w},$$
$$i, 0, 0, \bar{j}, m, x, \beta, \bar{y}, \bar{p}, \bar{q}, 0, 0, 0, e, \bar{\beta}, 0, 0, 1, g, 0, p, l, 0, \bar{\alpha},$$
$$t, h, \bar{d}, \bar{e}, \bar{w}, \gamma, \bar{\delta}, 0, \bar{p}, q, \bar{f}, 0, 1, \zeta, 0, \bar{c}, \zeta, \bar{\alpha}, \bar{s}, \bar{b}, \bar{\gamma}, \beta, 0, o,$$
$$0, q, \bar{i}, 0, 0, \bar{\alpha}, \underline{s}, \epsilon, \bar{e}, \bar{h}, 0, \bar{k}, \bar{n}, \bar{\zeta}, \alpha, \bar{s}, \bar{z}, \bar{n}, \bar{c}, \bar{o}, \bar{b}, 0, \bar{t}, 0,$$
$$\bar{y}, \bar{v}, 0, \zeta, \bar{o}, 0, \bar{\zeta}, 0, u, \gamma, 0, \bar{y}, k, \bar{u}, z, \bar{\delta}, \bar{q}, k, \bar{r}, \bar{u}, \bar{\zeta}, \bar{\gamma}, \bar{l}, \bar{l},$$
$$w, \bar{k}, \bar{a}, 0, \bar{\delta}, 0, \epsilon, \bar{m}, b, f, 0, 0, \bar{x}, \delta, \delta, 0, \_, \_, \_, \_, \_, \_, \_, \_, \_, \_, \_, \_,$$
$$\_, \_, \_, \_, \_, \_, \_, \_, \_, \_, \_, \_, \_, \_, \_, \_, \_, \_, \_, \_, \_, \_, \_$$

5.3 Attacks on the MediaMax Watermark

The MediaMax watermark fails to satisfy the indelibility and unforgeability requirements of an ideal disc recognition system. Far from being indelible, the mark is surprisingly brittle. Most advanced designs for robust audio watermarks [7, 6] manipulate the audio in the frequency domain and try to resist removal attempts that use lossy compression, multiple conversions between digital and analog formats, and other common transformations. In contrast, the MediaMax watermark is applied in the time domain and is rendered undetectable by even minor changes to the file. An adversary without any knowledge of the watermark's design could remove it by converting the tracks to a lossy format like MP3 and then burning them back to a CD, which can be accomplished easily with standard consumer applications. This would result in some minor loss of fidelity, but a more sophisticated adversary could prevent the mark from being detected with almost no degradation by flipping the least significant bit of one carefully chosen sample from each of the 30 watermark clusters, thereby preventing the mark from exhibiting the pattern required by the detector.

The watermark also fails to satisfy the unforgeability requirement. The mark's only defense against forgery is its complicated, unpublished design, but as is often the case this security by obscurity has proved tedious rather than impossible to defeat. As it turns out, an adversary needs only limited knowledge of the watermark—its location within a protected track and its confinement to the three least significant bits of each sample—to forge it with minimal loss of fidelity. Such an attacker could transplant the three least significant bits of each sample within the watermarked region of a protected track to the corresponding sample from an unprotected one. Transplanting these bits would cause distortion more audible that that caused by embedding the watermark since the copied bits are likely to differ by a greater amount from the original sample values; however, the damage to the audio quality would be limited since the marked region is only 0.4 seconds in duration. A more sophisticated adversary could apply a watermark to an unprotected track by deducing the full details of the structure of the watermark, as we did; she could then embed the mark in an arbitrary audio file just as well a licensed disc producer.

Though MediaMax did not do so, it is straightforward to create an unforgeable mark using digital signatures. The marking algorithm would extract a segment of music, compute its cryptographic hash, digitally sign the hash, and write the hash into the low-order bits of audio samples elsewhere in the music file. The recognition algorithm would recompute the hash, and extract and verify the signature. Though unforgeable, this mark would be no more indelible than the MediaMax scheme—making an indelible mark is a more difficult problem.

6 CD DRM Players

Increasingly, personal computers—and portable playback devices that attach to them—are users' primary means of organizing, transporting, and enjoying their music collections. Sony-BMG and its DRM vendors recognized this trend when they designed their copy protection technologies. Rather than inhibit all use with PCs, as some earlier anti-copying schemes did [10], XCP and MediaMax provide their own proprietary media players, shipped on each protected CD, that allow certain limited uses of the music subject to restrictions imposed by the copyright holder.[8]

The XCP and MediaMax players launch automatically using autorun when a protected disc is inserted into a PC. Both players have similar feature sets. They provide a rudimentary playback interface, allowing users to listen to protected albums, and they allow access to "bonus content," such as album art, liner notes, song lyrics, and links to artist web sites. The players access music on the disc, despite the active protection, by using a special back door interface provided by the active protection software.

XCP and MediaMax version 5 both permit users to burn copies of the entire album a limited number of times (typically three). These copies are created using a proprietary burning application integrated into the player. The copies include the player applications and the same active (and passive, for XCP) protection as the original al-

bum, but they do not allow any subsequent generations of copying.

Another feature of the player applications allows users to rip the tracks from the CD to their hard disks, but only in DRM-protected audio formats. Both schemes support the Windows Media Audio format by using a Microsoft product, the Windows Media Data Session Toolkit [17], to deliver DRM licenses that are bound to the PC where the files were ripped. The licenses allow the music to be transferred to portable devices that support Windows Media DRM or burned onto CDs, but the Windows Media files will not be usable if they are copied to another PC. Because XCP and MediaMax create Windows Media files, they are vulnerable to any attack that can defeat Windows Media DRM. Often, DRM interoperation allows attacks on one system to defeat other systems as well, because the attacker can transfer protected content into the system of her choice in order to extract it.

The XCP and MediaMax version 5 players both exhibit similar spyware-like behavior: phoning home to the vendor or record label with information about users' listening habits despite statements to the contrary from the vendors. Whenever a protected disc is inserted, the players contact web servers to retrieve images or banner ads to display. Part of the request is a code that identifies the album. XCP discs contact a Sony web site, `connected.sonymusic.com` [20]; MediaMax albums contact `license.sunncomm2.com`, a site operated by MediaMax's creator, SunnComm. These connections allow the servers to log the user's IP address, the date and time, and the identity of the album. This undisclosed data collection, in combination with other practices—installation without informed consent and the lack of an uninstaller—make XCP and MediaMax fit the consensus definition of spyware.

6.1 Attacks on Players

The XCP and MediaMax version 5 players were designed to enforce usage restrictions specified by content providers. In practice, they provide minimal security because there are many ways that users can bypass the limitations. Perhaps the most interesting class of attacks targets the limited number of burned copies permitted by the players. Both players are designed to enforce this limit without communicating with any networked server; thus, the player must keep track of how many allowed copies remain by storing state on the local machine.

It is well known that DRM systems like this are vulnerable to rollback attacks. A rollback attack backs up the state of the machine before performing the limited operation (in this case, burning the copy). When the operation is complete, the old system state is restored, and the DRM software is not able to determine that the operation has occurred. This kind of attack is easy to perform with virtual machine software like VMWare, which allows the entire state of the system to be saved or restored in a few clicks. XCP and MediaMax both fail under this attack, which allows unlimited copies to be burned with their players.

A refined variation of this attack targets only the specific pieces of state that the DRM system uses to remember the number of copies remaining. The XCP player uses a single file, `%windir%\system32\$sys$filesystem\$sys$parking`, to record how many copies remain for every XCP album that has been used on the system.[9] Rolling back this file after a disc copy operation would restore the original number of copies remaining.

A more advanced attacker can go further and modify the `$sys$parking` file to set the counter to an arbitrary value. The file consists of a 16 byte header followed by a series of 177 byte structures. For each XCP disc used on the machine, the file contains a whole-disc structure and an individual structure for each track. Each disc structure stores the number of permitted copies remaining for the disc as a 32-bit integer beginning 100 bytes from the start of the structure.

The file is protected by primitive encryption. Each structure is XORed with a repeating 256-bit pad. The pad—a single pad is used for all structures—is randomly chosen when XCP is first installed and stored in the system registry in the key `HKLM\SOFTWARE\$sys$reference\ClassID`. Note that this key, which is hidden by the rootkit, is intentionally misnamed "ClassID" to confuse investigators. Instead of a ClassID, it contains the 32 bytes of pad data.

