Analysis of the MediaMax CD3 Copy-Prevention System

John A. Halderman
Department of Computer Science
Princeton University

Version 1.1 - October 6, 2003

Abstract. MediaMax CD3 is a new copy-prevention technique from SunnComm Technologies that is designed to prevent unauthorized copying of audio CDs using personal computers. SunnComm claims its product facilitates "a verifiable and commendable level of security," but in tests on a newly-released album, I find that the protections may have no effect on a large fraction of deployed PCs, and that most users who would be affected can bypass the system entirely by holding the shift key every time they insert the CD. I explain that MediaMax interferes with audio copying by installing a device driver the first time software from the CD is executed, but I show that this provides only minimal protection because the driver can easily be disabled. I also examine the digital rights management system used to control access to a set of encrypted, compressed audio files distributed on the CD. Although restrictions on these files are more relaxed than in prior copy protected discs, they still prohibit many uses permitted by the law. I conclude that MediaMax and similar copy-prevention systems are irreparably flawed but predict that record companies will find success with more customer-friendly alternatives for reducing infringement.

The most recent version is available online at http://www.cs.princeton.edu/~jhalderm/cd3/.

1. INTRODUCTION

Several recent news reports (AFP [1], Washington Post [2], USA Today [3], AP [4], Arizona Republic [5], LA Times [6], CNet News [7]) describe a new copy-prevention method that has been applied to an album by Anthony Hamilton released by BMG on September 23. This system, called *MediaMax CD3*, was created by SunnComm Technologies, the producers of the first-generation copy-prevention system *MediaCloQ*. Discs manufactured with SunnComm's new technique include two versions of the music, each protected in a different way. One set of songs are CD audio tracks that play in standard CD players but are supposed to be difficult for computers to copy. The second set are compressed, encrypted Windows Media files that employ digital rights management (DRM) to restrict how they are used. Music producers hope that the combination of these technologies will help reduce illegal copying while still allowing legitimate customers to play songs on their PCs, but this can only be achieved if both components are secure.

In this report, I explain how MediaMax functions, analyze the weaknesses of its design, and discuss its implications for the debate about CD copy protection and the problem of copyright infringement. I find that although SunnComm has gone to great lengths to respond to criticisms of earlier systems, MediaMax still prohibits many uses of the recording that are allowed under law. At the same time, the system's protections are so weak that they are unlikely to cause any significant reduction in copying.

2. PHYSICAL DESCRIPTION

I bought the recording *Comin' From Where I'm From* by Anthony Hamilton (Arista Records/BMG) from Amazon.com and received it on September 25. The disc contains twelve tracks for approximately 52 minutes of listening time.

The album cover has a sticker with this message:

> This CD is protected against unauthorized duplication. It is designed to play on standard playback devices and an appropriately configured computer (see system requirements on back). If you have questions or concerns visit www.sunncomm.com/support/bmg.

The hyperlink points to a FAQ that explains that the audio tracks are protected against copying and provides solutions for common problems accessing the disc's DRM-controlled content.

The following text is printed at the bottom of the back cover:

> THIS CD IS ENHANCED WITH MEDIAMAX SOFTWARE. Windows Compatible Instructions: Insert disc into CD-ROM drive. Software will automatically install. If it doesn't, click on "LaunchCd.exe." MacOS Instructions: Insert disc into CD-ROM drive. Click on "Start." Usage of the CD on your computer requires your acceptance of the End User License Agreement and installation of specific software contained on the CD. Windows System Requirements: Windows 98/2000/XP, Internet Explorer 5.5 or later, Windows Media Player 7.1 or compatible player. Mac System Requirements: Mac OSX 10.1, Power Mac G3/G4, iMac, eMac, Powerbook G3/G4, iBook with 128 Mb of RAM, Windows Media Player for Mac OSX, Internet Explorer 5.2, Monitor capable of displaying 800x600 screen resolution & 256 colors (64K colors recommended), 12x or faster multi-session-enabled CD-ROM drive, Flash Player 6. Digital files on this CD will also play on portable devices supporting secure WMA files. Certain computers may not be able to access the enhanced portion of this disc. None of the manufacturers, developers, or distributor make any representation or warranty, or assumes any responsibility, with respect to the enhanced portion of this disc.

The "Compact Disc Digital Audio" logo is absent from the printed jacket and the face of the disc, but it is embossed in the plastic on the inside of the jewel case. The CD itself bears the warning: "This disc is protected against unauthorized duplication."

