Article in T-110.501 Seminar on Network Security 2001 ISBN 951-22-5807-2
Publications in Telecommunications Software and Multimedia TML-C7 ISSN 1455-9749
Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory

http://www.tml.hut.fi/Studies/T-110.501/2001/papers/index.html

Software Product Protection

Min Chen
Department of Computer Science and Engineering
Helsinki University of Technology, Finland
mchen@cc.hut.fi

Abstract

This paper presents an overview of some mechanisms that are currently available for the protection of software products. These mechanisms fall into two categories: legal protection approach and technical approach. The emphasis is to focus mainly on technical measures. Some robust and reliable products are introduced as examples of application in this field. The paper gives analytical view on each method presented. In addition, the features of a desirable software protection system are concluded based on the analyses of different methods.

1 Introduction

During the last two decades, the industry in computer software has been increasing rapidly. Today the Internet has become a major distribution channel for digital information. This presents both opportunities and challenges to software vendors. As digital information can be copied and transmitted at great ease, methods of safeguarding the investment are therefore important. Illegal software copying and sharing cause often software companies revenue loss. For every legitimate copy of software that is sold, it is estimated that three or four illicit copies are made. [10] This trend has driven software vendors to implement copy protection mechanisms to protect their applications and revenue by ensuring their applications are used legally.

This paper aims at the methods available for protecting the computer software from misuse. The methods of protecting cover a variety of techniques ranging from legal protection by copyright and patent to technical methods. The technical methods include both hardware-based and software-based approaches. They have very different features. Hardware-based approaches mainly provide preventive measure while software-based approaches provide both preventive and detective measures.

2 Why We Need Software Protection

A software product is expensive to produce but cheap to reproduce due to its digital nature. The cost of producing the first copy may be substantial, but the cost of producing additional is negligible. Digital technology poses two challenges for rights management. First, it reduces the cost of making copies. Second, it allows the copies to be distributed quickly, easily, and cheaply. Thus, we face threats against the software product. Software piracy is a major threat to the software production. Illegal downloading of software from the Internet is similar matter. These may cause severe economic harm and threaten software industries. Threats from viruses and product warranties still remains, but it is beyond the scope of this paper.

2.1 Software Piracy

Piracy is the illegal use or distribution of property protected under intellectual property laws. Software piracy can divide into following categories[4]:

- End user piracy
- Client-Server Overuse
- Internet piracy
- Hard-disk loading
- Software counterfeiting

The end user is the ultimate user of a computer system or product. End user piracy occurs when an individual or organization reproduces or uses unauthorized copies of software. This includes using one licensed copy to install a program on multiple computers; or copying disks for installation and distribution; or acquiring academic restricted software without a license for commercial use.

There are thousands of pirate websites located on the Internet and virtually every software product now available on the market can be located on one of these sites. Therefore, Internet piracy represents perhaps the greatest threats. These pirate websites provide unauthorized copies of software for free download or upload. Internet auction sites also offer counterfeit, infringing copyright software.

Client-server overuse is that the number of users connected to and accessing one server exceeds the maximum number allowed in the license agreement. Counterfeiting is the illegal duplication of software with the intent of directly imitating the copyrighted product. Hard-disk loading occurs when a computer hardware reseller loads unauthorized copies of software onto the machines it sells.

3 Legal Protection Approach

In this section, legal protection approaches are described in terms of copyright, patent and license.

3.1 Copyright

Copyright is a nearly exclusive right of an author to control the distribution and reproduction of his/her original works. [11] In general, a copyright law protects the form of expression of an idea, but not the idea itself. With respect to software, this means that both source code (human-readable form) and object code (machine-executable form), and the related manuals are eligible for copyright protection. But the methods and algorithms within a program are not protected.

Copyright law is a key legal protection mechanism. It can apply to virtually all computer software. The copying of copyrighted software without the permission of its owner may subject the copier to criminal penalties. This is very important for preventing theft and piracy of software products while encouraging developers to promote investments in new products and services.

The advantages of the copyright are the low cost, ease of obtain and speed of implementation. In addition, copyright protection is extremely important in mass-market channels because there is no need of enforceable agreement for implementation. However, Copyright laws usually provide protection only for a country's nationals. The availability of protection for foreign authors usually should under the condition of certain treaties or agreement. Also the scope of protection of software varies among different countries. Although the availability of copyright protection has increased significantly over the world, enforceability is still a major practical problem.

3.2 Patent

A patent is a legal right provided by a government entity (e.g. the European Patent Office) that allows an inventor to prevent others from manufacturing, selling or using the patent owner's invention. [7]

As expected, patent protection may become a valuable competitive tool as compared with traditional copyright protection. A focus of patent protection is to keep from selling similarity in an open market without permission. Inversely to copyright, a patent protects ideas and algorithms in a software product rather than the code itself. A typical example is the protection of functions, methods, system, and algorithms, as well as applied mathematical formulas.