Hiding the pad actually doesn't increase the security of the design. An attacker who knows only the format of the `$sys$parking` file and the current number of copies remaining can change the counter to an arbitrary value without needing to know the pad. Say the counter indicates that there are x copies remaining and the attacker wants to set it to y copies remaining. Without decrypting the structure, she can XOR the padded bytes where the counter is stored with the value $x \oplus y$. If the original value was padded with p, the new value will be $(x \oplus p) \oplus (x \oplus y) = (y \oplus p)$, y padded with p.

Ironically, Sony itself furnishes directions for carrying out another attack on the player DRM. Conspicuously absent from the XCP and MediaMax players is support for the Apple iPod—by far the most popular portable music player. A Sony FAQ blames Apple for this shortcoming and urges users to direct complaints to them: "Unfortunately, in order to directly and smoothly rip content into iTunes it [sic.] requires the assistance of Apple. To date, Apple has not been willing to cooperate with our protection vendors to make ripping to iTunes and to the iPod a

simple experience." [23]. Strictly speaking, it is untrue that Sony requires Apple's cooperation to work with the iPod, as the iPod can import MP3s and other open formats. What Sony has difficulty doing is moving music to the iPod while keeping it wrapped in copy protection. This is because Apple has so far refused to support interoperation with its FairPlay DRM.

Yet so great is consumer demand for iPod compatibility that Sony gives out—to any customer who fills out a form on its web site [22]—instructions for working around its own copy protection and transforming the music into a DRM-free format that will work with the iPod. The procedure is simple but cumbersome: users are directed to use the player software to rip the songs into Windows Media DRM files; use Windows Media Player to burn the files to a blank CD, which will be free of copy protection; and then use iTunes to rip the songs once more and transfer them to the iPod.

6.2 MediaMax Player Security Risks

Besides suffering from several kinds of attacks that expose the music content to copying, the MediaMax version 5 player makes the user's system more vulnerable to attack. When a MediaMax CD is inserted into a computer, Windows autorun launches an installer from the disc. Even before displaying a license agreement, MediaMax copies almost twelve megabytes of files and data related to the MediaMax player to the hard disk. Jesse Burns and Alex Stamos of iSEC Partners discovered that the MediaMax installer sets file permissions that allow any user to modify its code directory and the files and programs in it [5].

As Burns and Stamos realized, the lax permissions allow a non-privileged user to replace the executable code in the MediaMax player files with malicious code. The next time a user plays a MediaMax-protected CD, the attack code will be executed with that user's security privileges. The MediaMax player requires Power User or Administrator privileges to run, so it's likely that the attacker's code will run with almost complete control of the system.

Normally, this problem could be fixed by manually correcting the errant permissions. However, MediaMax aggressively updates the installed player code each time the software on a protected disc autoruns or is launched manually. As part of this update, the permissions on the installation directory are reset to the insecure state.

We discovered a variation of the attack suggested by Burns and Stamos that allows the attack code to be installed even if the user has never consented to the installation of MediaMax, and to be triggered immediately whenever the user inserts a MediaMax CD. In our attack, the attacker places hostile code in the `DllMain` procedure of a code file called `MediaMax.dll`, which MediaMax installs even before displaying the EULA. The next time a MediaMax CD is inserted, the installer autoruns and immediately attempts to check the version of the installed `MediaMax.dll` file. To do this, the installer calls the Windows `LoadLibrary` function on the DLL file, which causes the file's `DllMain` procedure to execute, along with any attack code placed there.

This problem is exacerbated because parts of the MediaMax software are installed automatically and without consent. Users who have declined the EULA likely assume that MediaMax has not been installed, and so most will be unaware that they are vulnerable. The same installer code performs the dangerous version check as soon as the CD is inserted. A CD that prompted the user to accept a license before installing code would give the user a chance to head off the attack.

Fixing this problem permanently without losing the use of protected discs requires installing a patch from SunnComm. Unfortunately, as we discovered, the initial patch released by Sony-BMG in response to the iSEC report was capable of triggering precisely the kind of attack it was supposed to prevent. In the process of updating MediaMax, the patch checked the version of `MediaMax.dll` just like the MediaMax installer does. If this file was already modified by an attacker, the process of applying the security patch would execute the attack code. Prior versions of the MediaMax uninstaller had the same vulnerability, though both the uninstaller and the patch have since been replaced with versions that do not suffer from this problem.

7 Deactivation

Active protection methods install and run software components that interfere with accesses to a CD. Users can remove or deactivate the active protection software by using standard system administration tools that are designed to find, characterize, and control the programs installed on a machine. Deactivating the protection will enable arbitrary use or ripping of the music, and it is difficult to stop if the user has system administrator privileges. In this section, we discuss how active protection may be deactivated.

7.1 Deactivating MediaMax

The MediaMax active protection software is easy to deactivate, being comprised of a single device driver named `sbcphid`. The driver can be removed by using the Windows command `sc delete sbcphid` to stop the driver, and then removing the `sbcphid.sys` file containing the driver code. MediaMax-protected albums can then be accessed freely.

7.2 Defenses Against Deactivation

To counter deactivation attempts, a vendor might try technical tricks to evade detection and frustrate removal of the active protection software. An example is the rootkit-like behavior of XCP, discovered by Mark Russinovich [21]. When XCP installs its active protection software, it also installs a second program—the rootkit—that conceals any file, process, or registry key whose name begins with the prefix `$sys$`. The result is that XCP's main installation directory, and most of its registry keys, files, and processes, become invisible to normal programs and administration tools.

The rootkit is a kernel-level driver named `$sys$aries` that is set to automatically load early in the boot process. When the rootkit starts, it hooks several Windows system calls by modifying the system service dispatch table (the kernel's `KeServiceDescriptorTable` structure) which is an array of pointers to the kernel functions that implement basic system calls. The rootkit modifies the behavior of four system calls: `NtQueryDirectoryFile`, `NtCreateFile`, `NtQuerySystemInformation`, and `NtEnumerateKey`.[10] These calls are used to enumerate files, processes, and registry entries. The rootkit filters the data returned by these calls to hide items whose names begin with `$sys$`.

On intercepting a function call, the rootkit checks the name of the calling process. If the name of the calling process begins with `$sys$`, the rootkit returns the results of the real kernel function without alteration so that XCP's own processes have an accurate view of the system.

The XCP rootkit increases users' vulnerability to attack by allowing any software to hide—not just XCP. Malware authors can exploit the fact that any files, registry keys, or processes with names beginning in `$sys$` will be hidden, thereby saving the trouble of installing their own rootkits. Malware that lacks the privileges to install its own rootkit can still rely on XCP's rootkit.

Only kernel-level processes can patch the Windows system service dispatch table, and only privileged users—normally, members of the Administrators or Power Users groups—can install such processes. (XCP itself requires these privileges to install.) Malicious code running as an unprivileged user can't normally install a rootkit that intercepts system calls. But if the XCP rootkit is installed, it will hide all programs that adopt the `$sys$` prefix so that even privileged users will be unable to see them. This vulnerability has already been exploited by at least two Trojan horses seen in the wild [15, 14].

The rootkit opens at least one more security vulnerability. The modified functions do not check for errors as carefully as the original Windows functions do, so the rootkit makes it possible for an ordinary program to crash the system by calling one of the hooked functions, for example by calling `NtCreateFile` with an invalid `ObjectAttributes` argument. We do not believe this vulnerability can be exploited to run arbitrary code.

7.3 Deactivating XCP

Deactivating XCP's active protection is more complicated because it comprises several processes that are more deeply entangled in the system configuration, and are hidden by the XCP rootkit. Deactivation requires a three-step procedure.

The first step is to deactivate and remove the rootkit, by the same procedure used to deactivate MediaMax (except that the driver's name is `aries.sys`). Disabling the rootkit and then rebooting exposes the previously hidden files, registry entries, and processes.

The second step is to edit the registry to remove references to XCP's filter drivers and CoDeviceInstallers. XCP uses the Windows filter driver facility to intercept commands to the CD drives and IDE bus. If the code for these filter drivers is removed but the entries pointing to that code are not removed from the registry, the CD and IDE device drivers will fail to initialize. This can cause the CD drives to malfunction, or, worse, can stop the system from booting if the IDE device driver is disabled. The registry entries can be eliminated by removing any reference to a driver named `$sys$cor` from any registry entries named `UpperDrivers` or `LowerDrivers`, and removing any lines containing `$sys$caj` from any list of CoDeviceInstallers in the registry.