3. THE ANTI-COPY SYSTEM

One component of the MediaMax system is designed to make it difficult to extract CD audio tracks as unprotected audio files using a PC. Thwarting extraction would prevent users from copying the CD or uploading tracks to peer-to-peer networks. SunnComm has published strong-sounding but carefully worded statements about this technology's effectiveness. In a press release [8] dated August 27, they cite "external testing" that demonstrated "'an incredible level of security for the music,'":

> CD copy protection robustness tests were performed to determine the security level of the product against unauthorized copying of the digital content. This was completed using a large set of Microsoft Windows and Apple Macintosh computer systems in tandem with many of the known ripper programs available on the market today. The PMTC *[Professional Media Test Center]* determined that **none of the ripper programs used in the testing process was able to produce a usable unauthorized copy** of the protected CD yielding a verifiable and commendable level of security for the SunnComm product. *[Emphasis added.]*

I assert that these claims are patently deceptive. In practice, many users who try to copy the disc will succeed without even noticing that it's protected, and all others can bypass the protections *with as little as a single keystroke*.

To understand why, we can compare MediaMax to prior anti-copy systems like the ones I studied in my earlier report, "Evaluating New Copy-Prevention Techniques for Audio CDs" [9]. These systems rendered CDs incompatible with most computers by modifying the table of contents (TOC) or other data structures on the discs in ways that deviate from published standards. Although this effectively prevented copying in many PC configurations, it also reportedly caused incompatibility with some DVD players, video game systems, and car CD players. The resulting public outcry over these "broken" recordings forced manufacturers to redesign the protections.

MediaMax is a second generation copy-prevention system, and SunnComm claims in the same press release [8] that it "provide[s] playability on any consumer's playback system without exceptions or limitations." Such perfect compatibility can only be achieved by leaving the standard CD audio portion of the disc unprotected, so MediaMax uses another method to block PC-based copying. Analysis of the Anthony Hamilton album shows that this method is special software loaded from the CD that interferes with copy attempts.

Windows has a feature called "autorun" that automatically starts programs from CDs when they are inserted into the computer. If a MediaMax-protected CD is placed in a PC that has autorun enabled, Windows runs a file called `LaunchCD.exe` located on the disc. This program provides access to the DRM-controlled encrypted content, but it also loads a special device driver into the system's memory. On Windows 2000/XP, this driver is called `SbcpHid`. The `LaunchCD.exe` program also presents an end user license agreement (EULA). If the user ever clicks Accept to agree to the terms of the license, the MediaMax driver is set to remains active *even after* the computer is rebooted. The driver examines each CD placed in the machine, and when it recognizes the protected title, it actively interferes with read operations on the audio content. Similar methods are used to protect the tracks on Windows 98/ME and Mac OSX systems.

This behavior can be verified by loading then disabling MediaMax according to the following instructions:

Start with a Windows 2000/XP system with empty CD drives.

1. Click the Start button and select Control Panel from the Start Menu.
2. Double-click on the System control panel icon.
3. Select the Hardware tab and click the Device Manager button.
4. Configure Device Manager by clicking "Show hidden devices" and "Devices by connection," both from the View menu.
5. Insert the Anthony Hamilton CD into the computer and allow the SunnComm software to start. If MediaMax has never been started before on the same computer, the `SbcpHid` driver should appear on the list for the first time. However, on some systems Windows needs to be rebooted before the driver becomes visible.

At this point you can attempt to copy tracks from the CD with applications like MusicMatch Jukebox or Windows Media Player. Copies made while the driver is active will sound badly garbled, as in this 9-second clip [10].

Next, follow these additional steps to disable MediaMax:

1. Select the `SbcpHid` driver from the Device Manager list and click "Properties" from the Action Menu.
2. Click the Driver tab and click the Stop button to disable the driver.
3. Set the Startup Type to "Disabled" using the dropdown list.

With the driver stopped, you can verify that the same applications copy every track successfully. Setting the Startup Type to disabled prevents MediaMax from restarting when the computer is rebooted. It will remain deactivated until `LaunchCD.exe` is allowed to run again.

