Design a Rigid CD Protection Method

Dr.Abdul Kareem Oglah Ibadi

Israa Ezzt Saleam

الخلاصـــة

لقد أولت شركات البرمجيات اهتماما كبيرا بإيرادات العقوبات المالية على مخترقي قانون الحرية الفكرية و أصبح يشكل نسبة مهمة من دخل هذه الشركات. وقد رأت أنها بدل إنفاقها الأموال في تطوير الأدوات والوسائل المستخدمة في الحماية من الاختراق لو إنها اهتمت بملاحقة المخترقين أنفسهم وجباية العقوبات المالية منهم.

في هذا البحث ركزنا على استنباط طريقة حماية للأقراص المدمجة تسهل عملية ملاحقة المخترقين وتفرض عليهم طريقة واحدة للاختراق سهلة الكشف. وهذه الطريقة هي منع نسخ محتويات القرص المدمج على الحاسوب (وهي التي يصعب ملاحقتها واكتشافها) والسماح باستنساخ القرص المدمج بقرص آخر مزور سهل الكشف.

الطريقة الجديدة في حماية نسخ محتويات القرص المدمج على الحاسوب هي سلاح جديد صعب الكشف يمكن استخدامه من قبل الشركات الكبرى لملاحقة المتطفلين وحماية القرص المدمج من النسخ على الحاسوب. الفكرة الأساسية في هذه الطريقة هي رفع المؤشر على الملف المراد حمايته من جدول المحتويات في القرص المدمج ووضعه في ملف تشغيلي آخر خاص بالتطبيق.

Abstract

The most of the large computer applications companies have a great concern of the taxes that are retrieved from the laws of deterring pirating copyrighted software, which becomes an important ratio for the companies' revenues. Instead of spending money for developing a deterring pirating copyrighted software which couldn't be stopped, overtaking hackers and criminals and got taxes.

In this research we focused on devising a method to avoid copying CD's to PC's which enforce hackers to make an illegal CD copy which is easy to revealed. The proposed method for deterring pirating copyrighted software is a great weapon for large companies to overcoming hackers.

The main idea behind this method is to wipe the TOC entry of the protected file and put it in an executable file belong to the same application on the CD.

1. Introduction

Since the approaching of commercial software, which are sold in the form of packages containing (CDs and DVDs), many methods have been used to prevent copying software from the original storage media.

In 2003, over $3 billion of counterfeit entertainment CDs were purchased worldwide. In addition, it is estimated that $29 billion of business software was used illegally. Software theft is a big business; so big that some of it is linked to worldwide organized crime[4]. At the same time, private individuals engage in software theft seemingly without recognition that it is illegal. This level of piracy exists even though software publishers attempt to stop piracy with software prevention methods and industry and government agencies monitor piracy, file litigation and shut down illegal operations.

This research will introduce a brief CD technology and the most common CD-protection schemes and produce a new method for protecting CD's to be copied to PC's. The impact of this new method can be quite dramatic on the financial performance of CD's publishers.

2. Technical Background

At the end of 1982, the Compact Disc Digital Audio (CD-DA) was introduced. This optical disc digitally stores audio data in high quality stereo. The CD-DA specification was drawn up by N.V.Philips and the Sony Corporation, was summarized in the so-called RED BOOK. All subsequent CD formats are based on this description. The extension of CD to storage of computer data was announced by N.V.Philips and Sony Corporation in 1983, and introduced to public in Nov 1985. This CD-ROM is described in YELLOW BOOK, which later led to the ECMA-119 standard, which specifies the physical format of a compact disc. In 1986, N.V.Philips and the Sony Corporation announced CD-I, which is described in GREEN BOOK. In 1987, Digitial Video Interactive (DVI) was presented to public. The primary emphasis in DVI is on algorithms for compression and decompression of audio and video data stored on a CD-ROM. In 1988, the CDROM-XA was announced. Since the beginning of 1990, CD-WO and CD-MO are specified in ORANGE BOOK. Since the beginning of 1995, CD-RW is also specified in ORANGE BOOK. At the beginning of 1997, Digital Versatile Disc (DVD) was introduced[5].

