Techniques using exterior component against software piracy

Qiang Liu

Department of Computer Science, University of Auckland, New Zealand

Abstract

Nowadays, software piracy is a major concern to electronic commerce since a digitized product such as software is vulnerable to redistribution and unauthorized use. Diversified practical methods have been applied in order to prevent this piracy. This paper will focus on some special protective approaches using some exterior components (such as smart cards, hardware security unit and dongles) to make more difficult for unauthorized use of software. The paper will also compare these approaches and offer some insight to the different approaches adopted. In final analysis, it will use the taxonomy from Cronin's [6] paper to try to classify these techniques to provide a means of understanding these methods.

1 Introduction

With the advent of Internet, computer software becomes easier to access, and as such, it has also become easier copy. There are instances where some people maliciously crack the programs and make copies to wholesale them. Hence software piracy becomes a very serious problem emerging in electronic and digital world.

Estimated losses for the software industry from 1994 to 1998 were approaching $60 billion [1] and "[2] according to the Business Software Alliance (BSA) 2001 Report on Global Software Piracy, business software applications accounted for worldwide revenues of $21.6 billion in 2000. During that same year, BSA calculated global revenue losses for the business software application market of $11.75 billion due to piracy." In some countries such as Russia, China, Indonesia, Vietnam, Lebanon and Oman, copies of programs are estimated to exceed 90% in the market place. Actually the main piracy problem areas are Eastern Europe, Latin America and the Asia-Pacific region in the world [1]. It is clear that the software piracy has been an issue of concern for the software vendor.

Due to the large revenues loss software vendors have to pay more attention to develop new protection against piracy. Although legal protection tools like trade secrets, copyright, patents and trademarks have been put into use, they are not adapted for the protection of software. Other methods such as using serial numbers or user/password offer only weak protection. Since programs are digital products they can be copied by bit by bit entirely. Without any help from hardware side, protected software eventually can be cracked by professional crackers. In this paper we present methods to allow only authorized users to run the software with the exterior component. So without this exterior component software can not be run, and thus they will protect against illegal copying and use of software.

2 Techniques using exterior component:

Authors of computer software always feel aggrieved that their works are copied by unauthorized pirates. Consequently program vendors have been researching extensively to invent a foolproof device to prevent piracy, and then they could sell their protected programs at a low price to achieve a large market. Schemes like using smart card and hardware security unit could meet these needs. Although traditional technique like dongle can make pirating more difficult, it brings inconvenience to the clients who use the programs. We will describe these schemes below.

2.1 Dongle:

The dongle is a hardware device connected to a port on a computer that can be read by the software. The dongle contains the serial number of the authorized software. If the dongle is plugged into the computer, its presence can be detected by the software. If you update/change computers or change hard disks, the software must be re-installed and the same dongle will activate the software.

Because every piece of dongle-protected software used its own dongle, so you could have multiple dongles hanging from the back of your computer. It will bring software clients much inconvenience.

At the other hand, since dongle only checks the correctness of the serial number corresponding to the specified authorized software it can not achieve high security level and easy to reverse engineering.

2.2 Hardware security unit [3]

The system of software protection consists of modified software in conjunction with a key cryptogram system which is implemented by a small microprocessor-based security unit that attaches to an input-output port. Each computer is provided with its own pair of public and private keys. The public key is used to encode messages and the corresponding private key is used to carry out the decryption process. Therefore a program would have to be customized for a computer and would only run on that particular computer.

To implement the system it needs some work to be done in two areas which are hardware side and software side.

2.2.1 Hardware side

At program start-up, a “decoding key” which is encrypted using the security unit’s public key cryptogram is passed from the program to the unit.

The security unit deciphers the decoding key and then can use it at the second cryptographic system.

A call to the unit would pass a value and encrypted instruction to it, and after this has been deciphered and executed, a result value will be returned by the security unit to direct the next program section.