MediaMax's protections are ineffective because the driver program can easily be disabled or, depending on the system configuration, it might never be installed to begin with. As a result, audio content is vulnerable to copying in nearly all deployed systems. SunnComm's press release may be technically correct--if their testers always ran the MediaMax application before trying to copy audio, they likely would see protection in every case. However, in practice the software often fails to start, and when it does start, users can manually suppress it. Here are some examples:

- Computers running Linux or Mac OS 9 can't run the MediaMax software at all, so they can always copy the recording.
- Many users disable the autorun feature [11] (autostart on Mac OS), so their systems will be able to copy the disc unless the user manually launches MediaMax.
- **Windows users who haven't disabled autorun can suspend it when they play a SunnComm-protected disc by holding down the shift key for a few seconds while inserting the CD. They can then copy the data normally.** (This won't work if the driver is active because the user has accepted the SunnComm EULA or because MediaMax ran since the system booted. However, affected users can still copy the disc by manually disabling the driver using a procedure like the one above.)

In all these cases, the audio tracks are left unprotected.

These vulnerabilities will be difficult or impossible to repair. SunnComm's software can't take any corrective action if it isn't started, and all these flaws involve ways that it is prevented from running in the first place. To make matters worse, MediaMax, unlike earlier copy-prevention techniques, works entirely in software. This means a moderately skilled programmer could, in only a few minutes, write an application to watch for and unload the `SbcpHid` driver, neutralizing MediaMax's copy resistance while leaving all the disc's other features intact.

SunnComm's claims of robust protection collapse when subjected to scrutiny, and their system's weaknesses are not only academic. The Washington Post story [2] notes that a key test of the disc's copy-prevention abilities would be how long after its release the tracks appeared on peer-to-peer music trading networks. I searched Kazaa on September 27, when the album had only been on sale for four days, and already all the songs were available for download. If SunnComm or BMG really believed this disc was difficult to copy, then its actual weakness should be as embarrassing as the discovery in 2002 that Sony's key2audio scheme can be defeated using only a felt-tipped pen [12].

4. THE DRM RESTRICTIONS

While one component of the MediaMax system tries to protect the disc's audio tracks from copying, a second component permits limited use of the recording subject to the control of a digital rights management framework. Some earlier anti-copy schemes also allowed playback of encrypted tracks, but these employed less sophisticated content protection methods. Users were generally restricted to playing the tracks through a proprietary player and only while the disc was in the drive. MediaMax allows a broader range of uses by employing true DRM techniques.

The protected disc includes Windows and Mac formatted data sessions that contain compressed, encrypted Windows Media audio (WMA) recordings of the tracks along with SunnComm's proprietary MediaMax software. After launching the driver software discussed in the previous section, the MediaMax application obtains and manages digital "licenses" the allow playback and other limited operations on the WMA files. When MediaMax loads, it presents an end user license agreement (EULA) [10]. If the user declines the EULA or closes the window, the software ejects the CD. However, users can simply ignore the EULA window and start other applications on top of MediaMax.

For the time being I've decided not to accept the EULA, so I can't access the software to evaluate it further. The agreement contains a number of terms that are undesirable from my position as a security researcher, including:

> II. You will not reverse engineer, decompile, disassemble or otherwise tamper with or modify the Digital Content;

and

> 1.3. Except as expressly provided herein, you shall not copy, modify, reproduce, sell, distribute or otherwise transfer the Digital Content. You may not reverse engineer, decompile, translate, adapt or disassemble the Digital Content or the software contained in it and/or on this CD.

Interestingly, the EULA also states:

> 1.2. Your rights to use the Digital Content are conditioned on your ownership of a license to use and possession of the original Compact Disc (CD) media and are terminated in the event you no longer own or possess the original CD media.

This apparently prohibits using copied tracks as backups in case the original disc is lost, stolen, or destroyed.

The SunnComm privacy policy [10] is featured prominently among the documents included on the disc. It promises: "No personal information is required from you. Since we don't collect it, we cannot store it or sell it." However, SunnComm also reserves the right to modify the policy, and it's unclear whether they are the only party with an opportunity to gather data when users download playback licenses.

Without accepting the EULA I can't personally evaluate the rights and restrictions placed on the WMA files. However, SunnComm's documentation and reports in the press indicate that users are permitted to:

- Copy tracks to the hard drive for playback without the original CD
- Burn tracks to CDs up to 3 times
- Share the songs with others by emailing them links to DRM-controlled tracks that expire after 10 days
- Download tracks to DRM-enabled portable players

The disc also contains a readme file [10] that describes some restrictions in more detail:

> 1. You may only download and use the digital keys *[licenses]* on a personal computer designated for your own private use.
> 2. Other than your PC, you may only use the content on compliant software players and/or compliant portable devices.
> 3. The PC, software players, and portable devices must be compliant with current security standards and compatible with the technology that is used to access, deliver, and secure the content.

It also mentions the capability to download to portable players, but this seems to be limited by a "Check-In - Check-Out" process to only three tracks at a time.