2.1 Basic Technology

In optical storage media, the underlying principle is that information is represented by using the intensity of laser light reflected during reading. A laser beam having a wave length of about 780 nm can be focused to a resolution of approximately 1um. In polycarbonate substrate layer, there are depressions, called pits, corresponding to the data to be encoded. The areas between the pits are called lands.

The substrate layer is smooth and coated with a thin, reflected layer. The reflected beam has a strong intensity at the lands. The pits have a depth of 0.12um from the substrate layer. Laser light hitting pits will be lightly scattered, that is, it will be reflected with weaker intensity. An optical disc consists of a sequential arrangement of pits and lands within a track. The pits and lands represent data on the surface [5].

2.2 Compact Disk – Digital Audio (CD-DA)

The CD-DA was developed jointly by N.V.Philips and the Sony Corporation for storing audio data. CDs have a diameter of 12cm, and are played at a Constant Linear Velocity (CLV). Information is stored in such a way that the length of the pits is always a multiple of 0.3um. A change from pit to land or from land to pit corresponds to the coding of 1 in the data stream. If there is no change, a 0 is coded. It stores up to 74 minutes of high quality stereophonic sound using 16-bit linear PCM at a sampling rate of 44.1 KHz. Analog long playing records and cassette tapes have a SNR of approximately 50 to 60 dB. The SNR of the CD-DA is exactly 96 dB. The audio data rate from a CD-DA is= 16 bits x 2 channels x 44100 = 1.4112 x 106 bit/s [5].

2.3 Advantages of CD-DA

Errors on a CD-DA can be caused by damage or dirt. For uncompressed audio, the CD-DA is very insensitive to read errors that usually occur.

An additional advantage is that there is no mechanical wear and tear.

The disadvantage is the achievable error rate is too high for general computer data, necessitating an extension of the technology in form of the CD-ROM [5].

2.4 CD-ROM

The Compact Disc Read-Only-Memory (CD-ROM) was conceived as a storage medium for general computer data, in addition to uncompressed audio data. It was specified by N.V.Philips and the Sony Corporation in the Yellow Book and later accepted as an ECMA standard.

CD-ROM tracks are divided into audio (corresponding to CD-DA) and data types. Each track may contain exclusively data of one type. In such a mixed mode disc, the data tracks are usually located at the beginning of the CD-ROM, followed by the audio tracks. The CD-ROM data unit is called block. A CD-ROM block consists of 2352 audio bytes of a CD-DA block [5].

Of the 2352 bytes of a block, 2048 bytes (computer data) or 2336 bytes (audio data) are available for user data. The remaining bytes are used for identification for random access and for another error correction layer that further reduces the error rate. 75 blocks per second is played back. Each block consists of 98 frames of 73.5 bytes (588 bits) each:

Block = 1.4112 x 106 x 1/75 s x 1/8 = 2352 bytes

2.4 Compact Disk Interactive (CD-I)

It was developed by N.V.Philips and the Sony Corporation, and announced in1986. CD-I was originally designed for consumer electronics as an addition to the TV Set. CD-I is a complete self-contained system, and it supports text, graphics, audio, image and video.CD-I is a complete delivery platform for multimedia applications.

CD-I hardware is called the decoder. CD-I system has its own processor unit based on Motorola 68000 family together with special video and audio chips. It also includes a CD-player with a controller and a joystick or mouse interface, and there is a provision for a connection to a RGB monitor or a TV [5].

It runs a real-time multi-tasking operating system called CD-RTOS. Audio in CD-I (A, B, C levels) generally uses ADPCM coding.

Generally speaking, full-screen full-motion video may not be possible in CD-I. However, it may be made possible by attaching an ‘FMV cartridge’ containing MPEG decoder and additional memory. CD-I is a consumer product, aimed at repeating the success of CD-DA, so a CD-I disk will play on any CD-I player anywhere in the world [5].

All CD-I players can play CD-DA disks. This system did not become widespread and disappeared entirely from the market by the end of 1997.