The third step is to delete the XCP services and remove the XCP program files. Services named `$sys$lim`, `$sys$oct`, `$sys$drmserver`, `cd_proxy`, and `$sys$cor` can be deactivated using the `sc delete` command, and then files named `crater.sys`, `lim.sys`, `oct.sys`, `$sys$cor.sys`, `$sys$caj.dll`, and `$sys$upgtool.exe` can be deleted. After rebooting, the two remaining files named `CDProxyServ.exe` and `$sys$DRMServer.exe` can be removed.

Performing these steps will deactivate the XCP active protection, leaving only the passive protection on XCP CDs in force. The procedure easily could be automated to create a point-and-click removal tool.

7.4 Impact of Spyware Tactics

The use of rootkits and other spyware tactics harms users by undermining their ability to manage their computers. If users lose effective control over which programs run

on their computers, they can no longer patch malfunctioning programs or remove unneeded programs. Managing a system securely is difficult enough without spyware tactics making it even harder.

Though it is no surprise that spyware tactics would be attractive to DRM designers, it is a bit surprising that mass-market DRM vendors chose to use those tactics despite their impact on users. If only one vendor had chosen to use such tactics, we could write it off as an aberration. But two vendors made that choice, which is probably not a coincidence. We suspect that the vendors let the lure of platform building override the risk to users.

7.5 Summary of Deactivation Attacks

Ultimately, there is little a CD DRM vendor can do to stop users from deactivating active protection software. Vendors' attempts to frustrate users' control of their machines are harmful and will trigger a strong backlash from users. In practice, vendors will probably have to provide some kind of uninstaller—users will insist on it, and some users will need it to deal with the bugs and incompatibilities that crop up inevitably in complex software. Once an uninstaller is released, users can use it to remove the DRM software. Determined users will be able to keep CD DRM software off of their machines.

8 Uninstallation

The DRM vendors responded to user complaints about spyware-like behavior by offering uninstallers that would remove their software from users' systems. Uninstallers had been available before but were very difficult to acquire. For example, to get the original XCP uninstaller, a user had to fill out an online form involving personal information, then wait a few days for a reply email, then fill out another online form and install some software, then wait a few days for yet another email, and finally click a URL in the last email. It is hard to explain the complexity of this procedure, except as a way to deter users from uninstalling XCP.

The uninstallers, when users did manage to get them, did not behave like ordinary software uninstallers. Normal uninstallers are programs that can be acquired and used by any user who has the software. The first XCP uninstaller was customized for each user so that it would only work for a limited time and only on the computer on which the user had filled out the second form. This meant, for example, that if a user uninstalled XCP but it was reinstalled later—say, if the user inserted an XCP CD—the user could not use the same uninstaller again but would have to go through the entire process again to request a new one.

Customizing the uninstaller is more difficult, compared to a traditional uninstaller, for both vendor and user, so it must benefit the vendor somehow. One benefit is to the vendor's platform building strategy, which takes a step backward every time a user uninstalls the software. Customizing the uninstaller allows the vendor to control who receives the uninstaller and to change the terms under which it is delivered.

As user complaints mounted, Sony-BMG announced that unrestricted uninstallers for both XCP and MediaMax would be released from the vendors' web sites. Both vendors chose to make these uninstallers available as ActiveX controls. By an unfortunate coincidence, both uninstallers turned out to open the same serious vulnerability on any computer where they were used.

8.1 MediaMax Uninstaller Vulnerability

The original MediaMax uninstaller uses a proprietary ActiveX control, `AxWebRemove.ocx`, created and signed by SunnComm. Users visiting the MediaMax uninstaller web page are prompted to install the control, then the web page uninstalls MediaMax by invoking one of the control's methods.

This method, `Remove`, takes a URL and a numeric key as arguments. `Remove` contacts the URL, passing it the key. If the server finds the key to be valid, it returns another URL for the uninstaller. The ActiveX control downloads code from the uninstaller URL and then executes it. After running the uninstaller, the ActiveX control contacts the server again to notify it that the key had been used. MediaMax has been removed, but the ActiveX control remains on the user's system.

At this point, a malicious attacker's web page can invoke the control's `Remove` method, passing it a URL pointing to a malicious server controlled by the attacker. The control could contact this server, and then download and run code from a location supplied by the malicious server. By this method, an adversary could run arbitrary code on the user's system.

The flaw in this design, of course, is that MediaMax ActiveX control does not validate the URL it is passed, and does not validate the downloaded code before running it. Validating these items, perhaps using digital signatures, would have eliminated the vulnerability.

8.2 XCP Uninstaller Vulnerability

The original XCP uninstaller contains the same design flaw and is only slightly more difficult to exploit. XCP's ActiveX-based uninstaller invokes a proprietary ActiveX control named `CodeSupport.ocx`. Usually this control is installed in the second step of the three-step XCP

uninstall process. In this step, a pseudorandom code generated by the ActiveX control is sent to the XCP server. The same code is written to the system registry. Eventually the user receives an email with a link to another web page that uses the ActiveX control to remove XCP, but only after verifying that the correct code is in the registry on the local system. This check tethers the uninstaller to the machine from which the uninstallation request was made. Due to this design, the vulnerable control may be present on a user's system even if she never performed the step in the uninstallation process where XCP is removed.

Matti Nikki first noted that the XCP ActiveX control contains suspiciously-named methods, including `InstallUpdate(url)`, `Uninstall(url)`, and `RebootMachine()` [18]. He demonstrated that the control was still present after the XCP uninstallation was complete, and that its methods (including one that rebooted the computer) were scriptable from any web page without further browser security warnings.

We found that the `InstallUpdate` and `Uninstall` methods have an even more serious flaw. Each takes as an argument a URL pointing to a specially formatted archive that contains updater or uninstaller code and data files. When these methods are invoked, the archive is retrieved from the provided URL and stored in a temporary location. For the `InstallUpdate` method, the ActiveX control extracts from the archive a file named `InstallLite.dll` and calls a function in this DLL named `InstallXCP`.

Like the MediaMax ActiveX control, the XCP control does not validate the download URL or the downloaded archive. The only barrier to using the control to execute arbitrary code is the proprietary format of the archive file. We determined the format by disassembling the control. The archive file consists of several blocks of gzip-compressed data, each storing a separate file and preceded with a short header. At the end of the archive, a catalog structure lists metadata for each of the blocks, including a 32-bit CRC. The control verifies this CRC before executing code from the DLL.

With knowledge of this file format, we were able to construct an archive containing (benign proof-of-concept) exploit code, and a web page that would install and run our code on a user's system without any browser security warnings, on a computer containing the XCP control. The same method would allow a malicious web site to execute arbitrary code on the user's machine. Like the MediaMax uninstaller flaw, this problem is especially dangerous because users who have completed the uninstallation may not be aware that they are still vulnerable.

Obviously, these vulnerabilities could have been prevented by careful design and programming. But they were only possible at all because the vendors chose to deliver the uninstallers via this ActiveX method rather than using an ordinary download. We conjecture that the vendors made this choice because they wanted to retain the ability to rewrite, modify, or cancel the uninstaller later, in order to further their platform building strategies.

9 Compatibility and Software Updates

Compared to other media on which software is distributed, compact discs have a very long life. Many compact discs will still be inserted into computers and other players twenty years or more after they are first bought. If a particular version of DRM software is shipped on a new CD, that software version may well try to install and run decades after it was developed. The same is not true of most software, even when shipped on a CD-ROM. Very few if any of today's Windows XP CDs will be inserted into computers in 2026; but today's music CDs will be, so their DRM software must be designed carefully for future compatibility.

The software should be designed for *safety*, so as not to cause crashes or malfunction of other software, and may be designed for *efficacy*, to ensure that its anti-copying features remain effective.

9.1 Supporting Safety by Deactivating Old Software

Safety is easier to achieve, and probably more important. One approach is to design the DRM software to be inert and harmless on future systems. Both XCP and MediaMax do this by relying on Windows autorun, which is likely to be disabled in future versions of Windows for security reasons. If the upcoming Windows Vista disables autorun by default, XCP and MediaMax will be inert on most Vista systems. Perhaps XCP and MediaMax used autorun for safety reasons; but more likely, this choice was expedient for other reasons.

Another safety technique is to build in a sunset date after which the software will make itself inert. A sunset would improve safety but would have relatively little effect on record label revenue for most discs, as we expect nearly all revenue from the disc to have been extracted from the customer in the first three years after she buys it. If in the future more copies of the album are pressed, these could have updated DRM software with a later sunset.

