

2.7 DRM Under Attack: Weaknesses in Existing Systems

*Tobias Hauser, Christian Wenz*⁵¹⁷

DRM systems are insecure. This statement seems to be too simple. But like all simplifications it has a true background: Every piece of software is breakable. This chapter shows what possibilities an unfriendly intruder has and which leaks DRM systems must close in consequence. We cover audio and video protection mechanisms as well as eBooks.

I Introduction

The interesting fight between crackers⁵¹⁸ and DRM systems is not a match just for the sake of entertainment. It also has consequences in the real world. The cracker itself is not the most terrible danger. He is only one person who uses the forbidden digital right for own purposes. It gets more dangerous when he shares his knowledge on cracking with others. Everybody has access to all kinds of information via the Internet. Although crackers have to have certain knowledge and skills they can distribute their cracking knowledge in “easy to use” software tools via the Internet so that everybody can easily download these “packages” without having any cracking skills of their own. Now this is where the real problem starts.

This chapter focuses on the available cracking tools suitable for the most common formats and DRM systems like Windows Media Player and PDF, which represent the virtual goods sound, video and eBooks. The chapter also shows methods for sound and video grabbing, an alternative for the direct attack to DRM systems. The technical background of cracking tools can help to create better DRM systems and to inform users about the danger. Only when you have the knowledge you can react. The intention of giving technical background information should not be misinterpreted as a guide for crackers. It much rather intends to reveal the weaknesses of some systems in order to understand them better.⁵¹⁹

II DRM Systems in Player Software

The attacks of crackers on DRM-protected content can generally be divided into two areas: Attacks directly targeted at the key of the DRM system and circumvention methods like sound and video grabbing which attack directly in

⁵¹⁷ Hauser Wenz Partnerschaftsgesellschaft.

⁵¹⁸ Someone who breaks systems is called a cracker. Hackers are persons who have an insight-view into systems but do not destroy anything. A discussion about these two terms can be found at:

<http://www.zdnet.com/special/stories/defense/0,10459,2504308,00.html>.

⁵¹⁹ See: *Lejeune* (page 366), *Dusollier* (page 462), *Dreier, Nolte* (page 479), *Goldmann* (page 502), *Günnewig* (page 528) within this book.

front of the hardware. The attacks on the key are in the nature of today's DRM systems. Keys and licenses are provided together with the data file by the license server and stored on the user's data processor. Again, both can be attacked in two separate ways: either the attacker knows the system or parts of the system and can therefore program circumventions or the encryption is going to be directly targeted by a brute force attack which can take some time and/or process power depending on the length of the key.

Real Player and Adobe PDF are examples for DRM systems with keys and licenses stored in the data files⁵²⁰. The Microsoft DRM system which is being used by Windows Media Player works differently. Here the Media Player stores the DRM key in Windows in separate DLL files. The encryption is placed in the *blackbox.dll* data file. After personalizing the first license the data file *IndivBox.key* (also a DLL) contains a specific version of the *blackbox.dll* for the individual PC. This special version also includes the hardware ID of the PC. This topic was heavily discussed after the release of Windows XP.⁵²¹ Tests showed that implemented licenses are invalid after a change of the CPU.⁵²² In the next section you find a description of a cracking tool for Microsoft's DRM system.

II.1 Attacks on Microsoft's Audio DRM System

This section covers ways to circumvent the protection mechanisms of Microsoft's DRM system in version 1 and 2. We will show which software products exist for that task and how they work. Please note that this section is specific to Microsoft's DRM system; more general means to disable DRM will be covered in the next section.

In April 1999, Microsoft released their first Windows Media Rights Manager SDK 6⁵²³, a collection of tools for the use of the DRM functionality of the Windows Media Player (WMP). It contains Rights Manager 1, the part of the software package that enables the management of the usage rights, which the user has for a given media file (e.g., how often/long to play the file). In 2001, along with the launch of the new version 7.1 of Windows Media Player, the Windows Media Rights Manager 7 SDK was released, containing Rights Manager 7. The version number of the DRM system itself has also been increased by one: The old system from 1999 was called DRM v1, the new system is known as DRM v2.

Since DRM v2 is not backwards compatible to DRM v1, many media files that are currently offered still use DRM v1. Since the earnings of the German music industry dropped by 11.3% in 2002⁵²⁴, a trend that can be witnessed worldwide, maximizing the potential audience is a key effort. This could be one of the reasons why at the end of 2002 the US band Bon Jovi offered all registered buyers of their

⁵²⁰ See: Section "PDF and ElcomSoft".

⁵²¹ An excerpt of the discussion can be found at:

<http://www.heise.de/newsticker/data/lab-10.07.01-001>.

⁵²² See: Hauser (2003).

⁵²³ Software Development Kit, term often used for tools specifically for developers.

⁵²⁴ See: <http://www.spiegel.de/wirtschaft/0,1518,237876,00.html>.

album “Bounce” a previously unreleased track⁵²⁵ in Microsoft’s WMA format. The track could not be copied on a music CD, but three times on mobile devices that are not SDMI-compliant⁵²⁶. This track was secured using the over three years old DRM v1 system.

DRM v1

Shortly after the release of DRM v1, a software called *unfuck*⁵²⁷ emerged that could quite reliably unprotect DRM v1-secured audio files. The software itself consists of only one binary file, *unfuck.exe*; alternatively, an installation program is available that also creates a start menu and uninstall entries for *unfuck*. In order to use the software, WMA codecs are necessary. If they do not exist on the system yet, they can be found on the *unfuck* homepage itself. However, it is uncertain whether this download is legal or not.