Patents are usually the broadest and most powerful protection form. The benefit of patent holder is to protect from others illegally using the corresponding method, functions etc. However, patents for computer software are not widely used. A main reason for this is that it is very expensive to obtain a patent. To obtain a patent, it usually takes several years for the application process. Furthermore, the disclosure of a large amount of product information required can jeopardize the information secrecy. Therefore, Patent protection is most suitable for core, long-life software features. However, not all software can be patented. As with any invention, the requirements, such as novelty and non-obviousness, will remain.

3.3 License

Much of today's software is not purchased by user but licensed to users. In this case the license agreement will state what rights are granted to the licensee while all other rights remain with the copyright owner.

License is a binding agreement in which one party grants certain rights and privileges to another. In the computer field, a software owner will typically grant a nonexclusive right (license) to a user to use one copy of its software and prohibits further copying and distribution of that software to another user. [4] A consistent and clearly formulated licensing scheme will always be beneficial in taking action against the illegal copier. It establishes the boundary between legal and illegal acts by the licensor with respect of his work.

4 Technical Protection Methods

The legal grant of exclusive rights to software protection via patents, copyright, and license does not provide complete power of control. There is still the issue of enforcement by technical mechanisms. Technical protection includes all programs and devices that prevent the unauthorized use of software. For example, software protection and distribution of licenses via smart cards is a good example. This is a hardware-based anti-piracy tool.

The following is to focus on discussion of technical protection. It involves two major approaches, hardware-based protection and software-based protection.

4.1 Hardware-Based Protection

Hardware-Based Protection provides a variety of features. It is powerful, fast and autonomous. Table 4.1 lists some of the hardware options available:

Company	Product	URL
Marx Software Security	Crypto-Box, SmartX-card	http://www.marx.com
Az-tech Software	EverKey	http://www.az-tech.com
DESkey	Hardware Options	http://www.des.co.uk
Aladdin Knowledge System	HASP	http://www.ealaddin.com
Rainbow Technologies	Sentinel Hardware Keys	http://www.rainbow.com

Table 1: Hardware options

These solutions provide a variety of features. The basic features include authentication procedure, data encryption, access control, unique serial number, key generator, reliable communication, and device identification. These solutions mainly focus on the copy protection. Some also support licensing schemes.

The following are some examples of production.

4.1.1 A Dongle

A dongle is a hardware-based security device that attaches either to the serial or parallel printer port of a PC. [14,9] It is a hardware key that uses codes and passwords embedded inside the key, which can control access to software applications. There is currently a wide range of commercially available protection devices. CRYPTO-BOX Hardware Keys developed by MARX Software Security is an example.

Protection is achieved by enabling software developers to include within a protected program a series of validation tests, queries or locks. These are used to verify that the corresponding model of the dongle is present in the parallel or serial port, and the correct response to queries is being received back. The dongle uses a unique algorithm, which is different for each model, to transform the character string into the numerical response, the result of which is passed back to the calling program for evaluation and validation. If the correct dongle is not detected, the program will not function at all.

However, the effectiveness of such a software protection system depends on the sophistication of the locking mechanism built into the software. It can be weak or strong depending on the level of protection required.

Despite the protection of software from unauthorized access, the dongle can also be used to authorize access to certain features or different versions of a software package. This can be achieved by instructing the system to respond differently depending on the numeric values of the response it receives. Dongles have several disadvantages that have limited their usage. Users usually do not like dongles for a variety of reasons.

Advantages

1. It protects valuable source codes, sensitive text information, and data files;
2. It is fully transparent, which helps to reduce interfering with other dongles.

Disadvantages

1. Can be troublesome to install and use since it requires special hardware driver;
2. Not an option for many software companies due to the additional manufacturing expense;
3. Does not facilitate Internet based distribution of software since it must be shipped to each customer;
4. Not a realizable copy protection mechanism for most software applications.

4.1.2 Media Limited Installations

Some software applications apply a copy protection mechanism refer to media limited installation. [17] By this method, the installation of the software can only be performed a limited number of times. It requires that the program be installed from a re-writable media.

When each installation is performed, the installation program writes to an install counter on the re-writable media. When a specified installation count is exceeded, no additional installations are allowed.

To ensure this protection mechanism, the cryptography must be deployed to encrypt the file containing the installation count. Thus the file is not easy to locate and modify. In addition, the re-writable media (such as a disk) is required to be manufactured hard to copy. For example, the disk may be manufactured to contain a signature that uniquely identifies it. This signature is sometimes referred to a signature. It is designed to be difficult to copy.

Advantages

1. Easy and cheap production;
2. Does not monopolize a slot or port;
3. No password needed;
4. Prevent user locating or modifying installation count.

