A Survey Of Contemporary Protection Mechanism For Preventing Piracy Of Digital Discs

Brijesh Rajput

Abstract: - Digital piracy is a major challenge faced by content publishers and software vendors today. The ease of copying and sharing digital content has resulted in piracy. In this paper we examined some recent protection mechanism based on structure of digital disc and other modern technology includes watermark. The objective of this paper is to analyzing the existing technology and some loopholes. Moreover this paper aims at reducing piracy in liaison with the educated user and not with a hacker since the hackers posses special skills as there is no absolute way to prevent copying.

Index Terms: - Anti piracy, Digital watermarking, File encryption, Illegal copying, Sony xcp scandal,

1. INTRODUCTION

The term DRM in today's world seems to be confusing to many people. For the normal users it means to have an extra protection which restricts them in their normal use. For the hackers point of view it is enemy that they constantly try to destroy. DRM is defined as a broad range of technologies that grant control and protection to content providers over their own digital media [1]. In this paper we will particularly focus on DRM systems used to prevent application piracy at considerable extent. Piracy of application software is a serious economic issue to the software developing industry. This piracy is not only restricted to application software. Music industries and Hollywood are most affected from piracy. According to RIAA (The Recording Industry Association of America) One credible analysis by the Institute for Policy Innovation concludes that global music piracy causes $12.5 billion of economic losses every year, 71,060 U.S. jobs lost, a loss of $2.7 billion in workers' earnings, and a loss of $422 million in tax revenues, $291 million in personal income tax and $131 million in lost corporate income and production taxes. For copies of the report, please visit www.ipi.org. The Business Software Alliance (BSA) speaks of an annual global loss of 59 billion US dollar[4]. The survey conducted by BSA includes that 13% of PC user has said that they buy illegal software CD's from street market[4]. Application developers are constantly trying to minimize the risk.This paper aims at minimizing application piracy by describing certain protection mechanism used in the past and some new protection mechanism used to protect from low-end recorder to copying further. This illegal copying is the new challenge for security experts. Optical formats such as CD and DVD are currently the most popular carriers for digital data. Existing format such as CSS and CPRM provides copy protections for DVD and recordable media respectively [2][3]. In the upcoming scenario for distributing electronic content, support for Digital Right Management is important. The reason behind is that more business models are supported by DRM than traditional copy protection systems2 Procedure for Paper Submission

2. MOTIVATION BEHIND COPYING

It has been a debatable question among scholars whether to disregard copyright and make unauthorized copies of software [5][6][7][8][9][10][11]. It is widely reported that members of the general public engage in the occasional unauthorized copying of software [12][13][14][15]. In turn software companies raise an alarm against this illegal practice and consider it as an economic threat. As a result institution like Business Software Alliance and Software Publishers Association has been established in support with the companies [16][17]. According to research conducted by SIGCAS Computers and Society [18], various reasons are discussed in the article for why copying of computer software is acceptable. The very first reason is the software cannot be bound by ownership or copyright because it is believed to be immaterial product [9][10][19][20]. The second reason is "everyone else does this". This reason according to scholars is morally unacceptable [21]. Another argument is "it is easy to copy software" can be found in literature as a potential reason for copying software [21][22]. Another stronger reason given for copying illegally is "high cost of software". This high cost forces an ordinary man to copy software illegally. In addition to this quality is also one factor which should be taken into consideration. Low quality software always allows an ordinary person to copy it. More over small risk of being caught for this illegal practice provides motivation to any person for copying without worrying about the law [21][23].

3. HISTORICAL ASPECT

The first attempts to protect CDs against copying were under taken in early 1990s [24]. At that time CD recorders were not in existence and the developers' main goal was to prevent unauthorized copying of CD content to hard disk. Only two main types of protection system were available in early 1990s, "LaserLock" and code wheel. Those who produces large amount of illegal copies of the disc employs experienced hackers who cracks these protection mechanism without any real effort as the software protection are naive. With the arrival of the recorders it became very important to protect the copying of the digital media. There were more than 50 various protection mechanisms available by the beginning of 2003 and all the techniques of their protection are same in principle.