During its first launch, *unfuck* creates an initialization file called *unfuck.ini* with the following default content:

```
[WMA Writing Output Driver]
config_waveoutdir=C:\WINDOWS\Desktop
config_bitrate=128
config_samplerate=44100
config_nch=2
```

An important value is the first parameter: *config_waveoutdir*. It contains the directory in which the unprotected media file will be saved. When you download only *unfuck.exe*, the current directory is written to the *.ini* file; with the installer distribution, the standard is the directory shown above. It is crucial to ensure that this directory exists and that *unfuck* has write access to it.⁵²⁸ If not, this entry in *unfuck.ini* can be changed after the program has been closed; after the modifications to the initialization parameters, *unfuck.ini* must be write-protected in order to preserve these settings after the next program launch.

⁵²⁵ A live version of the album’s title track, “Bounce”.

⁵²⁶ Secure Digital Music Initiative, a foundation consisting of around 160 companies. In 2000, the SDMI sponsored a challenge to try to crack their copyright protection system. A group of seven researchers from Princeton University succeeded, but when they wanted to present their findings at a conference, the RIAA (Recording Industry Association of America) reminded them that the scientists might violate the Digital Millennium Copyright Act (DMCA). See: <http://www.wired.com/news/politics/0,1283,46097,00.html>.

⁵²⁷ See: <http://go.to/unfuck>.

⁵²⁸ In particular, this is not the case under Windows NT and 2000, where the operating system usually resides in *C:\WINNT*; Windows XP has no standard subdirectory Desktop in its Windows directory. If the directory does not exist or is not writable for *unfuck*, the error messages “error playing writer” and “error creating file” is displayed.

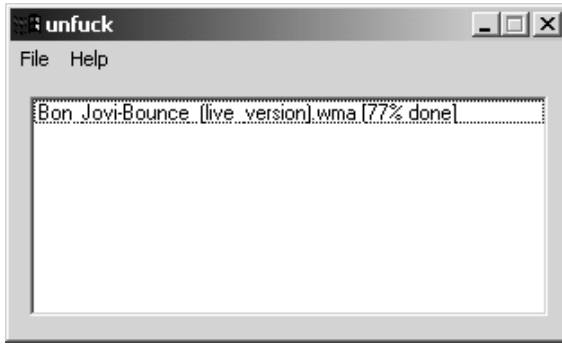


Fig. 1. The Software Unfuck (Unprotecting a Media File)

The software itself works using a very simple yet effective approach. The user must already have acquired a license for the WMA file; Windows Media Player must be able to play the file. In order to achieve that, a test within WMP (possibly including the acquisition of a license or the activation of the file) is mandatory. After that, the file may be opened within unfuck. The software now plays the file which usually would lead to a wave output of the file’s contents to the speaker system of the PC. However, unfuck captures this sound output, converts it back into a — this time, unprotected — WMA file and saves it into the directory provided in the *config_waveoutdir* parameter of the *unfuck.ini* file. The new filename is the old one, however, the part before the suffix is extended by “(unfucked)”.

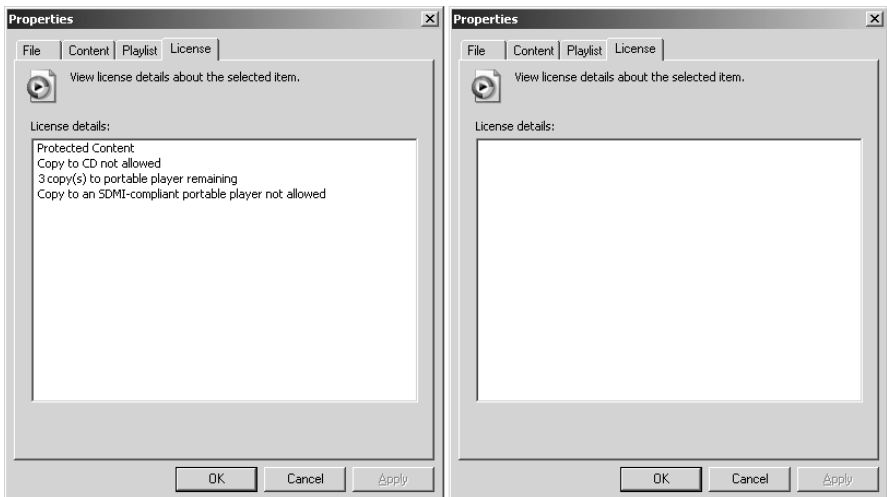


Fig. 2. The Audio File’s License Information before (left) and after (right) Running Unfuck

The quality of this output (i.e. the bitrate and the sample rate of the newly created WMA file) can also be tuned in *unfuck.ini* (parameters *config_bitrate* and *config_samplerate*).

Using this mechanism, the loss of quality is minimal; the only loss of information during the process occurs during audio encoding back to WMA which is not a lossless format. Apart from that, all information is preserved, including stereo information. The resulting WMA files are not protected in any way. Unfortunately unfuck does not offer a possibility to create a lossless WAV file; section “Attacks on Arbitrary Audio DRM Systems” describes ways to achieve that.

Whereas unfuck works with all DRM v1 audio files, it fails to “unprotect” DRM v2 data; the error message “error playing file” is displayed⁵²⁹.

DRM v2

The reason for the failure of unfuck with Rights Manager 7–encoded files is that the new version creates a secured channel to the audio driver; the mechanism which unfuck uses to redirect the sound data does not work any longer. However, another approach was found which proved very effective — for some time.

The approach is often linked to the name “Beale Screamer”, a nickname apparently inspired by the movie “Network”⁵³⁰ from 1976. Peter Finch plays “Howard Beale”; the character is known for the quote “I want you to go to the window, open it, stick your head out and yell: ‘I’m as mad as hell, and I’m not going to take this anymore!’”⁵³¹.