2.5 File Allocation Table (FAT)

The File Allocation Table is used to track which clusters have been allocated to a specific file. The FAT is relied upon by the operating system much like a card catalog system is used in a library to locate a book. References in the FAT act as pointers and they point to clusters by numeric reference [6].

When a file is created three things occur (see figure 1.):

1. An entry is made into the FAT to indicate where the actual data is stored in the Data Area.
2. A Directory Entry is made to indicate file name, size, the link to the FAT, and other information.
3. The data is written to the Data Area.

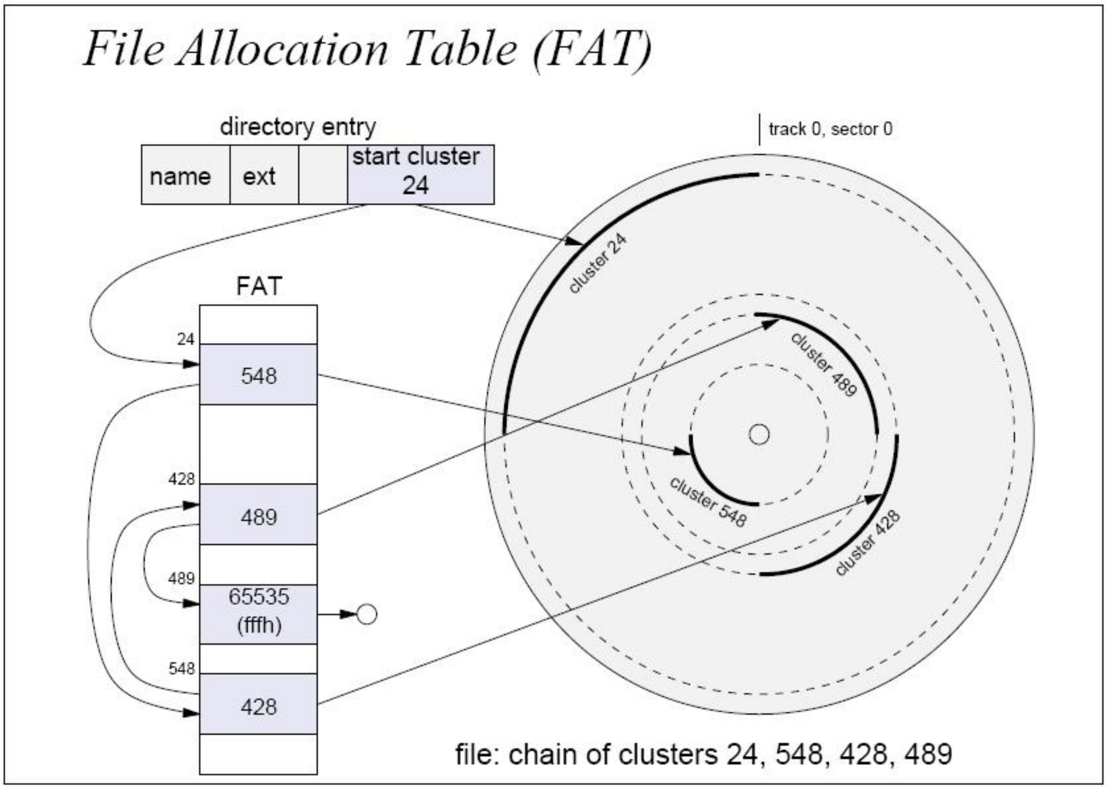

Figure 1. file Allocation Table on Disk

When a file is deleted only two things occur:

1. The File Allocation Table entry for that particular file is zeroed out and shown as available for use by a new file.
2. The first character of the Directory Entry file is changed to a special character (E5 HEX).

3. Nothing is done to the Data Area.

Recovery of a FAT file system file can be accomplished in 2 ways:

The first is:

1. The Table of Content entry for that particular file is linked to the particular location in the data are where the file data is stored.
2. The first character of the Directory Entry file is changed to a legal character.
3. Nothing is done to the Data Area.