9.2 Updating the Software

When a new version of DRM software is released, it can be shipped on newly pressed CDs, but existing CDs cannot be modified retroactively. Updates for existing

users can be delivered either by download or on new CDs. Downloads are faster but require an Internet connection; CD delivery is slower but can reach non-networked machines.

Users will generally cooperate with updates that help them by improving safety or making the software more useful. But updates to retain the efficacy of the software's usage controls will not be welcomed by users.

Users have many ways to stop updates from downloading or installing, such as write-protecting the software's code so that it cannot be updated, or using a personal firewall to block network connections to the vendor's download servers. System security tools, which are designed generally to stop unwanted network connections, downloads, and code installation, can be set to treat CD DRM software as malware.

A DRM vendor who wants to deliver unwanted updates has two options. First, the vendor can simply offer updates and hope some users will not bother to block them. For the vendor and record label, this is better than nothing. Alternatively, the vendor can try to force users to accept updates.

9.3 Forcing Updates

If a user has the ability to block DRM software updates, a vendor who wants an update must somehow convince the user that updating is in her best interest. One approach is to make a non-updated system painful to use.

Ruling out dangerous and legally risky tactics such as logic bombs that destroy the user's system or hold her (unrelated) data hostage, the vendor's strongest tactic for forcing updates is to make the DRM software block all access to protected CDs until the user accepts an update. The DRM software might check with a network server, which periodically would produce a digitally signed and dated certificate listing allowed versions of the DRM software. If the software on the user's system found that its version number was not on the list (or if it could not get a recent list), it would block all access to protected discs. The user would then have to update to a new version to get access to her protected CDs.

This approach would convince some users to update, and would thereby prolong the DRM's efficacy for those users. But it has several drawbacks. If the computer is not networked, the software will eventually lock down because it cannot get certificates. (If the software kept working in this case, users could avoid updates by preventing the DRM software from making network connections.) A bug in the software could cause an accidental but irreversible lockdown. Or the software could lock itself down if the vendor's Internet site is shut down, for example if the vendor goes bankrupt.

Strong-arm tactics can also be counterproductive, by giving the user further reason to defeat or remove the DRM software.[11] The software is more likely to remain on the user's system if it does not behave annoyingly. Trying to force updates can reduce the DRM system's efficacy if it convinces users to remove the DRM altogether. From the user's standpoint, every software update is a security risk—a possible vector for hostile or buggy code.

Given the problems with forced updates, and the user backlash they likely would have triggered, we are not surprised that neither XCP nor MediaMax tried to force updates.

10 User Outrage, and the Fight to Control Users' Computers

One notable aspect of the Sony CD DRM episode was the level of outrage expressed by users. All too frequently, bugs in popular software products endanger users' security or privacy, and users just grumble and update their software. Users' anger over the CD DRM episode was much more intense. What made this issue so different?

There are three answers. First, many users did not expect audio CDs to contain software. Users did not want the software, and they recognized that Sony-BMG chose to include it anyway. Unlike (say) an email client, which necessarily includes complex software components that might have bugs, CDs need not include software, so users are less willing to accept the risk of security problems in order to get CDs.

Second, some harmful aspects of the CD DRM software reflected deliberate choices by the vendors (and by extension, Sony-BMG). Users who might be willing to forgive implementation errors will not accept the deliberate introduction of security and privacy risks. There can be little question that XCP's rootkit functionality, the installation without consent of MediaMax software, the lack of uninstallers, and phone-home behavior were put in place deliberately by the vendors.

Third, when the vendors did make apparent implementation errors, the errors were compounded by the products' aggressive installation and reluctant uninstallation mechanisms. For example, the file permission problem discovered by Burns and Stamos was difficult to fix because the MediaMax autorun program aggressively reset the permissions to dangerous values, without asking the user for permission, every time a disc was inserted. Similarly, the vendors' apparent desire to limit use of their uninstallers led to designs that relied on downloading code using ActiveX controls—leaving users just one bug away from critical code-download vulnerabilities.

These factors led some users to conclude that Sony-BMG and the DRM vendors not only put their own busi-

ness interests ahead of their customers' interests, but also made deliberate choices that endangered customers' security and privacy. Users who would have forgiven a few implementation mistakes by a well-intentioned vendor were not so quick to forgive when they felt the vulnerabilities were less than accidental.

Though Sony-BMG and other copyright owners will presumably tread more carefully in the future, there remains a fundamental tension between DRM vendors' desire to control and limit how computers are used, and the need of users to manage their own systems. Users and DRM distributors will continue to struggle for control of users' computers.

11 Conclusion

Our analysis of Sony-BMG's CD DRM carries wider lessons for content companies, DRM vendors, policymakers, end users, and the security community. We draw six main conclusions.

First, the design of DRM systems is driven strongly by the incentives of the content distributor and the DRM vendor, but these incentives are not always aligned. Where they differ, the DRM design will not necessarily serve the interests of copyright owners, not to mention artists.

Second, DRM, even if backed by a major content distributor, can expose users to significant security and privacy risks. Incentives for aggressive platform building drive vendors toward spyware tactics that exacerbate these risks.

Third, there can be an inverse relation between the efficacy of DRM and the user's ability to defend her computer from unrelated security and privacy risks. The user's best defense is rooted in understanding and controlling which software is installed, but many DRM systems rely on undermining this understanding and control.

Fourth, CD DRM systems are mostly ineffective at controlling uses of content. Major increases in complexity have not increased their effectiveness over that of early schemes, and may in fact have made things worse by creating more avenues for attack. We think it unlikely that future CD DRM systems will do better.

Fifth, the design of DRM systems is only weakly connected to the contours of copyright law. The systems make no pretense of enforcing copyright law as written, but instead seek to enforce rules dictated by the label's and vendor's business models. These rules, and the technologies that try to enforce them, implicate other public policy concerns, such as privacy and security.

Finally, the stakes are high. Bad DRM design choices can seriously harm users, create major liability for copyright owners and DRM vendors, and ultimately reduce artists' incentive to create.

Acknowledgments

We are grateful for the expert legal advice of Deirdre Mulligan and her colleagues at U.C. Berkeley: Aaron Perzanowski, Sara Adibisedeh, Azra Medjedovic, Brian W. Carver, Jack Lerner, and Joseph Lorenzo Hall. We are also grateful to Clayton Marsh at Princeton. Sadly, research of this type does seem to require support from a team of lawyers.

We thank the readers of Freedom to Tinker for their comments on partial drafts that we posted there; thanks especially to C. Scott Ananian, Randall Chertkow, Tim Howland, Edward Kuns, Jim Lyon, Tobias Robison, Adam Shostack, Ned Ulbricht, and several pseudonymous commenters. Jeff Dwoskin provided valuable technical assistance, and Shirley Gaw, Janek Klawe, and Harlan Yu gave helpful feedback. We are also grateful to the anonymous reviewers for their suggestions. Thanks to Claire Felten for help with copy editing.

This material is based upon work supported under a National Science Foundation Graduate Research Fellowship. Any opinions, findings, conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Notes

[1] As news of the rootkit spread, we added to the public discussion with a series of 27 blog posts analyzing XCP and MediaMax. This paper provides a more systematic analysis, along with much new information. Our original blog entries can be read at http://www.freedom-to-tinker.com/?cat=30&m=2005.

[2] Music industry *rhetoric* about DRM often focuses on P2P, and some in the industry probably still think that DRM can stop P2P sharing. We believe that industry decision makers know otherwise. The design of the systems we studied in this paper supports this view.

[3] Similar application blacklisting techniques have been used in other security contexts. The client software for World of Warcraft, a massively multiplayer online role playing game, checks running applications against a regularly updated blacklist of programs used to cheat in the game [12].

[4] An extreme extension of this would be to adopt rootkit-like techniques to conceal the copying application's presence, just as XCP hides its active protection software.

[5] Forging a mark is probably not copyright infringement. Unlike the musical work in which it is embedded, the mark itself is functional and contains little or no expression, and therefore seems unlikely to qualify for copyright protection. In principle, the mark recognition process could be covered by a patent, but we are unaware of any such patent relating to XCP or MediaMax. Even if the vendor does have a legal remedy, it seems worthwhile to design the mark to prevent forgery if the cost of doing so is low.

[6] By locating the watermark nearly five seconds after the start of the track rather than at the very beginning, MediaMax reduces the likelihood that it will occur in a very quiet passage (where it might be more audible) and makes cropping it out more destructive.