I'd appreciate detailed reports about the restrictions from others who choose to accept the license agreement. It would be especially interesting to know how much effort it takes to use the DRM system on typical PCs (i.e., whether additional software needs to be downloaded and installed, whether there are compatibility problems, etc.). I'm also curious if and how the MediaMax software restricts users from loading encrypted tracks onto multiple PCs from the original disc.

Since I haven't tried it myself, I can't comment on the security of SunnComm's DRM protections except to say that they are a misplaced effort. Even if MediaMax employs foolproof DRM to protect the encrypted files, its impact on illegal copying will be limited, since any user can work around the restrictions by copying the CD audio tracks. This should serve as a reminder for future DRM implementors that a security design is only as strong as its weakest component.

5. DISCUSSION

The anti-copying technology used on this CD can be broken with only minimal effort, but the album remains a landmark as one of the first widely distributed recordings to combine DRM technology with copy prevention software. In my view, it can be seen simultaneously as an olive branch for those who oppose CD copy prevention and a trojan horse to encourage wider acceptance of DRM.

Critics of copy-resistant CDs should acknowledge that this system differs from earlier products in several positive ways, though notable drawbacks certainly persist:

- MediaMax supports both Windows and Mac platforms, rather than only Windows (although Linux users are still locked out of the WMA content)
- The system distributes media in a standard format, WMA, enabling playback on multiple applications rather than a single proprietary player (though WMA is a closed standard, and the disc still includes a restrictive EULA that must be accepted before the files can be accessed)
- The CD audio portion of the disc is compatible with a wider range of playback devices than earlier protections since the tracks themselves are unmodified (although the WMA files can only be used on a limited number of devices that qualify as "secure")
- MediaMax allows users to copy the WMA files to their PCs so the songs can be played without the original disc (but the EULA seems to forbid using these files as backups in case the CD is lost)
- SunnComm has included a privacy policy that promises not to collect or sell user data (but it's unclear whether this data actually is being collected)
- The DRM controls permit burning tracks to CDs and downloading them to digital devices for time and space shifting (although the number of burned copies and downloaded tracks are severely limited)
- Perhaps most intriguingly, the system grants a small number of rights beyond what is generally regarded as fair use, allowing users to legally share trial copies of the songs by emailing links to time-limited downloads (but like any DRM system, the rights permitted by the software fall short of the flexible, evolving permissions understood as fair use, which necessarily depend on human judgment)

These concessions aside, MediaMax can also be viewed as an attempt to condition music customers to accept a greater level of industry control over how they use the recordings they buy. SunnComm CEO William Whitmore addressed concerns about MediaMax's restrictions in an article in the Washington Post [2]:

> People may say, 'Why would you restrict me to three copies?' Well, we could have made it zero copies. You have to balance your rights and privileges versus your obligations and responsibilities.

Most people agree that such a balance is essential to copyright, but many believe setting the balance should be the purview of courts and legislatures rather than media companies. Opponents of DRM worry that CDs with permissive rights management may lead to wider public acceptance of restricted recordings. Once the technology is accepted, the skeptics fear, record companies could tighten the restrictions with each new release until no fair use is permitted, and ultimately they could charge for every time a recording is played. This outcome would not be balance but unilateral producer control.

6. CONCLUSIONS

Record companies will evaluate anti-copy technologies by weighing their ability to reduce infringement against their drawbacks. For customers who prize fair use rights--like the ability to time and space shift recordings and to create compilations of the music they own--the limitations SunnComm's system places on these rights undermine the value of purchased music. This loss in value for music customers may fail to yield any benefit for the industry because of the weakness of anti-copy technologies. CD copy-prevention schemes that depends solely on software, as SunnComm's does, will be trivial to disable, and alternative strategies that modify the CD data format will invariably cause public outcry over incompatibility with legitimate playback devices.

Even if copy-resistant CDs make it harder for users to illicitly copy CDs they own, the technology will not necessarily reduce the overall incidence of copyright violation. Peter Biddle et al. of Microsoft have much to say about this topic in their paper, "The Darknet and the Future of Content Distribution" [13]. "Increased security (e.g. stronger DRM systems) may act as a disincentive to legal commerce," they suggest, by driving would-be customers to underground sources, such as peer-to-peer file trading networks, that provide media in unrestricted forms. No existing security technology can prevent copying in every case, so protected recordings will inevitably become available from these so-called "darknet" sources. Biddle concludes that for content producers to effectively compete against illicit distribution, they must work to provide "convenience and low cost rather than additional security."