- Brijesh Rajput is currently pursuing masters degree program in Computer Forensic De Montfort University, UnitedKingdom, E-mail: brijesh_rajput3@yahoo.com

4 Contemporary protection mechanisms

The main contemporary protection mechanism which prevents a qualified user to make mass production of copyright materials (digital media) are listed and explained below

4.1 Non standard formatting

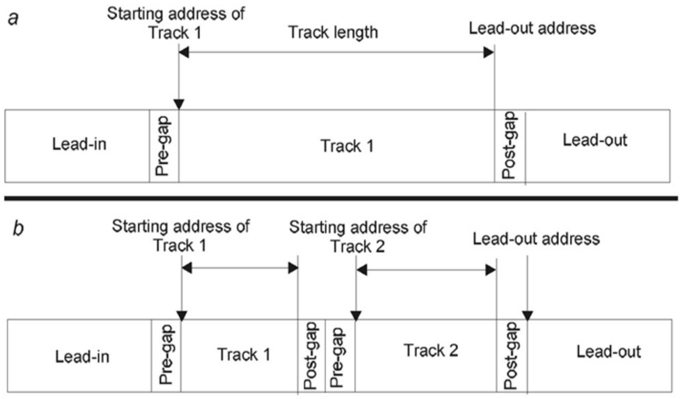
This type of protection mechanism basically produces some specific errors which do not allow the low-end recorders to process information correctly. What if we artificially increase the size to ~800GB of protected file by making changes on length field. This will be the wasted effort to copy such a file to hard disk. However this is not the strongest protection mechanism and this type of protected disc can be copied at the sector level [24] but for that exact number of sectors must be known in advance. The developer of disc can disguise with the disc structure as make the disc looks like blank or beyond any conceivable size. Some protection mechanism use very clever tricks that it introduce bad sectors at the end of the disc. Some recorders will fall in this trap assuming that they are now at the end but the clever recorders analyse the information returned by the drive and that's why they don't fall into trap.

4.2 Incorrect TOC

This is the most famous and a widespread though cruel trick available to use and is most used protection mechanism. A normal audio player is a single-session device. The burning device must support DAO means Disk at Once mode in order to write a disk in single pass. The SAO (Session at Once) mode is not suitable for copy purpose because it forces the drive to write the session contents before writing TOC. As a result a drive has to take a decision about session length and session address. If any attempt made to write incorrect TOC in SAO mode will result into unpredictable drive behaviour. The major drawback of using such protection system is that some drives do not react to Discs based on incorrect TOC. As a result a genuine user might have to throw his/her CD or return it to seller due to incompatibility of his/her hardware with the protection mechanism.

4.3 Adding a fictitious track in genuine track

Adding a fictitious track is sometimes called as fictitious entry. The motive behind this entry is to detect copyright infringement. Data discs which are addressed at sector level provide opportunity which can be used for playing tricks with placement of track. This trick is useful to fight against protected copiers who copies discs track by track rather than sector by sector.



(Figure 1)

Adding a fictitious track results in an incorrect length for the first track. Now correct length must be calculated by subtracting starting address of the first track from the starting address of the second track which is the fictitious track, minus the Post-gap size of the first track and the Pre-gap of the second which is shown in figure 1.1. Let's assume that we have a disc with a single track (Figure 1.1,a). After that, we add a fictitious entry into the TOC specifying that there is another, actually non-existent track, on the disc. As a result, the length of the first track will be reduced by a value equal to the sizeof (TRACK2) + sizeof (post-gap) + sizeof (pre-gap), and a "hole" equal in size to the sizeof (post-gap) + sizeof (pre-gap) bytes (Figure 1.1,b) will be created between tracks. Such a disc will be impossible to copy using standard end-user CD copiers! Placing a fictitious track in the middle of a genuine one (as was shown in Fig.1.1) is not of much interest. It is much better to place the fictitious track entirely in the Post-gap area of a genuine track. In this case, all copiers will go crazy when attempting to compute the number of the fictitious track. Recall, that, according to the standard, the length of any normal track is equal to: min (&Lead-Out, &NexTrack − 150) − &MyTrack − 150. If the track start is located so that min (&Lead-Out, &NexTrack − 150) < (&MyTrack − 150), its computed length will be negative, and most copiers won't even understand what to do with such a track. Furthermore, most copiers store the length of the tracks in variables of the unsigned long type. Therefore, a negative value with a small absolute value, erroneously interpreted by the processor as unsigned, will turn into a very large positive value. In this case, writing the "contents" of a fictitious track will require about 4 GB of disk space on the hard disk, and the same amount of space on the CD to be burnt. However this mechanism is also been broken and such a disk can be copied using Clone CD[24] but in this case it can be easily determined that which one is original and which one is copied.