On November 18, 2001, an anonymous poster with the self–chosen alias “Beale Screamer” sent a PGP–signed message⁵³² to the usenet group *sci.crypt*. The chosen newsgroup deals with the scientific analysis of encryption mechanisms, so it was a natural choice for the posting. The message included a technical description of how to overcome the DRM v2 copy protection, including C source code for a “proof–of–concept” program. Once compiled, an executable *FreeMe.exe* is created that allows users to unprotect DRM v2–secured audio files.

The approach by the anonymous hacker requires a valid license for the song; therefore, the software is used to artificially extended a license by creating a new version of the protected file, without any DRM restrictions.

When Windows Media Player 7.1 or higher is installed, a file called *Indivbox.key* is created. Although the file extension is *.key*, the file is a dynamic link library (DLL). The file is individualized for the current PC, so the *Indivbox.key* file differs from machine to machine. This file contains all licenses the user has acquired. All FreeMe is doing is to extract these licenses out of this file.

⁵²⁹ This error message may also occur when no suitable WMA codec is installed; however, most of the time a popup message warns the user if the codec is missing.

⁵³⁰ For more information see <http://us.imdb.com/Title?0074958>.

⁵³¹ See: <http://us.imdb.com/Quotes?0074958>.

⁵³² The message ID is 1762008I37182.4630787037@anonymous.poster; it can be viewed using Google and is also available at various mirrors, inter alia at: <http://cryptome.org/beale-sci-crypt.htm>.

This task has not been easy, and Microsoft has implemented several countermeasures, including the well-known “security through obscurity” approach. The license keys are encrypted in several ways. The positions of the license keys in the file differ from system to system. This prevents users from transferring their licenses from one PC to another one.⁵³³ In order to further increase security, the license keys are stored in the memory in the form of linked lists. This ensures that the complete key exists in memory in non-contiguous memory blocks. So it is not possible to just scan the application memory for the key.

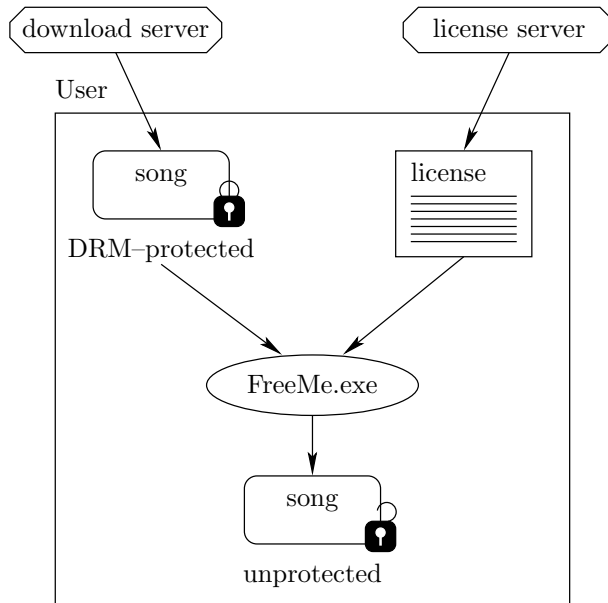


Fig. 3. FreeMe Uses the (Existing) License to Unprotect the Sound File

Another issue for “Beale Screamer” was that all communication between the various components of the WMP DRM system is encrypted, obfuscated and secured. For instance, when data shall be decrypted by the WMA system, first a temporary session key is created. The data is unscrambled, but immediately re-encrypted, this time using the session key. Thus the encryption/decryption DLL cannot be used directly; it is also necessary to reverse-engineer the session authentication and encryption mechanism. There are also other interesting aspects that obviously made it harder to crack the system: The base64 encoding sometimes uses non-standard characters, the message authentication code (MAC) used for DLL-to-DLL communication is a nonstandard algorithm⁵³⁴, apparently developed directly by Microsoft.

⁵³³ Windows Media Player includes functionality to back up licenses (menu command Tools/License Management); however, it is possible for content owners to disable this functionality for their media files.

⁵³⁴ “Beale Screamer” calls this mechanism “MultiSwap”, since the algorithm consists of numerous swap operations (exchanging two halves of a 32-bit input data).

For some time, the file *FreeMe.exe* that is retrieved by compiling the C sources succeeded in decrypting DRM v2-secured WMA files. The program loads the WMA file and uses Microsoft's WMP components to gain access to the (already existing) license. This license is used to access the sound data itself and then to write it into a new, unprotected WMA file. All other information about the file is left intact; there is also no quality loss due to a new encryption/compression of audio data as it occurs with *unfuck.exe*.⁵³⁵ FreeMe adds "Freed-" to the old file name in order to generate the new WMA.

Trying this software with a recent WMA file, however, does not work any longer. Here is a typical output of FreeMe:

```

Found DRMv2 header object.
Found KID (74321785342-01|1|128)
Found DRMv1 header object.
Starting to look for license.
License file full path:
  D:\Dokuments and Settings\All Users\DRM\drm2.lic
BlackBox library to use:
  D:\Dokuments and Settings\All Users\DRM\IndivBox.key
Keystore to use:
  D:\Dokuments and Settings\All Uers\DRM\v2ksndv.bla
Created BlackBox instance --- extracting key pairs

Public key 1 x: 6bdbae3a7518ed828816c696a01fab20a9a0f4ed
Public key 1 y: 72377a5a879511277973dbc888864d0fc34f9dbc
Private key 1: f9527926c3d854c076dcfe1b2e900fcf24bcfe7c

Checking license with PUBKEY
6bdbae3a7518ed828816c696a01fab20a9a0f4ed
Matched public key! Proceeding...
Decrypted content key is too big!

Press <ENTER> to acknowledge error.
```

The reason for that is that Microsoft has released a fix⁵³⁶ specifically for the FreeMe approach. After this patch has been applied to Rights Manager 7, all newly created, secured WMA files cannot be unprotected by FreeMe any longer. Since then, there have been no new life signs by "Beale Screamer" in *sci.crypt*; periodically, users get the "Decrypted content key is too big!" error message and complain, but it is no software fault, the reason for it has been given above.