2.2.2 Software side

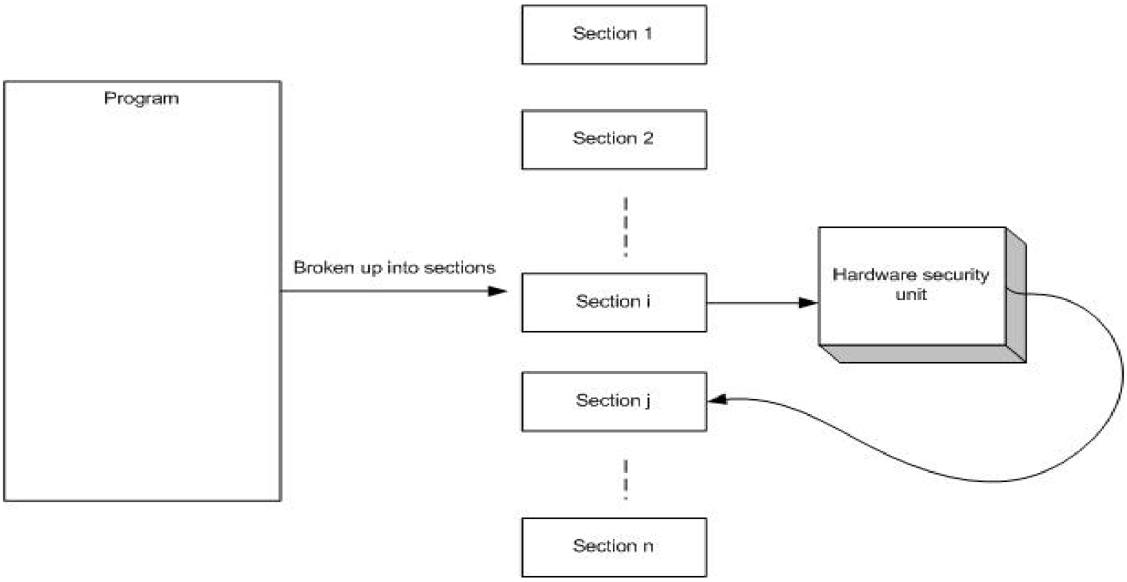

Figure 1

Because each program would not always be executed in linear order, it has the property of branches. Hence each program can be broken up into sections which are connected with the GOTO or CASE statements.(As it is shown in figure1, the program is broken up into n sections.)

Once the program has broken up into sections, the sections have to be rearranged in random order to make the program vague to read.

At next stage a given integer would be returned by the security unit to determine which section would be executed when a value is passed to the security unit. (E.g. In figure 1 as we finished executing section i, we passed a value to hardware security unit and it returned a value which decided to execute the number j section.)

2.2.3 Difficulty need to be solved to implement this scheme

Because each program will be broken up into sections, a high-level language program has to be written so that it can scan the program and identify the places which are used to divide the program. The function calls to the security unit are inserted into these places.

2.3 Smart card [4]

In this scheme some sections of software are substituted by functionally equivalent sections in the smart card. When user wants to execute the software, some sections of the program are executed by the smart card. In this way the protected software is divided into two parts: one part is executed by the computer and another part is executed by the smart card. Also the protected software will not work unless it cooperates with the right card.

2.3.1Implementation:

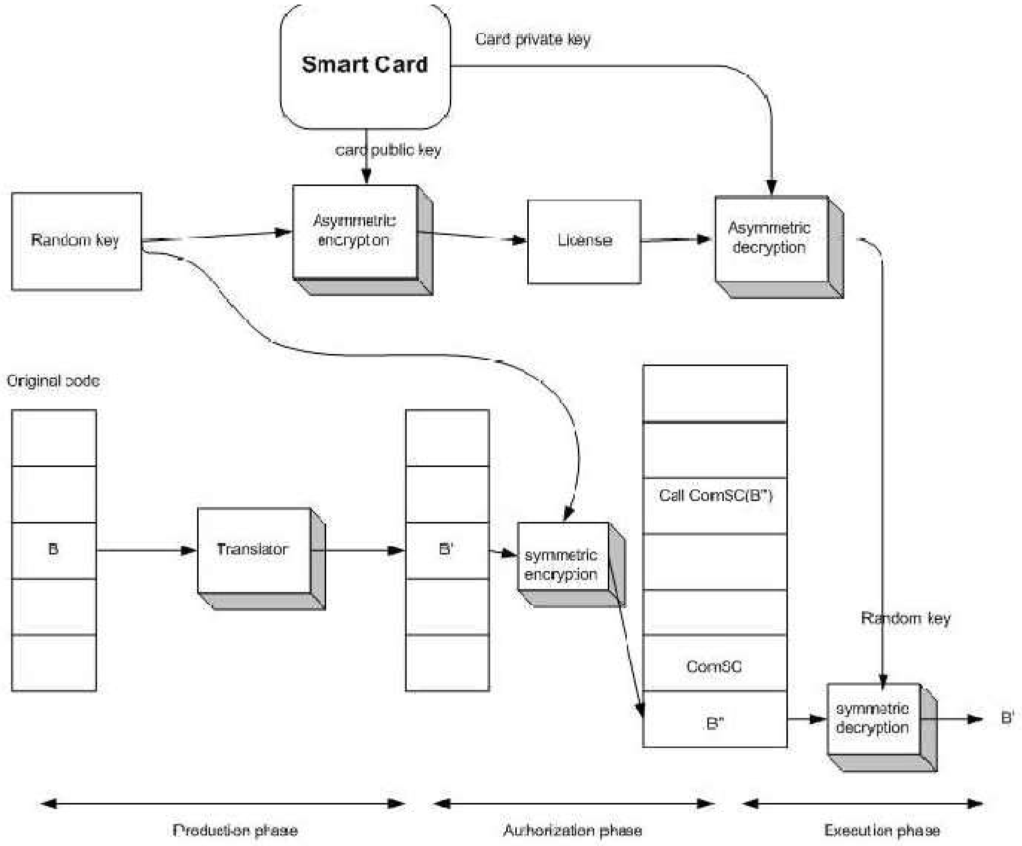

Figure2

As it can be seen from the figure2, at the production phase the original code sections are substituted by their equivalent card specific code. (e.g. B is substituted by B')

At the authorization phase some card-specific code is encrypted symmetrically using random key. (e.g. B' is encrypted into B") The original code sections are substituted by calls to a function that transmits their equivalent protected sections, including code and data, to the card. (e.g. B at original code is substituted by the function "Call ComSC(B")" and B" is also transmitted to the card. So at executed phase B" will be decrypted and executed by the card and a return value will be sent back.) Also a new license is produced containing the random symmetric key, information about conditions of use, the identification of the software and the identification of the license. All the information is encrypted with the card public key.