The second is :

The data can be “carved” from unallocated space using specialized utilities.

3. Common CD Protection Techniques

In the following sections, some of the widely used CD protection techniques will be discussed.

3.1 CD Cops

CD Cops is a commercial CD protection developed by link data security; it could detect original CDs from copied ones. When running a CD protected by CD Cops, a window titled 'CD Cops' will appear on the screen also the file CDCOPS.DLL and some other files with .GZ_ and .W_X extensions will exist on the CD. The protection mechanism is embedded into the executable file, when this file is executed, it checks to see whether the CD is original, this is done by verifying the physical angle between the first and the last accessible logical block on the CD.

The original CD contains an 8-byte code that holds the angle information and a checking routine that verifies the angle on the CD and then compares it with the encoded value. The angle between the first and the last accessible blocks differs from one CD to another based on the CD-R type; this means no special mastering machine is required to produce CDs protected with CD Cops [2].

The testing routine is known to be complicated, also it sets a timer to check if the testing routine takes much time which usually means it is being traced (a debugger is being used). If it takes much time to perform the check, an error in the program will be produced.

Though CD Cops seems to be tricky it is possible to decrypt the executable file without the original CD this is because the correct code is stored in the program though it is encrypted but this did not prevent crackers to produce tools to decrypt the program without the original CD.

3.2 DiscGuard

DiscGuard was developed by TTR technologies, it stores the protection routine along with the executables on the CD and then encrypts them, a digital code on the original CD is used for the decryption, and this digital code is not reproducible by re-mastering or disc copying. When the program runs from the original copy that contains the digital code, the program will be executed normally. If the program runs from a copied CD then the digital code does not exist, then it might work as a demo version or any other program could be exeuted at the developer's choice [2].

In order to store the digital code, a special machine, DG-Author, is required to perform this task. CDs protected by DiscGuard could be identified by the existence of IOSLINK.VXD and IOSLINK.SYS files. However, there is no universal decoder for DiscGuards but there exist a number of patches that could be used to crack it.

3.3 LaserLock

LaserLock was developed by MLS LaserLock international. It could be detected by a hidden directory that contains unreadable errors. A combination of encryption routine and unique laser marking on the CD surface are used to make it impossible to copy the CD [2].

Though it is practically impossible to copy files from CDs protected by LaserLock, there exists workaround for it, the simple way to go is to set the CD burning program to ignore the errors and copy the CD, also there exist public decoder for this protection.

3.4 SafeDisc [3]

SafeDisc was developed by C-Dilla (Macrovision now) and is considered the most commonly used CD protection. SafeDisc is used by famous game producers like Ubi soft, interplay Entertainment, GT interactive and Microsoft. Despite the propaganda that precedes the release of SafeDisc claiming that it cannot be removed, it took just about one week to break the first game protected by safeDisc, but generally it still the main choice of many software distributors.

The existence of SafeDisc is denoted by the presence of those files 00000001.tmp, clcd16.dll, clcd32.dll, clokspl.exe and dplayerx.dll. On the CD, there exist two files (game_name).exe and (game_name.icd) the .exe file contains the SafeDisc protection whereas the .icd file contains the original game executable but in an encrypted form also it includes some anti-disassembling tricks which makes it difficult to trace the code.

SafeDisc divides the .exe file into two parts, the first one stores only the decrypting information that are used to decrypt the second part, other than the decrypting information it contains no important code.

The second part is encrypted using the first part, which makes it impossible to change anything in the first part; this method is used to deter some anti-debugging programs like soft-ice in particular. Also the .exe file contains a simple detection routine that checks whether soft-ice is running, this is done by using the CreateFileA API call to check the existence of (siwvidstart) driver which is needed by soft-ice, if this driver is detected then a warning message will appear indicating that soft-ice was detected and should be unloaded from the memory. Another trick that is used to detect soft-ice known as INT 68 in which the AH register must contains the value 43h before calling INT 68, if soft-ice is loaded the return value in AX will be F386h, this trick to detect soft-ice works only under Windows 9x.