This means that FreeMe was a technically sophisticated demonstration of a flaw in DRM v2, but there is no new version or update in sight. One of the most compelling features of this approach is that there is absolutely no loss of quality, one reason that Microsoft implemented countermeasures.

⁵³⁵ See section "Attacks on Microsoft's audio DRM system".

⁵³⁶ See:

<http://www.microsoft.com/windows/windowsmedia/wm7/drm/freemefix.aspx>.

II.2 Attacks on Arbitrary Audio DRM Systems

After the analysis of tools that were specifically written against certain versions of Microsoft’s DRM systems, this section will describe software products that make it possible to overcome any DRM system to unprotect secured audio files. The basic principle is very simple: DRM-secured systems first open and then examine secured files. If an appropriate license exists on the user’s machine, the file is started and played. The audio data are then sent to the sound card driver, which activates the sound hardware in the machine.

The software *unfuck* we described in section “*Attacks on Microsoft’s audio DRM system*” used the approach to capture the audio data on their way from the audio player to the soundcard driver. However, with DRM v2 this is no longer possible, as a secured channel is established; thus unfuck does no longer work there.

The simple, but obvious approach is now to capture the audio data on their way from the sound card driver to the hardware. In other words: A special sound card driver is written. It makes the player software believe that there is a “real” soundcard behind the driver; however, all the driver is doing is that the audio data is written to the hard disk in real-time. This ensures lossless audio data with the highest possible quality — the newly written audio files on the hard disk offer the same quality the player would have produced for the available audio hardware.

For the Windows platform there exist several products that can achieve this task. All of them implement a kind of virtual soundcard; they differ in the additional features they offer, including multi format support and audio editing capabilities. There are two different kinds of wave filters⁵³⁷: a wave capture filter takes an audio signal from a microphone or any other external source and creates a digital wave stream. A wave-rendering filter takes a digital audio stream and creates analogous (e.g. for external speakers) or digital (for instance S/PDIF⁵³⁸ output) audio data streams. Using the Microsoft technologies that are bundled with the operating system, such filters can be created. Of vital importance is DirectShow, Microsoft’s API⁵³⁹ for capturing and playing back various media data.⁵⁴⁰

There exist several software products that provide this functionality, with additional features like audio editing. Basically, most of these programs create a virtual soundcard that comes with its own drivers. These drivers offer — among other things — the possibility to directly write the audio data to the hard disk, in wave or other formats.⁵⁴¹

⁵³⁷ See: <http://www.microsoft.com/hwdev/tech/audio/highperf-driv.asp>.

⁵³⁸ Sony/Philips Digital Interface, format to transfer digital audio signals (avoiding the quality loss that occurs when converting the data to an analog format).

⁵³⁹ Application Programming Interface

⁵⁴⁰ See: <http://www.microsoft.com/Developer/PRODINFO/directx/dxm/help/ds/default.htm> for an introduction.

⁵⁴¹ Due to the enormous resources (processor power, etc.) required for encoding audio data in another format but WAV, this is not always possible or advisable, since the encoding must be done in real-time.

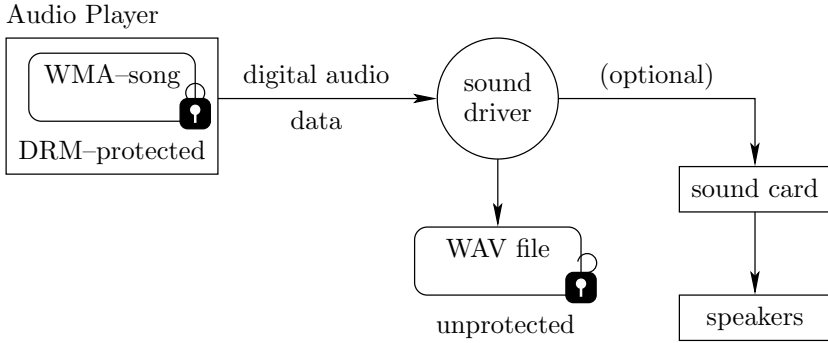


Fig. 4. The Sound Driver Writes the File to the Hard Disk

Below is a representative selection of suitable software products (as of March 1st, 2003):

- Audio Record Wizard
- SoundCapture
- Streamripper
- Super Mp3 Recorder
- Total Recorder
- Virtual Audio Cable

However, other operating systems also offer ways to capture audio data into files. Under the “old” Mac OS, that means up to version 9.x, the software MacAmp⁵⁴² offered audio capturing. Currently (March 2003) there is no full version for Mac OS X available, only a stripped-down “lite” version⁵⁴³. The full version was announced in April 2002, however, there is still no released version available yet. Since the company behind the product, Subband Software, Inc., has ceased to exist, the “full” version will most probably never appear. An alternative product that works on Mac OS X (and no previous versions) is Audio Hijack⁵⁴⁴; according to the MacAmp Lite homepage, some of the MacAmp programmers now work on this product.

Under Linux, DRM systems are not so widespread yet, mostly because of the lack of appropriate software and the “free” approach of the operating system. However, there also exist software approaches to capture audio data.