4.4 Invalidating the track number

Information tracks must be numbered sequentially starting from number 1 followed by number 2 and so on [25]. The common sense possessed by hardware and software developers leads them to hold the same opinion. Therefore, there is agreement that every operating system can rely on track number one being followed either by track number two or by the Lead-out. However, track numbering can easily be modified so that the first track is followed either by, for instance, track number 9, or even by another track "number 1"! Tests have shown that the vast majority of drives and copiers react inadequately to modified track numbering. Sometimes, they refuse to recognize such discs at all. Sometimes, they display the data track as audio. No wonder the copying of modified discs of this type causes serious problems. Even advanced tools like Clone CD and Alcohol 120% are unable to grasp the numbering of the protected disc. Consequently, the copies are either horribly disfigured or completely unusable.

4.5 Data track disguised as audio

The only difference between audio and data track is that automatic correction of the Q- and P-level errors won't be carried out by the drive. However, bad sectors can be corrected manually. The protection mechanism, knowing the true format of the sectors being read, can carry out this correction without difficulty. However, this is not true for software copiers. Therefore, if the disc is copied many times, the number of read errors will grow constantly. At some point, the error-correcting capabilities of the Reed-Solomon codes will become insufficient, and the next copy will be unusable. However, with the quality of optical media today (especially provided that they are handled carefully), the number of Q- and P-level errors are negligible. Therefore, the copies of at least the first three generations are guaranteed to be readable even by old, loose, no-name drives. Therefore, this approach doesn't promise dependable protection.

4.6 The introduction to key marks

Another technique is introducing key marks. All copiers can copy user data area. There are other areas also available other than user data area which has been poorly investigated. First area on the CD is the subcode channel. There are eight subcode channel in total. First channel contains service related information, second contains the number of pauses and remaining six are free. These are the area where the key marks can be inserted and this does not allow standard copiers to copy or write in this area.

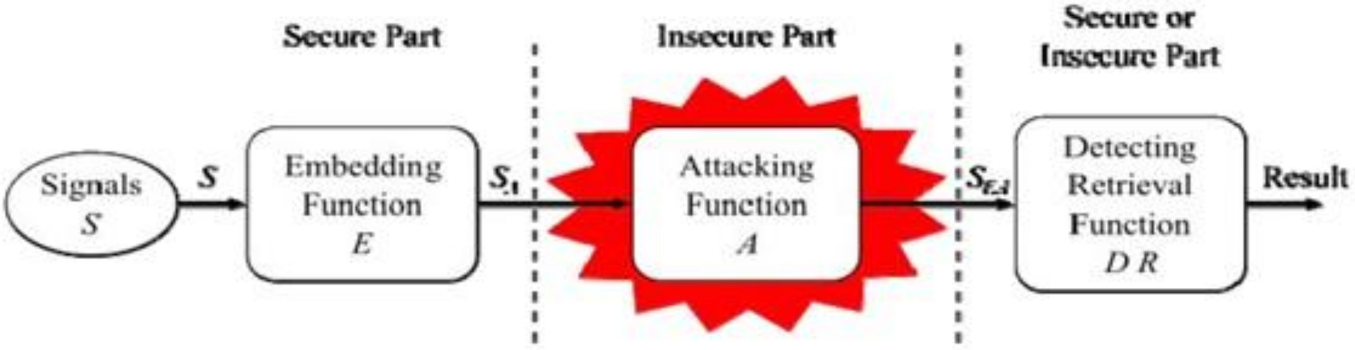


Figure 2 : [Digital watermark life cycle]

4.7 file encryption

Encryption of file contents is also a valuable non standard protection mechanism for preventing copyright infringement. Once encrypted it is not possible to view or play the contents by simply bypassing the shell program. This mechanism is also can be broken at sector level. This protection is based on existing file format and encrypted before writing to the master disc and decrypted when playing back. As mentioned earlier this type of protection method is very easy to crack by simply setting a breakpoint at CreateFile function and wait until the file is opened and trace the EAX register value at the instance of exiting from function. Setting a breakpoint to the memory area containing data read from CD will easily allow a hacker to access a decrypting procedure and after having analysed it is possible to writing a custom decrypting procedure[24].