The second part of the .exe file contains a routine to calculate the code required to decrypt the original executable file, it executes first CLOKSPL.EXE, which views a picture during the loading process, then the routine will calculate the decryption key based on number of conditions. CD errors are read and according to the existence or lack of errors, conditions are either true or false. The calculation result is then XORed with the current date, which means that the code is not the same every day. Eventually the second part of the .exe file decrypts a small routine in the memory that contains the address for calling DPLAYERX.DLL and the correct decryption key.

The DPLAYERX.DLL file works as the previously mentioned .exe file the _DllMain@12 function is called then it decrypts the second part of the DLL, and then the 0x77F052CC function is called with the key to decrypt the original EXE file. The key is Xored once again with the date to produce the key that will be used for decryption; the original EXE file is decrypted in the memory then executed afterwards.

Some workarounds were used to overcome the SafeDisc protection such as 1: 1 copy that involves copying the original CDs as is and simply ignore the errors and usually reading the CD at a low speed (1X) is required, also there exists generic patches that could be used along with the 1: 1 copy to run the game without protection. In addition, there exist unwrappers/decryptors like unSafeDisc that can extract the original .exe file from the .icd file then the extracted file could be burned along with the other files or simply replace the original one with the extracted one after software installation.

3.5 SecuROM

SecuROM was developed by Sony DADC. It could be detected from the existence of one or more of the following files CMS16.DLL, CMS_95.DLL or CCMS_NT.DLL, also the main exe file contains the string 'CMS' two times. There exist some similarities between SecuROM and SafeDisc, some SecuROM data are encrypted in an EXE file and this file could only be decrypted if the original CD is present. Memory dumper (ProcDump) could be used to save the EXE file to the hard disk after the file is correctly decrypted [2].

3.6 VOB

VOB is considered to be the latest commercial protection in the SecuROM and SafeDisc family. The new thing regarding VOB is that it uses anti-disassembling routines that makes the debugging takes considerable amount of time, other than this it works the same way as SecuROM and SafeDis [2].

3.7 Other CD Protection methods

In addition to the above-mentioned commercial CD protection products, some universal tricks were also used, those tricks were based on some assumptions as soon as they become invalid those tricks no longer works.

4. Designing Rigid Protection Method

We called the protection method explained in this research **rigid** because as we knew there is no way to hack or to break it as we will discuss in the following sections.

4.1The Protection Concept

The concept of the protection method is not to let the application to be executed when it is copied to the hard disk. The protection must not be performed in an easily exposed tricky-wise method but programmable method. In such other method the programmers tend to put some checking point in the executable program like checking serials or passwords before starting the application. The hackers use to jump blocks from the start of the executable program and test the remaining code and they always succeeded when they pass the checking points.

In this research we are going to build a rigid hard to break method for protecting compact disks and surely it is not a tricky method and not containing a checking points. We must perform some changes in the program code far enough to be jumped by hackers or it can't be jumped.

The idea behind this method is that we must have a content on CD without a reference to it in TOC (table of content). This means when we write a file to a CD we have to delete the entry of this file from the TOC, but before that we have to save the address of the file in an executable file.

For example if we have a dictionary application, the executable file of the dictionary have the address of the dictionary data file on CD instead of its name to be opened during execution .In this case the application must be executed anywhere but it will refer to the dictionary data file which is on CD and it can't be moved to PC because the file reference was removed.

4.2The main steps

We can summarize the method in four main steps:

1. Making and ordinary application CD without any protection.
2. Calculate the necessary information.
3. Perform the protection(Rewrite the application executable file(s) with the address reference instead of file name).
4. Burning the protected CD.

As shown in figure 2,The first step is to copy the application (which contain the executable file(s), and the data file(s) at least) to the Rewritable CD. In the second step we must select the main source data file(s) and calculate the necessary information from the TOC entry. The third step is to delete the selected file or files, in this case the TOC entry of the file(s) are delete only while the whole data will remain in the CD. After that we must replace the deleted data file(s) name(s) with the address reference in the executable file.