The software vsound by Erik de Castro Lopo does just that. On the project homepage⁵⁴⁵ de Castro Lopo states that he took the project offline in October 2002 due to the Digital Agenda Bill in Australia which forbids the distribution of products like vsound; however, there still exist mirrors of the original content of the page⁵⁴⁶.

⁵⁴² See: <http://www.subband.com/macamp/macamp.html>.

⁵⁴³ Available at: <http://www.macamlite.com/>.

⁵⁴⁴ See: <http://www.rogueamoeba.com/audihijack/>.

⁵⁴⁵ See: <http://www.zip.com.au/~erikd/vsound/>

⁵⁴⁶ For instance see: <http://www.devnull.fsworld.co.uk/vsound/vsound.htm>; relevant search engines also effectively find other alternatives.

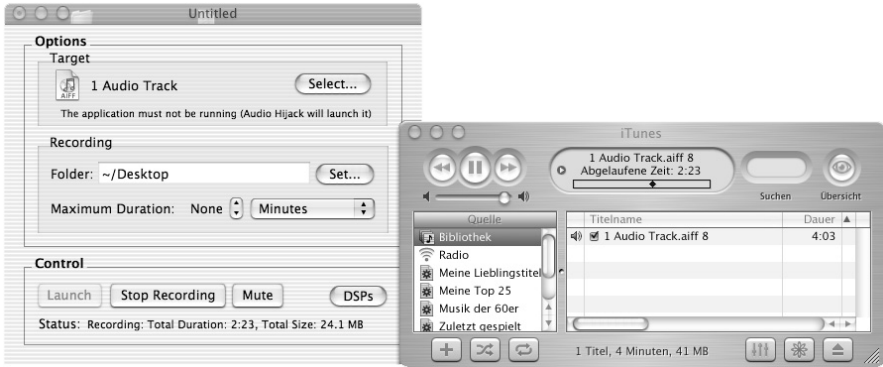


Fig. 5. iTunes is Playing the Track (right Side),
Audio Hijack is Saving the Content (left Side)

vsound uses a very simple approach: Most Linux applications that output audio data write those to the device `/dev/dsp`⁵⁴⁷. Writing to this device activates the D/A converter and produces sound output. What vsound is doing is that all access to `/dev/dsp` is intercepted and redirected to vsound. Thus, if `/dev/dsp` is first accessed, an ordinary file handle is returned, instead of the expected device handle. All subsequent `write()` calls to `/dev/dsp` write the audio data to the newly created file instead. The syntax for vsound is the following:

```
vsound -f outputfile.wav application [parameters]
```

So the following call would call Real Player (one of the few ways to play DRM-protected audio data under Linux) within vsound, `input.ram` is played, and is written in wave format into `output.wav`:

```
vsound -f output.wav realplay input.ram
```

But does it always have to be so difficult and must the audio ripping always include the usage of external software? In many cases, yes. The obvious approach, plugging a suitable hardware into the digital (S/PDIF) output of a soundcard, does not always work. For instance, recent soundcard drivers by Creative⁵⁴⁸ warn the users that the digital output of the card is shut down upon detection of audio data secured by Microsoft's DRM.⁵⁴⁹ It is a logical step that Creative's own media player (that often comes with the driver package or the soundcard) also reports to the driver if files are DRM-secured; ironically, part of many SoundBlaster software distributions is also the software product "Creative Recorder" that enables the users to record audio data. One of the provided input sources is "What You Hear", thus making the software work like many of the programs we have described further above.

⁵⁴⁷ DSP stands for the general term "digital signal processing".

⁵⁴⁸ A company widely known for their "Soundblaster" audio card products.

⁵⁴⁹ Original text from the readme file of the Sound Blaster Live! drivers: "To protect against unauthorized duplication, Sound Blaster Live! shuts down its digital output when encrypted files are played back through a Microsoft DRM supported audio player (for example, Creative PlayCenter).".

It must be noted that all those programs and approaches not only work with DRM-protected, “static” audio files, but are also suitable for capturing streams like webradio, providing additional value to the software products.

This section showed that all protected media data can be unprotected with very little or no quality loss — since all audio data must be sent to a sound card driver, a specially constructed driver can always redirect the data to a local file. However, this also means that watermarks⁵⁵⁰ embedded into the audio files still exist, especially if 1:1 copies are created. Thus, watermarking is in our opinion the only viable option to add an almost unbreakable security to audio files. Copying and recording cannot be avoided, but it would be possible to retrieve the origin of an audio file.

II.3 Attacks on Video DRM Systems

For streaming video, by far fewer applications are available on the market, due to the much more complicated structure of the required software. CoCsoft Stream Down⁵⁵¹ promises to capture streams and download them to the hard disk. The user enters the URL of the stream (that itself is sometimes hard to find out), the software then requests the data from the server and saves them directly on the hard drive.

A more sophisticated approach is taken by the Korean software VOD Recorder⁵⁵². This program uses the Windows capturing DLL WinPcap⁵⁵³ to filter out all packages that are sent to the video player. This data is intercepted and saved on the hard drive.

Camtasia Studio⁵⁵⁴, a software primarily used to “film” the user’s actions on the PC desktop (which, in turn, is then used to create educational videos, e.g. “how to use your word processor”), which of course means that the output of the system’s video player can also be saved to disk. However, due to the special field of application of this software, the performance and resulting video quality is unsatisfying on some machines. Additionally, hardware acceleration must be turned off in order for video data to be captured, which slows down the video performance of the PC.