Disadvantages

1. Problems with the compilation of a licensed installation due to the mechanism used to make the disk hard to copy;
2. Require specific disk type such as floppy drive;
3. Do not support Internet based distribution;
4. Software not transferable to other media;
5. Software is less accessible to the user.

4.1.3 Hidden Serial Numbers [17]

By this protection mechanism, a pseudo-random serial number is synthesized and hidden on the PC when the software application is installed. The serial number is hidden in either an encrypted file or in a special system file. The user must perform a registration process to get the program functioning. During the registration process, software vendor verifies the serial number and supplies customer corresponding password.

Advantages

1. The serial number can be used to detect the location of software;
2. Prevent abusive copies of software.

Disadvantages

1. New registration process needed corresponding to a new serial number when upgraded;
2. Hard for software vendors to trace a prior registration during re-registration, since the serial number is generated randomly;
3. Fairly troublesome for end-users due to high rate of unintentional deletion of serial number file.

4.2 Software-Based Protection

There are a number of software solutions available, and they vary significantly in features and approach. Table 4.2 lists some options.

Company	Product	URL
GLOBEtrotter	FLEXlm	http://www.globetrotter.co
Marx Software Security	Protection Plus	http://www.marx.com
Crypkey	Software Developers Kit (SDK)	http://www.crypkey.com
Az-tech Software	EverLock	http://www.az-tech.com
Microcosm	Unlock-it	http://www.microcosm.co.uk
Rainbow Technologies	SentinelLM	http://www.rainbow.com

Table 2: Software options

Software-Based Protection is easy to implement. Sometimes it is relatively cheaper than hardware-based mechanisms. This software protection mechanism includes features as ease of use, easy maintenance, minimal size increment, redundancy of methods, robust exception handling, strong encryption etc. The following are some examples of products.

4.2.1 FLEXlm

GLOBEtrotter Software and Highland Software developed FLEXlm. It is a widely used license management technology. FLEXlm allows software from several vendors to be supported with a single license management system on a network. It also supports variety of licensing police such as: [8]

- Node locked - software can only run on a particular machine
- User based - software can only be run by particular user-ID
- Site licensing - all users at a particular site may run the software
- Floating license - users anywhere on the network may run the software up to the licensed number of copies

The FLEXlm includes four components, which are license manager daemon, vendor daemon, license file, and application program. When the application program starts, it calls a function to fetch a license, and the license module looks in the license file to find the host and port that the license manager daemon is listening on. The license manager tells the application program which host and port the vendor daemon is on. The client then establishes a connection with the vendor daemon. The vendor daemon keeps track of the licenses in use and their location, and enforces the license policy. Finally, the license module informs the application if the requested is granted or denied. If the vendor daemon dies, then all licenses in use become invalid, and re-obtain of a license is required to run the program.

Advantages

1. Relatively easy to incorporate in your software;
2. Supports the specification of start and end date for licenses and license policies;
3. Allows software from several vendors work under a single license management system on a network;
4. Can run a set of redundant license managers on different hosts on a network.

Disadvantages

1. It is distributed as a shared library;
2. It is relatively easy to decipher the communication between the application program and the license module and then replace the license module with a set of functions that always return a “grant”;
3. The arguments to the license module functions need to be encrypted;
4. Weakness in node locking, kernel support needed.

4.2.2 The Protection PLUS[15]

The Protection PLUS system is produced by the MARX Software Security. It is a software licensing toolkit that insures proprietary security and control. The system consists of two parts. One is the License File Editing facility, which creates encrypted, binary License Files and generates Trigger Codes. The other is the language-specific library, which contains functions for implementing the software licensing features.

License Files allow you to store information to control the execution flow of your application. This can be either completed before sending the application or manipulated by the application remotely using Trigger Codes. License Files may be stored in a file or a CRYPTO-BOX hardware key. The Trigger Codes are numbers generated by a generator that can switch on/off certain program features. These numbers are unique for the computer running the software.

PLUS supports following features:

- Remotely unlock and extend demo versions
- Convert illegal copies into demos using software-based protection
- Protect network-based applications using fixed or floating licensing schemes (Remotely control the number of allowed users)

Protection is achieved by allowing you to authorize a particular computer using a unique ID combination with an encryption algorithm provided in the PLUS library. The system detects illegal copies of the software application. If an illegal copy is detected, you may switch it into a demo mode or abort the program. The PLUS system also protects from copying the protected software from file server, limits the number of workstations connected at same time, or assign the application to specific machines. Moreover, It can detect the client stations aborted and automatically free up the license being used.

Advantages

1. Create fully or partially functional demos;
2. Incorporate expiration dates in your applications to insure payment from users;
3. Establish workstation parameters by limiting network access;
4. Prohibit your application from being copied onto unauthorized computers;
5. Enhance protection scheme by integrating CRYPTO-BOX hardware key.