If this theory is correct, the industry has the best chance of accomplishing its goals by giving customers more for their money and making it easier for them to buy music. I believe anti-copy CD technologies will prove unfruitful, and will therefore eventually be abandoned by record companies. There firms may take a cue from the movie industry and increase the value of CDs by bundling interesting bonus features rather than restrictive copy-control software. It seems likely that they will also capitalize on the popularity of digital distribution by aggressively supporting online services like Apple's successful iTunes Music Store. These strategies likely will pave the way to reduced infringement by enticing more listeners to pay for recordings.

7. REFERENCES

1. "US firm hopes anti-piracy CD will rock blackmarket." AFP via Yahoo News, September 24, 2003.
   http://story.news.yahoo.com/news?tmpl=story&u=/afp/20030924/tc_afp/us_music_piracy_030924221124
2. Frank Ahrens. "BMG Offers Legal Song Sharing." Washington Post, September 23, 2003.
   http://www.washingtonpost.com/wp-dyn/articles/A49456-2003Sep22.html
3. Mike Snider. "Anti-swap CD hits the racks." USA Today, September 22, 2003.
   http://www.usatoday.com/tech/news/techinnovations/2003-09-22-copycd_x.htm
4. Alex Veiga. "Recording Industry Eyes 'Smart' CDs." Associated Press via Excite News, September 18, 2003.
   http://apnews.excite.com/article/20030918/D7TL3G4O0.html
5. Glen Creno. "Phoenix firm gets CD-piracy contract." Arizona Republic, September 13, 2003.

http://www.azcentral.com/arizonarepublic/business/articles/0913sunncomm13.html

6. Jon Healey. "BMG is Releasing Copy-Protected CDs." LA Times, September 13, 2003. http://www.latimes.com/business/la-fi-cd13sep13,1,578082.story
7. John Borland. "Copy-protected CDs take step forward." CNET News.com, September 12, 2003. http://news.com.com/2100-1027-5075656.html
8. "SunnComm's MediaMax CD-3 Technology Passes International Test with 'Flying Colors.'" SunnComm press release, August 27, 2003. http://www.sunncomm.com/press/pressrelease.asp?prid=20030827630
9. John A. Halderman. "Evaluating New Copy-Prevention Techniques for Audio CDs." In *Proc. ACM Workshop on Digital Rights Management*, Washington, DC, November 2002. http://www.cs.princeton.edu/~jhalderm/papers/drm2002.pdf
10. The following materials related to the MediaMax-protected Anthony Hamilton CD are available on my homepage:
    - sample of garbled audio, http://www.cs.princeton.edu/~jhalderm/cd3/cd3-sample.mp3
    - BMG end user license agreement (EULA), http://www.cs.princeton.edu/~jhalderm/cd3/bmg-eula.html
    - SunnComm privacy policy, http://www.cs.princeton.edu/~jhalderm/cd3/sunn-privacy.html
    - SunnComm readme file, http://www.cs.princeton.edu/~jhalderm/cd3/sunn-readme.html
11. "How to Enable or Disable Automatically Running CD-ROMs." Microsoft Knowledge Base Article 155217. http://support.microsoft.com/support/kb/articles/Q155/2/17.ASP
12. "CD Crack: Magic Marker Indeed." Reuters via Wired News, May 20, 2002. http://www.wired.com/news/technology/0,1282,52665,00.html
13. P. Biddle, P. England, M. Peinado, and B. Willman. "The Darknet and the Future of Content Distribution." In *Proc. ACM Workshop on Digital Rights Management*, Washington DC, November 2002. http://crypto.stanford.edu/DRM2002/darknet5.doc

Acknowledgments

I'd like to thank Ed Felten, David Robinson, and Fred von Lohmann for making insightful contributions to this report.

Revisions

Changes in version 1.1: Several readers pointed out a technical oversight in the initial version of this paper. If the user has ever accepted the SunnComm end user license agreement (by clicking Accept when the license is displayed), the MediaMax driver does not become deactivated when the computer is rebooted, as I had stated. Rather, it reloads every time unless the user takes steps to disable it. I did not notice this behavior in my earlier tests because I have not accepted the agreement. Nevertheless, this observation does not mean MediaMax is more secure than I previously believed. Users who have accepted the license can easily disable the driver using a procedure like the one in section 3. This would allow them to copy the disc normally as long as the `LaunchCD.exe` program is not allowed to start.

John A. Halderman (jhalderm@cs.princeton.edu)