It can be said that video, especially streamed data, still is very secure. Whatever is displayed on the user’s monitor can be filmed and saved in certain ways, but due to the enormous amount of data to be processed and the associated potential loss of quality, this neither is an easy task nor will it be one in the near future.

⁵⁵⁰ See for more information: *Petitcolas* within this book on page 81.

⁵⁵¹ Available at: <http://stream-down.cocsoft.com/>.

⁵⁵² See: <http://www.dkcasino.com/eng/record.php3>; a very rough translation of the Korean original at <http://www.dkcasino.com/kor/record.php3>.

⁵⁵³ Additional download required; software available at: <http://winpcap.polito.it/>.

⁵⁵⁴ See: <http://www.techsmith.com/products/studio/>.



Fig. 6. The Original Stream (left) and the Captured Video by Camtasia (right)

III eBooks

One of the biggest markets for DRM-protected goods is the eBook market. In the beginning eBooks were not very popular because they were too expensive, only available on few portable devices and equipped with incompatible formats. Nowadays lots of PDAs and mobile devices are in use and on the Internet, Adobe PDF and Microsoft Reader are the most common and widely used formats. On the other hand, there are a lot of proprietary formats for portable eBooks. All these various forms and formats of eBooks were under attack of some crackers.

III.1 PDF and ElcomSoft

The most spectacular case of eBooks began during the DEFCON Nine fair in Las Vegas from July 13th until July 15th 2001. On July 16th the FBI had arrested a man in his hotel room. This man was the developer Dmitry Sklyarov, who worked for a company named ElcomSoft⁵⁵⁵. ElcomSoft is a Russian software company with headquarters in Moscow that specializes in the removal of password protection for Office documents and packed archives. One month before the DEFCON Nine ElcomSoft had introduced the new software Advanced PDF Password Recovery which is used to override several DRM restrictions of PDF formats. Sklyarov, as the head of development for this new software, spoke at the DEFCON mainly about the cracking of eBooks in general and specifically about cracking PDF.

A closer look at the software, which is available as a standard, a professional and a trial version, reveals interesting insights about methods to by-pass the protective measures of PDF data files.

⁵⁵⁵ See: <http://www.elcomsoft.com/>.

PDF data files can be provided with owner and user passwords. The standard version of Advanced PDF Password Recovery cracks owner passwords and minimizes all appending PDF rights. Thereby, safeguard mechanisms which prevent printing and/or copying of the PDF document are canceled. The professional version of the software is needed if the PDF has both an owner and user password. The user password is used for access protection whereas the owner password manages the rights of PDFs.

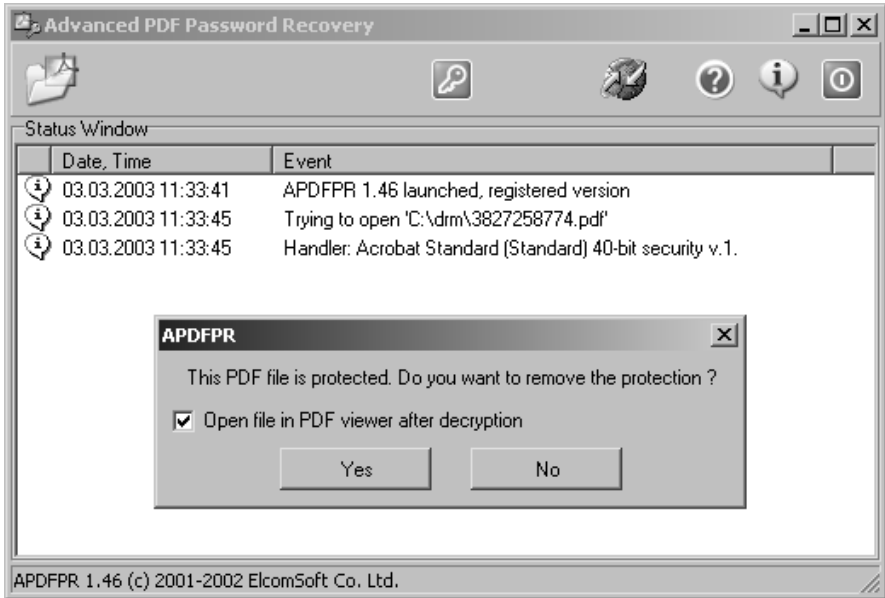


Fig. 7. The Software Advanced PDF Password Recovery

The brute-force attacks on encryption are doomed to failure with the new PDF format 1.4. The key used in this format is 128 bit long and consequently too long for trying out passwords in due time. PDF version 1.3 has only a 40 bit long key. Subsequently the 1.3 version with user password can be cracked within a few days. Of course this can be done more rapidly if there is more CPU power and more processors. The rights of a PDF without user password can be cracked immediately. For this, flags for the rights are being implemented in the PDF data file after the owner password has been cracked.

Advanced PDF Password Recovery is still (March 2003) available for download. This obviously raises the question to what happened after Sklyarov's arrest. The reason for his arrest was said to be a violation of the US DCMA (Digital Millennium Copyright Act) dated 1992. This law prohibits the development and distribution of software which purpose it is to steal intellectual property.

During the following days the situation climaxed. After rumors abounded that the founder of the PDF format, the company Adobe, had actually given the police the information which led to Sklyarov's arrest, Adobe distanced themselves

on July 23rd 2001 from the imprisonment and charges against Skylarov. Adobe stated that the developer was not the guilty party and Advanced PDF Password Recovery was not available anymore at least in the United States.⁵⁵⁶

This reaction emerged from the cooperation with the EFF (Electronic Frontier Foundation), an association which advocated the protection of freedom of a digital world. Adobe also reacted to the large number calls for protest and private initiatives⁵⁵⁷ to prevent damage to the image of Adobe.