[7] This design seems to be intended to lessen the audible distortion caused by setting one of the bits to the watermark value. The change in the other two bits reduces the magnitude of the difference from the

original audio sample, but it also introduces a highly uneven distribution in the three least significant bits that makes the watermark easier to detect or remove.

[8]The restrictions imposed by the DRM players only loosely track the contours of copyright law. Some uses that could be prohibited under copyright—such as burning three copies to give to friends—are allowed by the software, while some perfectly legal uses—like transferring the music to one's iPod—are prevented.

[9]This file is hidden and protected by the XCP rootkit. Before the user can access the file, the rootkit must be disabled, as described in Section 7.2. We did not determine how the MediaMax player stores the number of copies remaining.

[10]The rootkit also hooks `NtOpenKey` but does not alter its behavior.

[11]Users could also mislead the DRM software about the date and time, but most users with the inclination to do that would probably just remove the DRM software altogether.

References

[1] Class action complaint. In *Hull et al. v. Sony BMG et al.*, 2005. http://www.eff.org/IP/DRM/Sony-BMG/sony_complaint.pdf.

[2] Consolidated amended class action complaint. In *Michaelson et al. v. Sony BMG et al.*, 2005. http://sonysuit.com/classactions/michaelson/15.pdf.

[3] Original plantiff's petition. In *State of Texas v. Sony BMG Music Entertainment*, 2005. http://www.oag.state.tx.us/newspubs/releases/2005/112105sony_pop.pdf.

[4] Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman. The Darknet and the future of content distribution. In *ACM Workshop on Digital Rights Management*, November 2002.

[5] Jesse Burns and Alex Stamos. Media Max access control vulnerability, November 2005. http://www.eff.org/IP/DRM/Sony-BMG/MediaMaxVulnerabilityReport.pdf.

[6] Ingemar Cox, Joe Kilian, Tom Leighton, and Talal Shamoon. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12):1673–1687, 1997.

[7] Scott A. Craver, Min Wu, Bede Liu, Adam Stubblefield, Ben Swartzlander, Dan S. Wallach, Drew Dean, and Edward W. Felten. Reading between the lines: Lessons from the SDMI challenge. In *Proc. 10th USENIX Security Symposium*, August 2001.

[8] Edward W. Felten and J. Alex Halderman. Digital rights management, spyware, and security. *IEEE Security and Privacy*, January/February 2006.

[9] Allan Friedman, Roshan Baliga, Deb Dasgupta, and Anna Dreyer. Understanding the broadcast flag: a threat analysis model. In *Telecommunications Policy*, volume 28, pages 503–521, 2004.

[10] J. Alex Halderman. Evaluating new copy-prevention techniques for audio CDs. In *Proc. ACM Workshop on Digital Rights Management (DRM)*, Washington, D.C., November 2002.

[11] J. Alex Halderman. Analysis of the MediaMax CD3 copy-prevention system. Technical Report TR-679-03, Princeton University Computer Science Department, Princeton, New Jersey, 2003.

[12] Greg Hoglund. 4.5 million copies of EULA-compliant spyware, October 2005. http://www.rootkit.com/blog.php?newsid=358.

[13] Greg Hoglund and James Butler. *Rootkits: Subverting the Windows Kernel*. Addison-Wesley, 2005.

[14] Kazumasa Itabashi. Trojan.Welomoch technical description, December 2005. http://securityresponse.symantec.com/avcenter/venc/data/trojan.welomoch.html.

[15] Yana Liu. Backdoor.Ryknos.B technical description, November 2005. http://securityresponse.symantec.com/avcenter/venc/data/backdoor.ryknos.b.html.

[16] MediaMax Technology Corp. Annual report (S.E.C. Form 10-KSB/A), September 2005.

[17] Microsoft Corporation. Windows Media data session toolkit. http://download.microsoft/com/download/a/1/a/a1a66a2c-f5f1-450a-979b-ddf790756f1d/Data_Session_Datasheet.pdf.

[18] Matti Nikki. Muzzy's research about Sony's XCP DRM system, December 2005. http://hack.fi/~muzzy/sony-drm/.

[19] K. Reichert and G. Troitsch. Kopierschutz mit filzstift knacken. *Chip.de*, May 2002.

[20] Mark Russinovich. More on Sony: Dangerous decloaking patch, EULAs and phoning home, November 2005. http://www.sysinternals.com/blog/2005/11/more-on-sony-dangerous-decloaking.htm.

[21] Mark Russinovich. Sony, rootkits and digital rights management gone too far, October 2005. http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html.

[22] Sony-BMG Music Entertainment. Portable device: iPod information. http://cp.sonybmg.com/xcp/english/form10.html.

[23] Sony-BMG Music Entertainment. XCP frequently asked questions. http://cp.sonybmg.com/xcp/english/faq.html.

Comment of:
Edward W. Felten
Professor of Computer Science and Public Affairs
J. Alex Halderman
Department of Computer Science
35 Olden Street
Princeton, NJ 08544
Princeton University

Represented by:
Deirdre K. Mulligan
Director
Aaron Perzanowski
Law Clinic Intern
Samuelson Law, Technology & Public Policy Clinic
Boalt Hall
University of California
346 North Addition
Berkeley, CA 94720-7200

Office of the General Counsel
U.S. Copyright Office
James Madison Memorial Building, Room LM-401
101 Independence Avenue, SE.
Washington, DC 20559-6000

December 1, 2005

Re: RM 2005-11 – Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies

I. Proposed Class Of Works

We respectfully request an exemption to § 1201(A)(1)(a) for sound recordings and audiovisual works distributed in compact disc format and protected by technological measures that impede access to lawfully purchased works by creating or exploiting security vulnerabilities that compromise the security of personal computers. The creation of security vulnerabilities includes running or installing rootkits or other software code that jeopardize the security of a computer or the data it contains. The exploitation of security vulnerabilities includes running or installing software protection measures without conspicuous notice and explicit consent and failing to provide a permanent and complete method of uninstalling or disabling the technological measure.

II. Summary of Argument

Technological measures protecting works distributed on Compact Discs have been found to pose unreasonable security risks to consumers' personal computers, corporate and government networks and the information infrastructure as a whole. Vulnerabilities inherent in widely distributed CD protection measures create the potential for a frightening range of abuses. Viruses and Trojan horses are already leveraging these technologies to hide from antivirus programs and system administrators. Exacerbating the unacceptable risks posed by these technological protection measures, is that fact that the uninstallers provided to remove these measures pose additional security risks allowing a malicious web site to hijack a consumer's computer.

Security holes of this sort are regularly exploited by criminals. They may be used to turn the computer against its owner by sniffing passwords (including login information for financial sites), stealing business secrets and confidential data, and even holding the data on the PC for ransom. Such weaknesses also serve as launching points for attacks on third parties. Attackers can use such holes to penetrate otherwise secure home or corporate networks. Criminals can use them to enlist thousands of machines, unbeknownst to their owners, into massive "botnets"—armies of so called "zombie" computers—which are directed to relay spam (including pornographic messages) or conduct crippling distributed denial of service (DDOS) attacks. Past targets have included corporations and national security assets, including the infrastructure of the Internet itself. Zombies may also be used to relay anonymous messages and hide the activities of cyber criminals, including terrorist organizations, from law enforcement.

The security holes created by these protection measures force consumers to choose between two equally unappealing options: to accept intolerable security risks in order to access lawfully purchased CDs[1] or to circumvent the protection measures in order to gain lawful access *and* maintain a safe computing environment. This is a Faustian bargain. If consumers choose to listen they open their own systems as well as the broader Internet to countless security risks. The proposed exemption would allow users to take steps to ensure the security of their computers while enjoying access to the CDs they purchase without fear of liability under the DMCA for circumventing protection measures that undermine computer security.

[1] In addition to creating security risks, these technical protection measures interfere with lawful and customary uses of audiovisual works, limiting the ability of lawful purchasers to shift formats, choose listening platforms, and "shuffle" music tracks in order of their liking. Some of these programs invade privacy by actively collecting data about the in-home use of copyrighted works.

III. The Submitting Parties

Edward W. Felten is a Professor of Computer Science and Public Affairs at Princeton University. Professor Felten's groundbreaking computer security research has established him as one of the field's leading experts, and his ongoing technology policy research addresses developing concerns regarding the legal regulation of technology and innovation. The DMCA has played a particularly important role in Professor Felten's research activities. In 2000, he and a team of researchers, after accepting a challenge from the Secure Digital Music Initiative (SDMI), succeeded in breaking SDMI's digital audio watermark. After facing legal threats under the DMCA, Professor Felten filed for declaratory judgment seeking a determination that his research did not violate the DMCA. Only after the RIAA disavowed any intent to file suit was that action dismissed.