The last step is to replace the application executable file with the modified new one on CD and then make a distribution copy of the last CD with rewritable or writable once CD.

4.3Implementation Aspects

The necessary information that must be calculated before performing the protection method must be retrieved from the TOC entry of the application data file(s), which has the following form:□□**Filename, Attribute byte, Modification time, Modification date, Starting allocation unit, File size**. The most important part of this information concerning the protection method are **Starting allocation** unit and **File size**.

Performing the protection method will be done by replacing the read statement which defined by the file reference with read statement defined by location reference which is retrieved by previous step.

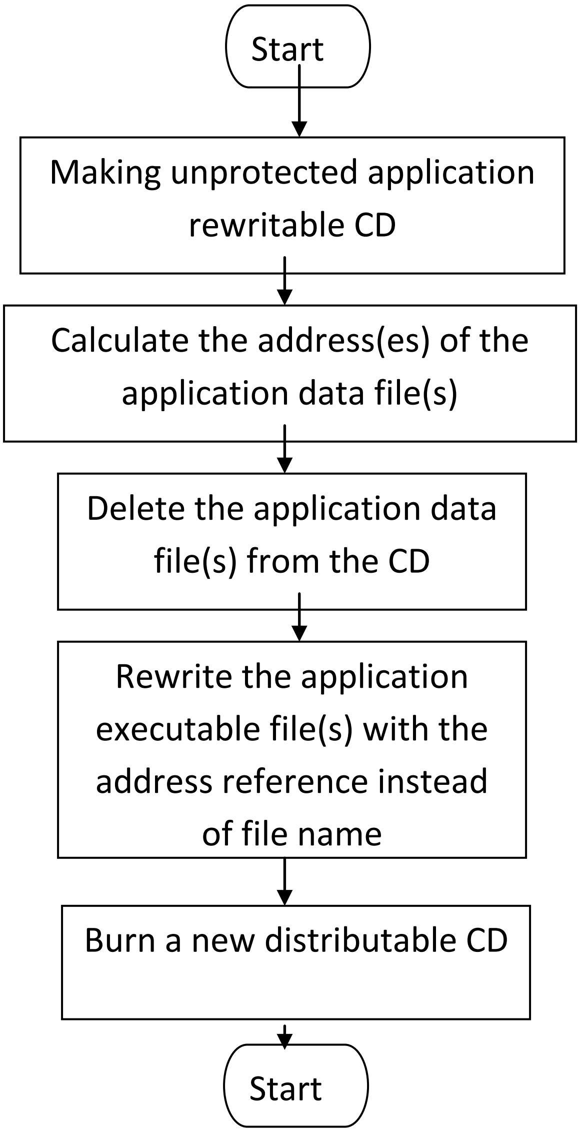
Start
Making unprotected application rewritable CD
Calculate the address(es) of the application data file(s)
Delete the application data file(s) from the CD
Rewrite the application executable file(s) with the address reference instead of file name
Burn a new distributable CD
Start

Figure 2. the flow chart of the complete method

5. Conclusions

The new protection we discuss in this research is a standard protection method with the following conclusion:

- The method provided that the CD must contain an executable application which means, it is suitable for application CD's only. In fact, the audio and video CD's need a protection for not copying the CD's themselves and are low coast in comparison with application CD's.
- This method can be considered as a general protection method because any other case the user must have the ability to copy a backup CD for the probability of damaging the original CD.
- This method of protection can't be broken because there is no way to replace or jump the statement of reading data from the CD because if we can do such thing we must replace location reference of the data file on CD with a reference on the RAM, which is not possible.

References

1. Matthew Territo, Compact Disc Copy Protection, paper, Dec. 2003.
2. Ahmed Enany, CD Protection techniques, paper.
3. Cerven, Pavol. Crack proof your software, William Pollock, 2002.
4. Software Piracy and Uvarta copy protection systems, www.uvarta.com, Nov. 2004.
5. N.V.Philips, "Compact Disc standards and specifications", Sony Corporation,Red book.
6. Techno Forensics , Gaithersburg, 2007.