The criminal law suite against Skylarov and his company ElcomSoft nevertheless took its course. The two defendants pleaded “not guilty”. Thereinafter Skylarov and his company parted. Skylarov made a deal with the Public Attorney’s office to end the legal proceedings but therefore had to depose against his own company. In the meantime Skylarov and the CEO of ElcomSoft had difficulties getting their visas approved to enter the United States for their appearance at court.⁵⁵⁸ But finally the hearings started. Although elaborate research was made by Adobe they could not prove that the ElcomSoft software was ever really used to crack eBooks. The federal prosecutor renounced the deposition of Skylarov but instead showed a videotape. Finally the charges were dropped. The explanatory statement confirms that the software under DCMA is illegal, but also acknowledges the fact that ElcomSoft can’t be charged with deliberate breach of this law. It is of importance in this matter that the software is actually legal under Russian law and that the economical risk would have obviously stopped a renowned company like ElcomSoft from breaking the DCMA law if they would have been aware of the consequences.⁵⁵⁹

III.2 Microsoft eBook Reader

The Microsoft format for eBooks has the extensions *.lit*. Files in this format can be read by the Microsoft eBooks Reader. The user must activate his installation of the Microsoft Reader. For this activation process the user needs a Passport account for identification. Once he has identified himself he has access to eBooks he has obtained. The DRM system for these files is also called DRM v5.

The Microsoft Reader’s DRM system has been discussed many times.⁵⁶⁰ Successful cracking attempts were reported on various news sites and in newspapers. The latest try was attempted by Dan Jackson, a programmer living in the UK.⁵⁶¹ His tool, *convert lit*, is command line-based and converts *.lit* files in such a way that they can be used on as many PCs as the user wishes. The maximum amount of PCs in the Microsoft Reader is restricted to eight. The attempt by Dan Jack-

⁵⁵⁶ See: <http://www.adobe.com/aboutadobe/pressroom/pressreleases/200107/20010723dcma.html>.

⁵⁵⁷ Exemplary <http://www.freesklyarov.org/>.

⁵⁵⁸ See: <http://www.heise.de/newsticker/data/anw-26.11.02-005>.

⁵⁵⁹ See: <http://news.com.com/2100-1023-978176.html>.

⁵⁶⁰ One example: <http://www.heise.de/newsticker/data/daa-30.08.01-000>.

⁵⁶¹ See: <http://members.lycos.co.uk/hostintheshell/>.

son to crack the Microsoft Reader-format was fear on the side of the content publishers. The trust in the Microsoft *.lit* format decreased immediately.

III.3 Portable eBooks

Most experts think that portable eBooks and their formats can be protected much better because hardware and software can interact. That may be right, but there still were some successful cracking attempts:

The best-known case is the Rocket eBook format from Gemstar.⁵⁶² In April 2001 a cracker made the information about his crack available via several newsgroup-postings after he had cracked Rocket eBooks. In the end the Internet trend magazine *Wired* wrote a widely acknowledged article about this topic.⁵⁶³

Gemstar reacted by updating the operating system of the Rocket eBook. The new version was updated in a way the users could only download eBooks from Gemstar web servers and/or eBooks submitted by Gemstar web servers. The crackers worked around this safety-feature by recovering the old operation system on newer or updated devices.

III.4 eBooks under Fire

Almost all important eBook formats have some problems with cracking tools. The question here is indeed not the fact that something happens but how to react to it properly. In all three cases mentioned above the DRM system manufacturer reacted, at least after some time, in a relatively contained manner. The content suppliers of eBooks, thus the publishers, on the other hand were considerably more frightened. Here the uncertainty spread. Non-printable books in PDF format which are distributed free of charge are being critically observed by the computer industry. Many Microsoft Reader eBooks suppliers are worried about their future after the latest successful crack attacks. Even publishers of fiction books are hesitant to produce new works of fiction as eBooks. The future will show if the suppliers of DRM system will be able to fend off cracking attempts on a continuing basis and regain the trust of the publishers.

IV Implications

Today's DRM safeguards can be circumvented, for instance with relevant tools like Advanced PDF Password Recovery from ElcomSoft or FreeMe. Furthermore, there is always the problem with grabbing the data output of sound and/or video card data.

However the here introduced tools also show the following: If the user interest of a technology or an entertainment offer has reached a certain level, it will not be long until methods to circumvent the safeguards will turn up.

⁵⁶² See: <http://www.gemstar-eBook.com/>.

⁵⁶³ See: <http://www.wired.com/news/business/0,1367,43401,00.html>.

Most of the time hackers do not work for money but for prestige. Prestige and status can be acquired best with technologies that attract a lot of interest. For this reason the Microsoft DRM system is a very interesting target for FreeMe and consequently music is the digital good that's made DRM free the most. A company like ElcomSoft does not look for prestige but even here a lot of money can be made with systems of the market leader, namely with eBooks and thus Adobe.