4.8 SecuRom

A well known proprietary copyright protection mechanism “SecuRom” is developed by Sony DADC[26]. It prevents the copying of whole disc program. It is noted that "SecuROM” installs a shell extension that prevents Windows Explorer from deleting 16-bit executables, and is therefore a controversial DRM scheme[27]. Early version of SecuRom distinguish original copy by modifying CD-ROM’s Q-sub channel."A set of nine locations where the Q-Channel is purposely destroyed is computed by a specific function that calculates nine sector numbers; if the corresponding Q-channel is not readable at these locations, the CD is considered being original[27]."

4.9 Digital watermarking

It has been recognized that current copyright laws are not able to deal with digital data[29]. This motivates researchers towards developing new copyright protection and detection mechanisms. One such effort made is “Digital Watermark”. Digital Watermarking is a technology that can be used for copy control, content identification and tracing [28]. It is not actually the protection mechanism but it is used to store information of copyright owner, distributor and purchaser information. The above figure 2 shows a lifecycle of digital watermark. As seen above watermarking system is divided into three part embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal [29]. When someone tries to modify, it is called as an attack in sense of copyright where pirates or hackers try to remove watermark by modifying it. Possible modification includes extracting a video, lossy compression or intentionally adding a noise[29]. Inserting a watermark can also useful for protecting illegal copying. For example in multimedia content it can be specified that maximum numbers of copies that are allowed legally by inserting watermark. Every time you make a copy then watermark is modified based on algorithm. When it reaches to a maximum limit after that hardware would not create further copies of that digital disc.

Issues in digital watermarking

Some issues based on watermark properties are described below.

1. **Capacity**
   Capacity in the sense of how much amount of data can be embedded in a given signal? And later what is the optimum way to extract and embed this information?
2. **Security**
   It’s difficult that how to determine whether the embedded information been tampered or not?
3. **Robustness**
   How do we embed and retrieve data such that it would survive malicious or accidental attempts at removal [29]

4. **Transparency**
   How do we embed data such that it does not perceptually degrade the underlying content?[29]

5 SONY XCP SCANDAL

One effort is made by SONY BMG towards protecting audio CD from illegal copying but this turned out as a Sony XCP rootkit scandal. What SONY did is they put extended copy protection (XCP) on 52 titles and Mediamax CD-3 software on 50 titles [30]. When user agrees to terms and condition it additionally also installs another software without user knowledge which was later discovered as rootkit or Trojan horse [31]. XCP rootkit installs a device driver which interrupts a call to CD-ROM drive if any other player reads the data section of audio CD. This filterdrive adds the noise and make the music unlistenable. As a result of this a number of lawsuit were filed against SONY BMG and the company ended up by recalling all the affected CDs. When being asked to Thomas Hesse the President of SONY BMG's business division about this XCP scandal he just replied that their ultimate goal is to preventing the unauthorised ripping and the copying and rootkit is the best technology to do it[32].

6 CONCLUSION

As long as CD can be read there is a way to copy it. There is no absolute protection available against copying for optical media [30]. The second realization is "Struggling against professional crackers is absolutely pointless." The end result is that protections are built into CD creator software and firmware of CD players. The two main types of protection are non-standard formatting and binding to the physical characteristics of the media surface. After 1990 when the first attempt was made to protecting Disc and till this time many technologies have been developed that the publishing industry is witnessed that power our digital world. The scope of DRM system and responsibility is proportional to the method of distribution. As the more and more media is distributed worldwide there is a need for a robust and effective DRM system. In this paper we looked at many existing and past technologies but we found that they provide only partial solution to this burning issue. In addition to this people goes for illegal copying because of the high marked price of product. If the product is priced at affordable level than everyone will go for the original version of product instead of getting motivated for copying. At last, if the application level security also supports the protection mechanism describe in this paper than stronger system can be developed as their goal is to reducing piracy and not preventing hacker.

REFERENCES

[1]. Xiao Zhang. A Survey of Digital Rights Management Technologies. Available: http://www.cse.wustl.edu/~jain/cse571-11/ftp/drm/index.html. Last accessed 16th Mar 2013.

[2]. Content Scramble System (CSS). Available: http://www.dvdcca.org/css.aspx. Last accessed 16th Mar 2013.

[3]. TECHNOLOGIES. Available: http://www.4centity.com/technologies.aspx. Last accessed 16th Mar 2013

[4]. Global Software Piracy. 2010 Available: http://portal.bsa.org/globalpiracy2010/. Last accessed 16th Mar 2013.