J. Alex Halderman is a computer science Ph. D. candidate and researcher at Princeton University. His computer security and privacy research encompasses a variety of topics, but focuses particularly on the threats introduced by access and copy protection measures. In 2003, he published an academic paper discussing his research on SunnComm's MediaMax protection measure. Shortly thereafter, SunnComm threatened Halderman with legal action for his academic publication. After scathing criticism of its attempt to silence legitimate research, SunnComm publicly retracted this threat.

IV. The Technological Protection Measures

For most of their twenty-five year history, audio Compact Discs (CDs) have been freely accessed and used by consumers who legally purchase them. Increasingly, however, record labels have sought to exercise greater control over consumers' access and post-sale uses of CDs. Although the particular protection measures employed to control access and use vary between labels and even between titles, these measures can be broadly categorized as either passive or active. Passive protection measures rely on changes to the structure of the data contained on the CD, such as inaccurate Tables of Contents, to assure compatibility with traditional audio CD players while preventing access and controlling use of the same CDs on many personal computers. In contrast, active protection measures, the focus of this comment, rely on the installation of software on the consumer's computer to prevent certain forms of access and use of audio files.

The current breed of active technological protection measures rely almost invariably on the AutoRun feature of the Windows operating system for initial installation. AutoRun allows software code contained on removable media like CDs to run automatically when inserted into a computer. Using AutoRun a CD can automatically install software on a computer without the knowledge or consent of its owner. In the context of CD protection measures, the software installed using AutoRun often includes a device driver that limits the functionality of the consumer's CD-ROM drive, preventing consumers from playing or copying their CD and creating the security risks described above. The current active technological protection measures exploit this aspect of AutoRun, because most consumers would prefer the freedom to make personal backup copies, listen to tracks in order of their preference, or transfer CDs to iPods or other

portable media players and are therefore reluctant to install software that would limit these lawful activities. Absent the installation of the this software, the CD format by nature allows consumers to freely access and use CD audio files.[2]

Once the consumer's CD-ROM drive has been altered, these protection measures typically present an End User License Agreement (EULA) detailing the permitted and prohibited uses of the CD. If the consumer "accepts" the EULA terms, these protection measures install software that the consumer may use to play the CD and copy DRM-protected Windows Media files. These files, unlike MP3 files, cannot be copied to portable media players like Apple's iPod. Most importantly the acceptance of the EULA and installation of this software introduces gaping holes in system security leaving the personal computer, and the networks it can be triggered to attack, open to a range of malicious activity. If instead, the consumer refuses the terms of the EULA, the disc is ejected and she is left unable to listen to her lawfully purchased CD on her computer.[3]

These protection measures have created serious threats to the security of personal computers, private and public networks, and the Internet generally, forcing consumers to choose between lawfully accessing the CDs they purchase and risking a hostile takeover of their computers. A protection measure called XCP developed by First4Internet and included in several million CDs distributed by Sony BMG included a rootkit, a software tool, the use of which is virtually unheard of in legitimate software development, designed to hide processes and files from computer users. Not only did this rootkit hide other components of Sony BMG's protection measure (ostensibly to render their removal more difficult), but it also created a serious security risk easily exploited by malicious hackers. Within days of the discovery of the rootkit, malicious code that took advantage of the rootkit's cloaking capabilities were being spread across the Internet.[4] Since millions of the CDs had been installed on some 500,000 computer networks[5] (including military, government, and business networks), the rootkit resulted in a major security threat to both individual consumers' personal computers and the nation's information infrastructure.

---

[2] Protected CDs often include "bonus" or "enhanced" multimedia content, such as music videos, in addition to audio content. We argue that the audiovisual works contained on CDs should fall within the exempted class of works as well.

[3] Although no court has determined that the active protection measures employed by protected CDs "effectively control access" to the discs' contents, this comment assumes—solely for the purpose of this rulemaking—that, at least for those users of the Windows operating system who have enabled the AutoRun feature, the protection measures described above are effective in controlling access to the audio files contained on those CDs.

[4] *Backdoor. Ryknos*, http://securityresponse.symantec.com/avcenter/venc/data/backdoor.ryknos.html.

[5] Paul F.Roberts, *Sony's 'Rootkit' Is on 500,000 Systems, Expert Says*, http://www.eweek.com/article2/0,1895,1887181,00.asp (Nov. 15, 2005).

Nearly a month after it first learned of the dangers posed by its rootkit,[6] and only after unrelenting pressure from consumers, security researchers, and the press, Sony BMG provided a program to uninstall the XCP rootkit. Unfortunately this uninstaller was fraught with security flaws even more dangerous than the original rootkit technology, allowing any webpage a user visits to secretly install or run code on her computer.[7] Subsequently, Sony BMG announced a recall of the effected CDs and, in recognition of the valuable contribution of security researchers, promised to forego potential DMCA claims against those engaged in legitimate research on its protection measures.[8] Despite the recall several organizations, among them the Electronic Frontier Foundation, filed class action lawsuits against Sony.[9] Finally, Texas Attorney General Greg Abbott filed suit against Sony BMG for violations of that state's anti-spyware legislation.[10]

Other measures that protect releases by Sony BMG and other labels, including SunnComm's MediaMax technology, permanently install software despite the consumer's explicit rejection of the software EULA.[11] This same protection measure collects and transmits data about consumers despite statements in both the software EULA and SunnComm's website denying any such behavior.[12] Not only must users fear surreptitious installation of software that compromises security and privacy, they must also fear deliberate disregard of their choice not to install unwanted software. Simply by placing a CD in their computer, consumers are exposed to potential security breaches even if they refuse to install the protection measures necessary to access their lawfully purchased CDs.

Sony BMG's rootkit and SunnComm's MediaMax software demonstrate the dangers of irresponsible attempts to protect copyrighted content. Software that sacrifices the security of consumers' computers and ignores their explicit refusal to install such software in order to increase control over the uses of CDs made by lawful purchasers creates unnecessary and unacceptable risks. These risks are compounded by software that installs without conspicuous notice and explicit consent, particularly when that software does not include a safe and effective method of permanent uninstallation. Unless

---

[6] See Steve Hamm, *Sony BMG's Costly Silence*, http://www.businessweek.com/technology/content/nov2005/tc20051129_938966.htm (Nov. 29, 2005).

[7] Ed Felten and J. Alex Halderman, *Sony's Web-Based Uninstaller Opens a Big Security Hole; Sony to Recall Discs*, http://www.freedom-to-tinker.com/?p=927 (Nov. 15, 2005).

[8] Letter from Jeffrey P. Cunard to Robert S. Green, Nov. 18, 2005, http://www.eff.org/IP/DRM/Sony-BMG/sony_response.pdf.

[9] Matt Hines, *EFF Takes Action Against Sony BMG*, http://www.eweek.com/article2/0,1895,1891843,00.asp (Nov. 21, 2005).

[10] *Attorney General Abbott Brings First Enforcement Action In Nation Against Sony BMG For Spyware Violations*, http://www.oag.state.tx.us/oagnews/release.php?id=1266&PHPSESSID=m0af3v583ms482pstg39o16lq6 (Nov. 21, 2005).

[11] J. Alex Halerman, *MediaMax Permanently Installs and Runs Unwanted Software, Even If User Declines EULA*, http://www.freedom-to-tinker.com/?p=936 (Nov. 28, 2005).

[12] Congress explicitly allowed the circumvention of technological measures that exhibit this sort of privacy–invasive behavior in 17 USC § 1201(i).

consumers are permitted to circumvent technological measures that create such risks, they will be forced to choose between maintaining the security of their computers and enjoying their lawfully purchased CDs.

V. The Adversely Affected Non-Infringing Activity

The technological measures described above adversely affect at least four varieties of non-infringing uses: (1) listening, (2) engaging in security research, (3) device and format shifting, and (4) creating backups.

A. Listening

The act of listening to a CD on a personal computer is lawful under any reading of the Copyright Act. Playing a CD on a computer for one's personal enjoyment implicates none of the exclusive rights granted to copyright holders under § 106. No copies are made or distributed; no derivative works are prepared; and no works are publicly performed. Nonetheless, without an exemption rational consumers would be dissuaded from engaging in this unquestionably lawful activity in light of the security risks posed by protection measures that are a barrier to access.