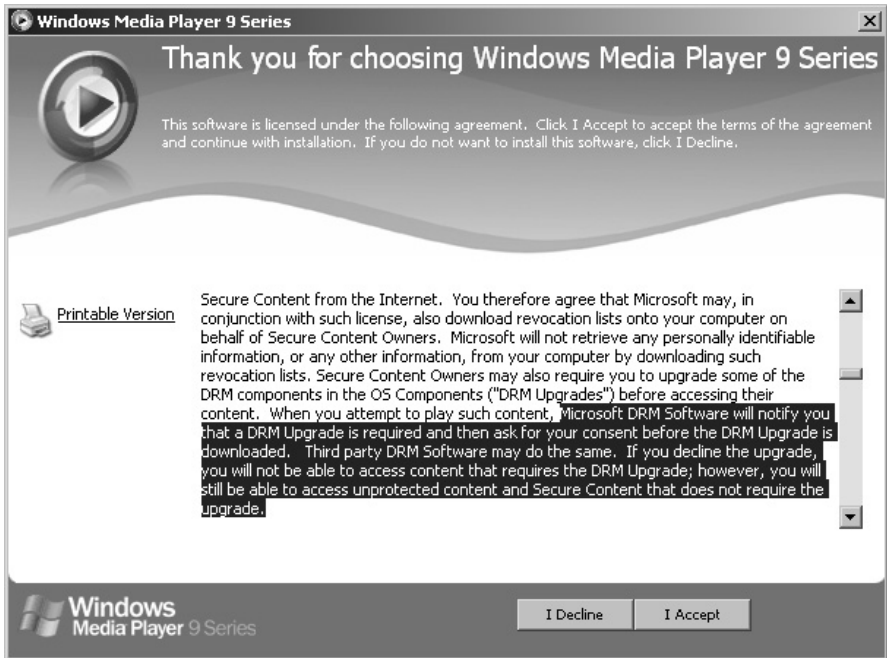


Fig. 8. Microsoft States that DRM Upgrades for new Content Could Be necessary for the Windows Media Player 9.

The image gain and the increasing publicity are certainly a welcome side effect. The remaining ElcomSoft product range, which is primarily composed of products like password recovery software for Microsoft Office products and for important data formats like zip archives, proves this fact.

If DRM systems are labeled as “easy to circumvent” it should also be mentioned that presently these systems are often one step ahead. Microsoft offers an update against FreeMe. Advanced PDF Password Recovery of ElcomSoft cannot crack the encryption of PDF 1.4 anymore or yet. In this area mostly update cycles and update possibilities for DRM systems will be of importance. Microsoft already announces the performance of automatic DRM system updates of the Windows Media Player in the accordant license agreements. These automatic updates however must be approved by the user.

The reaction time with eBooks and Adobe is longer since the content supplier has to have the latest Adobe Acrobat which is relatively expensive⁵⁶⁴. Likewise the user has to update his Acrobat Reader in case there are any changes in the DRM system.

From experience the latest version leaps caused these updates to be quite extensive and not all users execute the update right away. Consequently many eBooks are still encrypted with Adobe Acrobat 4.x

The problem with sound and video grabbing is not yet controllable in contrast to the attacks which are focusing directly on the DRM systems. The occurring loss of quality (if any) is acceptable for most music-lovers and until now there are no effective counteractive measures against crack-tools which imbed themselves as soundcard drivers.

V Helpful Crackers?

Cracking tools for DRM systems are without doubt dangerous for content and DRM system suppliers. However, before the legal club gets unpacked a peaceful approach should be sought after to make use of the know-how of the cracker or the attacking firm. A revealed circumvention always has the advantage that the attacked company can close the gap. If the company closes the gap quickly and without hesitation it will rather cause positive publicity than negative headlines. Everybody who has a certain technical interest and knowledge knows that a leading technology will always be subject to attacks.

A round table relationship between cracker and target company should not be a taboo but much rather considered as a peaceful option. Naturally the cracker should not have to be integrated into the company at once. Nobody likes to leave a burglar responsible for the alarm system, but especially for know-how and image reasons an amicable agreement should be sought after.

VI The Future

Direct attacks and brute-force attacks on DRM systems can hereafter be averted with the help of system updates. One possibility to inhibit sound and video grabbing could be a closer linkage of the DRM systems and the operating system. Microsoft pursues this path with the security initiative Next Generation Secure Computing Base (NGSCB) previously known as Palladium. This initiative uses a hardware chip according to the specification of the Trusted Computing Platform Alliance⁵⁶⁵ as technical basis.

⁵⁶⁴ Currently approx. 249 US-\$/€360; upgrade 99 US-\$/€135.

⁵⁶⁵ See: <http://www.trustedcomputing.org/>; the current version of the specification is 1.1b (<http://www.trustedcomputing.org/docs/main%20v1.1b.pdf>). *Kuhlmann, Gehring* within this book on page 178.

This alliance is a union of hardware and software manufacturers and was originally founded by Microsoft, HP, IBM, Intel and Compaq. The goal of the TCPA is to establish a security system that comprises both hardware and software. Together with the operating system the hardware chip is meant to assure the system integrity, thus protection against changes, for at least part of the system. The accordingly protected part of the PCs is also kind of a black box. To ensure the system integrity both hardware and software have to be certified. This would also be a possible solution for the sound and video grabbing problem. A piece of music that requires the highest possible security level can only be played with a certified soundcard and an appropriate driver unit. In addition the PC system should have an unprotected area which allows trouble-free download of insecure data. Until now all announcements made by Microsoft in regard to this issue are characterized by the subjects of cutting image losses against data privacy protectors and users who worry about their privacy. Technical background or beta versions are not yet available. The renaming of the Palladium into the incomprehensible acronym NGSCB was probably made to dispose of the negative term.

It is also very interesting that some declarations of Microsoft state that NGSCB is actually not meant for DRM but to protect the user's computer. For two reasons these statements don't seem plausible. On the one hand NGSCB solves the main problem of DRM systems, namely the insecure placement of the key in a data file, by relying on additional encrypting information on a hardware chip. On the other hand it allows in the same way for counteractive measures against sound and video grabbing. Neither Microsoft nor other large industry moguls will miss out on these chances for DRM systems.

If an initiative like NGSCB will however really constitute the future for DRM can not be anticipated at this point of time. It is however certain that cracker will try to overcome this challenge as well.