[5]. Johnson, D.G., 2000. Computer Ethics. Upper Saddle River, New Jersey: Prentice Hall.

[6]. Kallman, E., Grillo, J., 1993. Ethical Decision Making and Information Technology. New York: McGraw-Hill.

[7]. Mason, R.O., 1986. Four ethical issues of the information age. MIS Quarterly, 10 (1) 5-12.

[8]. Moor, J.H., 1985. What is computer ethics? Metaphilosophy, 16, 266-275.

[9]. Weckert, J., 1997. Intellectual Property Rights and Computer Software. Journal of Business Ethics. 6 (2) 101-109.

[10]. Weckert, J., Adeney, D., 1997. Computer and Information Ethics. Westport, Connecticut: Greenwood Press.

[11]. Siponen, M.T., 2001. The Relevance of Software Rights: An Anthology of the Divergence of Sociopolitical Doctrines. AI & Society, 15 (1&2), 128-148

[12]. Gattiker, U.E., Kelley, H., 1999. Morality and Computers: Attitudes and Differences in Mora Judgements. Information Systems Research, 10 (3) 233-254.

[13]. Gopal, R.D., Sanders, G.L., 1998. International Software Piracy: Analysis of Key Issues and Impacts. Information Systems Research, 9 (4) 380-395

[14]. Vitell, S.J., Davis, D.L., 1990. Ethical beliefs of MIS professionals: The frequency and opportunity for unethical behaviour. Journal of Business Ethics, 9 (1) 63-70.

[15]. Traphagan, M., Griffith, A., 1998. Software Piracy and Global Competitiveness: Report on Global Software Piracy. International Review of Law, Computers & Technology, 12 (3) 431-451

[16]. Bowyer, K.K., 2001. Ethics and Computing - Living Responsibility in a Computerized World. Los Alamitos, California: IEEE Computer Society Press

[17]. Forester, T., Morrison, P., 1993. Computer Ethics: Cautionary Tales and Ethical Dilemmas in computing, MIT Press.

[18]. Kuflik, A., 1995. Moral Foundations of Intellectual Property Rights. In: D.G. Johnson, H. Nissenbaum, eds., Computers, Ethics & Social Values. New Jersey: Prentice Hall. 169-180.

[19]. Ladd, J., 1997. Ethics and the Computer World: a New Challenge for Philosophers. Computers & Society, 27 (3)8-13

[20]. Langford, D., 1995. Practical Computer Ethics. Guildford, Surrey: McGraw-Hill.

[21]. Nissenbaum, H., 1995. Should I copy my neighbours' software. In D.G. Johnson, H. Nissenbaum, eds, Computers, Ethics & Social Values. New Jersey: Prentice Hall.

[22]. Cheng, H.K., Sims, R.R., Teegen, H., 1997. To purchase or to pirate software: an empirical study. Journal of Management Information Systems, 13 (4), 49-51

[23]. Kris Kaspersky (2004). CD Cracking Uncovered: Protection Against Unsanctioned CD Copying

[24]. http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-130.pdf

[25]. Xiao Zhang. (2011). A Survey of Digital Rights Management Technologies. Available: http://www.cse.wustl.edu/~jain/cse571-11/ftp/drm/index.html. Last accessed 11th Apr 2012

[26]. SecuROM09 "CD Protection - SecuROM," 2009, http://www.encrypt.ro/cd-encryption/cd-protectionsecurom.html Last accessed 11th Apr 2012.

[27]. William Ku and Chi-Hung Chi. (-). Survey on the technological aspects of Digital Rights Management. Available: http://www.cs.bham.ac.uk/~mdr/teaching/modules04/security/etc/ku-drm.pdf. Last accessed 11th Apr 2012.

[28]. Dukhi, R.G. Watermarking: A copyright protection tool .Vol5 36-41 IEEE 2011

[29]. BBC NEWS. (2006). Anti-piracy CD problems vex Sony . Available: http://news.bbc.co.uk/1/hi/technology/4511042.stm. Last accessed 15 Apr 2012

[30]. spyware information(2005). Available: http://gsa.ca.com/pest/pest.aspx?ID=453096362. Last accessed 15 Apr 2012.

[31]. Neda Ulaby. (2005). Sony Music CDs Under Fire from Privacy Advocates. Available: http://www.npr.org/templates/story/story.php?storyId=4989260. Last accessed 15 Apr 2012.