Possible disadvantages

1. Supports only windows system;
2. May not work with specific environment;
3. Robustness may depends on encryption algorithm.

4.2.3 IP-Safe [18]

IP-Safe is a set of software libraries and tools developed by Power Technology. With it, software providers can protect their products by mean of license. It can work directly with licensees to customize IP-Safe for particular product and marketing needs.

The protection is achieved by using IP-Safe application to internally generate a unique Machine ID number for each PC. This number is based on physical properties of the CPU and motherboard, and is unaffected by operating system upgrades and installs, disc replacements and system utilities.

Advantages

1. Not affected by system utilities, OS upgrades, disc formatting and replacements;

2. No need of hardware modules or special media;
3. Support Internet based distribution of software products;

   Possible disadvantage
4. Robustness of the protection mechanisms may depend.

It is worth mentioning that cryptography is used to strengthen the protection in many of the above methods. However, cryptography may not work well on certain conditions. Note that it is necessary to update of security devices and information in security hardware in time.

5 The Features of a Desirable Software Protection System

As analyzed above, no methods of software protection are perfect. Any method is only makes breaking the mechanism harder, but not impossible. When managing intellectual property, we should choose the terms and conditions that maximize the value of the intellectual property, not the terms and conditions that maximize the protection. It is very important to have a desirable software protection system. This system should effectively prevent the unauthorized access of software programs while allow the authorized use of these programs. Our desired system should have the following features:

- Inexpensive
- Ease of use
- Compatible well with existing unprotected programs and with other protection systems
- Not affected by system utilities, OS upgrades
- Easy for software vendors to incorporate the system into their software distribution
- Robust and should not be denied by the license
- Consideration of management system breaking
- With prevention, detection and response mechanism

As prevention mechanisms are never perfect. Most software products have security bugs, and users make mistakes. Without detection and response, the prevention mechanisms only have limited value. Detection and response are more cost effective.

6 Conclusions

Software piracy has always been a concern of software vendors. There are two classes of protection methods: the legal and technical protection. The legal protection via copyright and sometimes patent law protects software from unauthorized copying, distribution, and sale. With respect to Internet, the law also prohibits users from uploading, downloading, or transmitting unauthorized copies of software online. Anyone breaks the law is liable to criminal penalty. However, patents and copyright does not confer complete power to control software product. Certain markets are not subject to copyright protection. Therefore, we need also adequate technical means for protection. There are many products available on the market either hardware-based or software-based. Many of them available today use very robust techniques and are continually improved with additional encryption and tamper resistance mechanisms such as the protection PLUS. A combination of software-based solution and hardware-base solution will provide additional level of software protection.

Nevertheless, there are few techniques that both satisfy the requirements of developers and legitimate users. Usually, use of any security measure creates problems against average users. It annoys most users and sometimes prevents users from running the legitimately purchased software on nonstandard equipment. Thus, we should evaluate and balance the cost, value, risks, and customer to deploy a desirable software protection system.

References

[1] Aladdin Knowledge System, < http://www.ealaddin.com>

[2] Az-tech Software, < http://www.az-tech.com>

[3] BCS Software Protection Specialist Group, <http://www.bcs.org.uk/siggroup/softprot/prevmeet.htm>

[4] Business Software Alliance, Software Management Guide, <http://www.bsa.org/usa/freetools/business/gsmus.pdf>

[5] Crypkey, < http://www.crypkey.com>

[6] DESkey Data Encryption System, DESlock Software Encryption Utility, <http://www.des.co.uk/deslock.htm>

[7] ESA, Guide to ESA Software Copyright Protection and Patents, November 1998

[8] GLOBEtrotter, FLEXlm, <http://www.globetrotter.com/flexlm/lmmodels.shtml>

[9] Grover, Derrick, The protection of Computer software, pages 63-78

[10] Holmes, Bill, Single-copy security, page 55, Oct. 1988, System international

[11] IEEE, Glossary of IPR terms, <http://www.ieee.org/about/documentation/copyright/glossary.htm>

[12] International Legal Protection for Software, <http://www.softwareprotection.com/>

[13] Microsoft, Protecting Against Software Piracy, <http://www.microsoft.com/piracy/>

[14] Marx Software Security, What is a Dongle? <http://www.marx.com/products/cbox/desc_ dongle.html>

[15] MARX software security, Protection PLUS, <http://www.marx.com/products/ppp/index.html>

[16] Microcosm, < http://www.microcosm.co.uk>

[17] Power Technology, Software and Media Copy Protection Backgrounder <http://www.power-t.com/copy_ protect.html>

[18] Power Technology, IP_Safe Overview, <http://www.power-t.com/ipsafe_ over.html>

[19] Rainbow Technologies, <http://www.rainbow.com>

[20] <http://www.wipo.org>