Without the proposed exemption, millions of computer users will be forced to risk the potential security threats created by protection measures like Sony BMG's rootkit in order to simply listen to their lawfully purchased CDs. For the millions of Windows users who have not opted to disable the default-enabled AutoRun feature,
playing their CDs on their computers requires the installation of technological protection measures. In order to access their lawfully purchased CDs, these consumers must endure potentially crippling security breaches like those created by Sony BMG's rootkit, that allow malicious code authored by third parties to run imperceptibly on consumers' computers or risk other equally dangerous undiscovered threats.

B. Engaging in Security Research

Without the efforts of security researchers who discover and publicize risks such as those created by Sony BMG's rootkit, consumers would be nearly universally uninformed about the security threats they face. As Sony BMG's month-long delay in responding to the revelation of the dangers created by its rootkit demonstrate, consumers cannot rely on copyright holders to react with speed in providing information about the dangers of the software they foist on consumers. Thomas Hesse, Sony BMG's President of Global Digital Business appears to have summed up the attitude of copyright holders when he asked, "Most people, I think, don't even know what a rootkit is, so why should they care about it?" The vast majority of computer users lack the expertise to discover these threats independently. As a result, consumers must either rely on the research conducted by security experts or blindly trust software developers and content owners to exercise restraint in designing protection measures that respect consumers' security interests.

Unfortunately, the DMCA's anti-circumvention provision chills the efforts of security researchers. Because of the narrow scope of the DMCA's research exemption, the security researchers who are best situated to discover and disclose serious threats to personal computers face uncertain liability for their activities. In their efforts to determine the security threats posed by these protection measures, these researchers are likely to disable or remove some portion or the entirety of the protection measure, and thus potentially run afoul of the DMCA.

Researchers like Professor Edward Felten and Alex Halderman waste valuable research time consulting attorneys due to concerns about liability under the DMCA. They must consult not only with their own attorneys but with the general counsel of their academic institutions as well. Unavoidably, the legal uncertainty surrounding their research leads to delays and lost opportunities. In the case of the CDs at issue, Halderman and Felten were aware of problems with the XCP software almost a month before the news became public, but they delayed publication in order to consult with counsel about legal concerns. This delay left millions of consumers at risk for weeks longer than necessary.

Engaging in such research does not constitute copyright infringement. Security researchers are interested in the manner in which protection measures function and the security threats they may pose; they have no interest in the copyrighted content those measures are meant to protect. Copying of the CD audio files is often not even necessary to conduct their research.[13]

With no potential violations of § 106, the DMCA's ban on circumvention simply functions as a barrier to legitimate and publicly valuable research. As the ongoing spyware crisis has demonstrated, the efforts of independent researchers are crucial to maintaining a safe computing environment. An exemption for the above-described class of works would enable research that would help to ensure the security of consumers' personal computers.

C. Device and Format Shifting

While we recognize that the purpose of this rulemaking is to consider exemptions to the DMCA's prohibition against circumvention of access controls, the dual function of the protection measures at issue requires consideration of their affect on lawful copying as well. The active protection measures used on CDs typically control both access and use, including copying, of audio content. Because of the dual function of these protection measures, many consumers are prevented from creating lawful copies of their CDs despite the absence of a prohibition against circumventing copy controls in the DMCA. As a result, consumers are unable to create personal copies of their CDs in the format of their choice. Instead, they are typically permitted only to access compressed and DRM-protected Windows Media (WMA) files.

[13] When such copying is necessary, it should be deemed a fair use.

This limitation on consumer choice is problematic for a number of reasons. First, the Windows Media files are incompatible with the Apple iPod, the dominant portable media player. As complaints lodged on Amazon.com demonstrate, the inability to transfer lawfully purchased music to an iPod, which supports only the MP3 and AAC audio formats, is a pressing concern among consumers. Second, many users object to their inability to access an uncompressed digital copy of their purchased music. These audiophiles prefer to convert the Compact Disc Digital Audio (CDDA) files contained on their CDs to the WAV, SHN, or FLAC formats that, unlike lossy compressed standards like WMA and MP3, retain the highest digital fidelity.

Even for those consumers satisfied with the Windows Media file format, the presence of protection measures that satisfy the definition set out above interfere unreasonably with consumers' fair use rights to transfer CDs to other devices and convert them to other formats. Because the protection measures jeopardize security, many users will be unwilling to copy their CDs with the supplied software out of a justified fear of compromising the security of their computers.

Converting lawfully purchased CDs to other formats and transferring the resulting copies to another device are unquestionably fair uses. Even the record industry itself admits that both of these activities are lawful. Before the Supreme Court of the United States during the oral argument in Metro-Goldwyn-Mayer v. Grokster, counsel for the copyright holders explained, "The record companies, my clients, have said, for some time now, and it's been on their Website for some time now, that it's perfectly lawful to take a CD that you've purchased, upload it onto your computer, put it onto your iPod. There is a very, very significant lawful commercial use for that device, going forward."

Analysis of the four fair use factors supports this conclusion. First, the character of the use, while not transformative, is non-commercial. Consumers who transfer CDs to their iPods do so for their own enjoyment and not for any commercial gain. Similarly, the court in *Sony v. Universal Studios* determined that this first factor weighed in favor of fair use when considering non-commercial time shifting of over the air television broadcasts by VCR owners. The second factor, the nature of the copyrighted work, weighs against fair use because the sound recordings at issue here are entitled to full protection of copyright law. The third factor, too, weighs against fair use since consumers typically copy the entire work when format and device shifting. However, factors two and three are typically given relatively little weight in the overall fair use analysis. Finally, the fourth factor supports a finding of fair use. As portable electronic devices continue to displace traditional means of listening to music, the value of a copyrighted work increases as it becomes easier to use on a variety of platforms. From the perspective of consumers, music that cannot be played on the device of their choice is less valuable. In recognition of this fact, record labels and artists routinely instruct users on how to circumvent their own protection measures to convert CDs to other formats. Given the relative weight of the first and fourth factor, the analysis heavily favors fair use.

D. Creating Backups

Just as the protection measures on CDs prevent many users from creating copies of audio content in other formats, they can also preclude consumers from creating backup copies of their CDs. Backup copies allow consumers to guard against damage, theft, or loss of the original CD media. True backup copies offer consumers functionality equivalent to the original media.

Although some protection measures allow consumers to copy CDs, these measures ensure that copies are of limited utility. These copies cannot be used to create additional backup copies in the event the original disc is damaged. Nor can these copies be used to copy DRM-protected files to the consumer's computer or portable player. As a result of the technological protection measure, these copies do not serve the same purpose as backup copies.

The creation of backup copies is lawful under copyright's fair use doctrine. Again, just as in *Sony*, the non-transformative non-commercial nature of backup copies supports a finding of fair use. Although both the nature of the copyrighted work and the amount copied weigh against fair use, these factors typically contribute little to the overall balancing of the fair use factors. Finally, the fourth factor weighs in favor if fair use. While record labels would undoubtedly appreciate the opportunity to sell consumers another copy of a CD should their original be damaged or stolen, the creation of personal archival copies is unlikely to harm the value of or market for the copyrighted works in question since the consumers in question have already purchased the CDs they hope to back up.

In addition, § 117 of the Copyright Act explicitly permits copying of the software contained on the CDs—the very software that restricts consumers' ability to access and copy their CDs. Consumers who purchase CDs are in lawful possession of the computer programs that serve as protection measures. Therefore, they are entitled under § 117(a)(2) to create archival copies of those programs.

Since copying the audio and other media files contained on the CDs constitutes a fair use and copying the software programs is permitted under § 117, creating backup copies of protected CDs in their entirety is a non-infringing activity.

VI. Statutory Considerations

As detailed below, consideration of each of the factors described in § 1201(a)(1)(C) supports exempting the above-described class of works from the DMCA's anti-circumvention provision.

A. Such factors as the Librarian considers appropriate

Because the primary concerns driving our request for this exemption do not fit easily within the other statutory considerations, we address § 1201(a)(1)(C)(v) first.

Protection measures like Sony BMG's rootkit pose a genuine threat to the security of both individual computer users and the network environment. Without providing notice or obtaining consent, Sony BMG installed software on the computers of millions of consumers that, unbeknownst to them, would enable any virus writer or computer hacker on the planet to secretly run programs on those consumers' machines. While consumers may expect this sort of behavior from spyware vendors, they did not — prior to this incident—expect the simple act of listening to a CD to result in effectively ceding control of their computers to the authors of malicious code.

By any objective evaluation of their characteristics, the XCP rootkit and SunnComm MediaMax protection measures would qualify as spyware. Both are installed without notification or consent, and both collect and transmit information about consumer usage without consent. In fact the primary distinction between these software programs and typical spyware applications is that, because of the DMCA, consumers and researchers may be legally prevented from removing and disabling dangerous and unwanted software. Such an outcome cannot be squared with Congressional intent in passing the DMCA. The DMCA was passed to protect the legitimate interests of copyright holders, not to prevent consumers from taking reasonable and necessary steps to ensure their own computing security. Because of the dangers posed by these protection measures, informed consumers must sacrifice lawful access to the works they purchase in order to secure their computing environment. Meanwhile less informed consumers will likely sacrifice both security and access by inadvertently installing these dangerous and restrictive protection measures.

B. Availability for use of copyrighted works

The proposed exemption will have no negative effect on the availability of copyrighted works. Instead, the exemption would likely increase the availability of those works.

The CD titles sold in protected format are typically unavailable in unprotected format in the United States. However, there is no reason to suspect that the CDs sold in protected formats would not be produced or sold if protection measures that create serious security risks to consumers could be circumvented. The vast majority of CDs sold contain no copy or access protection measures at all. Clearly the presence of protection measures is not a prerequisite for distributing a CD. Moreover, if protection measures were deemed a necessity for some titles, the proposed exemption would provide an incentive for the creation of protection measures that respect the security of consumers' computers while protecting the interests of the record labels.

The Sony BMG rootkit fiasco offers a telling example of the affect dangerous protection measures can have on the availability of copyrighted works. After public outcry forced a recall of several million CDs, the works of many artists are simply unavailable in most markets. During the busiest shopping season of the year, consumers are unable to purchase these CDs. By mitigating the damage suffered by consumers and

encouraging the development of safe protection measures, the proposed exemption would likely increase the availability of copyrighted works.

Given that consumers increasingly use computers and portable media players, rather than traditional Compact Disc players, to listen to the music they purchase, the proposed exemption would increase the availability of copyrighted works for high-demand uses. Many consumers purchase CDs primarily to convert them to compressed formats and transfer those files to portable devices like the iPod. To the extent the proposed exemption would enable such uses, more copyrighted works will be available for the uses that matter most to consumers. Without fear of security risks introduced by unwanted and unknown protection measures, these lawful uses are likely to become even more prevalent. By providing a disincentive to distribute dangerous protection measures, the proposed exemption would ensure the safety of purchasing and listening to music. Moreover, by allowing circumvention of these dangerous measures, the exemption would clarify the legality consumers' self-help efforts to ensure their security while enjoying their CDs. The added security, both technical and legal, provided by this exemption would likely spur an increase in the demand for and availability of copyrighted works distributed in CD format.

C. Availability for use of works for nonprofit archival, preservation, and educational purposes

The proprietary file formats and DRM schemes employed by the current breed of protected CDs face obsolescence in the future, some in the immediate future. Without the ability to archive the contents of CDs in the format of their choice, archivists risk the creation of stockpiles of data that may prove unreadable in a decade. An exemption would enable archivists to preserve protected CDs that fall within the class in the format of their choice.

Perhaps more importantly, an exemption would free archivists from the security risks posed by these protection measures. Archivists, because of the volume of material they process, face an increased likelihood of exposure to a variety of security risks introduced by security-compromising protection measures. These security risks are perhaps of even greater significance in the archival context since technologies like Sony BMG's rootkit could endanger the entire archive. An exemption would permit archivists to continue their efforts to preserve digital artifacts without risking the deleterious effects of security breaches.

D. Impact of the prohibition on the circumvention has on criticism, comment, news reporting, teaching, scholarship, and research

Research of the sort likely to expose security flaws created by protection measures like Sony BMG's rootkit often involves activities that could give rise to anti-circumvention claims under the DMCA. As a result, the pace and scope of research in this field has suffered. Absent research that first identifies security risks, debate and criticism of the tactics of copyright holders is necessarily stifled. The DMCA's ban on

circumvention functions as an effective barrier to research that would otherwise lead to increased consumer and industry awareness of serious security risks posed by certain software-based protection measures.

The authors of this comment have first hand knowledge of the chilling effect of potential liability under the DMCA on research and criticism. If the exemption we propose had been law just a few months ago, the discovery and disclosure of Sony BMG's rootkit technology would have undoubtedly come much sooner. The public outcry, expert discussion, and industry reaction likewise would have proceeded on a shorter timeline. Given the potentially dire consequences of mass-distributed malware such as Sony BMG's rootkit, research delays created by uncertain legal liability should be minimized. In short, researchers should busy themselves with discovering and disclosing security threats and not with engaging in protracted discussions of the DMCA with their attorneys.

E. Effect of circumvention of technological measures on the market for or value of copyrighted works.

Circumvention of technological measures protecting the above-described class are unlikely to prove detrimental to the market for or value of copyrighted works. Copyright holders derive little if any additional value from the presence of these protection measures. In fact, the real and perceived dangers of protection measures like Sony BMG's rootkit are likely to substantially detract from the value of those works. Perhaps most importantly, since the proposed exemption includes only those protection measures that create or exploit security risks or ignore consumers' decisions not to install the protection measure, the impact of the exemption could be easily avoided by the creation of protection measures that do not pose these threats to consumers.

As the software developers and record labels that create CD protection measures admit, they are intended to function merely as "speed bumps." While they cannot prevent all unlicensed copying of the audio content of CDs, they may sometimes succeed in restricting the uses that unsophisticated computer users can make of copyrighted works. But the utility of these protection measures is severely limited under a variety of circumstances. For Mac and Linux users, these protection measures are often entirely inoperative. Even on Windows, the effectiveness of these measures depends in large part on the easily disabled AutoRun feature. Regardless of their usefulness for the average computer user, for determined pirates, these technological measures create little if any "speed bump" affect. Preliminary data shows that protected CDs are just as widely available on peer-to-peer networks as their unprotected counterparts.[14]

Moreover, any added value to copyrighted works gained by these protection measures is already significantly undermined by copyright holders' own policies. The

[14] Of course, even if an exemption is granted copyright law still prohibits infringing distribution of the content of these CDs. Just as copyright's exclusive rights—coupled with secondary liability under *Sony* and *Grokster*—have proven sufficient to protect the market for and value of unprotected CDs, they will offer protection for works under this proposed exemption.

labels and the artists they represent have gone to great lengths to inform unsatisfied customers of methods by which they can create DRM-free digital copies of their CDs. Posts on artists' and labels' websites as well as technical support emails from the labels offer step by step instructions that undercut any beneficial effects on the value of or market for these works. While the conciliatory efforts of artists and record labels demonstrate the limited necessity and value of these protection measures, consumers should not be forced to rely on the discretionary good faith efforts of copyright holders in order to engage in lawful activity free from the fear of security threats.

Not only is the proposed exemption unlikely to detract from the value of the copyrighted works within the above-described class, it would likely increase the value of those works to both the copyright holders and the public. Even if some copyright holders believe, protection measures are necessary to profitable distribution of music, protection measures that compromise security only serve to devalue both their DRM systems and the works they are meant to protect. The public controversy surrounding the Sony rootkit debacle has shaken consumer confidence in the safety of Sony BMG's products and CD protection measures generally. The proposed exemption would help to restore confidence that lawfully purchased CDs will not harm consumers' computers. An exemption would help ensure that such measures are less likely to be employed in the future and that if they are, they can be discovered removed without fear of liability. The restored consumer confidence and increased CD sales resulting from the proposed exemption would help rather than harm the value of these works.

VII. Conclusion

As the Department of Homeland Security cautioned copyright holders in reaction to Sony BMG's rootkit, "It's very important to remember that it's your intellectual property -- it's not your computer. And in the pursuit of protection of intellectual property, it's important not to defeat or undermine the security measures that people need to adopt in these days."[15] The proposed exemption, in keeping with the Congressional intent underlying the DMCA, would allow consumers to undertake the sort of self-help measures necessary to access and lawfully use the CDs they purchase without accepting unnecessary risks created by carelessly designed protection measures. For these reasons, we respectfully request that the Copyright Office recommend this proposed exemption.

[15] Michael Geist, *Sony's long-term rootkit CD woes*, http://news.bbc.co.uk/2/hi/technology/4456970.stm (Nov. 21, 2005).