At executed phase the license is decrypted with the card private key and hence the key contained in the license is used to decrypt the protected sections. After we decrypt the protected sections, then the card's processor can executed the code and return a result value back.

2.3.2 Software management

In order to buy a protected application a client needs to send his random number and the certificate of the public key of his card to the software producer. The software producer will validate the certificate. If the validation succeeds, a new license, which is encrypted together with random number using the received public key, is send back to the client. The card in the client side will verify that the license matches the random number which is sent previously and store it. The software producer will store the all the licenses in his database to be able to produce the new licenses when the clients request. Therefore the application can be distributed and copied freely and it can only be run with the help of smart card.

3 Schemes Analysis

3.1 Contrast and comparison

When the schemes of using hardware security unit and smart card are compared, some similarities can be concluded [5].

-They can prevent the unauthorized execution of the software:

Traditionally when software is installed, it only needs the customers to provide the serial number. This gives the pirate the chance to make pirated software and sell them with the exactly same serial number for the products. It is not the method of using serial number to try to prevent the unauthorized execution of the software.

Although the schemes of using hardware security unit and smart card do not provide absolute and unconditional security, it puts the degree of security at a high level. It is considered that it is easier and cheaper to buy copyright software than to try to crack the protected software and mechanism of the hardware.

On the other hand although authorized user can lend his software and exterior component to his friend and someone else, at each time only one user can run the software. Hence at some point it still prevents the software against piracy.

-Both the schemes need support of hardware component:

The two schemes have to be supported with the help of the hardware component. Without the hardware protected software can not be run by the users.

-Both the schemes use the cryptograph system with a pair of public and private keys:

Public key is used to encrypt the software and corresponding private key is used to decrypt the software. Each program is customized for the each individual private key. So actually each computer is running its own software and user has to purchase software and exterior component for each computer.

-The schemes are independent of specific CPU's:

To decrypt and execute the protected sections both schemes need to use their own processors in their components to do the executions. Thus the protected software can be run on each suitable computer. It's very important that we can choose any computer to be replaced to execute the protected software in case of a computer's hardware troubles.

-They are independent of storage media:

As both systems do not physically prevent copying except the execution of the software, so protected software can be stored in any storage media.

-Copies can be produced without restriction:

Although the user can make copies of the protected programs as many as he can, without the hardware no computer can execute the programs. Also even if he sends his copies to another user who did not purchase the authorized software, but only the corresponding the private key in the component can decrypt and execute the corresponding public key's software.

Although the schemes of hardware security unit and smart card have many similarities, there is a main difference between them which exists in their mechanisms. As we know, the protected the sections in smart card are all executed by the processor of smart card, however each section is still executed by the computer's processor in the hardware security unit since the task of the hardware security unit is only to decide which section will be executed next. With regards to the speed of executing software I would say that the scheme of hardware security unit is faster than the scheme of smart card.

Comparing scheme of dongle with the schemes with cryptograph systems, the dongle's security is much lower than the hardware security unit's or the smart card's security. Because the mechanism in the dongle is only to simply check the correctness of serial number in the dongle, the dongle system has a bad reputation and it can easily be cracked. In some cases it can not be used in the circumstance needing high security.

3.2 Prospects:

If we can have a high-level language which can automatically identify the places where the program is divided for the scheme of security unit and the smart card has a big memory to store enough functions, then we can have universal hardware components to be implemented for different software. As a result many software vendors can share the advantage of the hardware to protect their software from unauthorized execution. At the end it will protect the software against from piracy. This will bring the standards of programming for all the software vendors and software vendor will have to cooperate with the hardware component manufacturer.

3.3 Classification

"[To understand] of the ways in which piracy is currently addressed and directions for the future development [6]" it would be a good idea to classify the schemes that we are currently discussing. It is important that to classify these current methods employed against piracy which will provide a way to help understand possible piracy used by pirates and to direct and to find more advanced methods carried out to protect digitized products in the near future.

According to Cronin's[6] paper the three methods all belong to the technical class and they are all increasing difficulty of duplicating software in order to sell copies in the market. However the schemes of hardware security unit and smart card are in the "Encryption" [6] sub-category and the scheme of dongle is in the "Simple Checking"[6] sub-category.

4 Conclusion

In this paper the two schemes (Hardware security unit and smart card) are needed to be carried out, we have to bind the software with exterior component (hardware). The cost of exterior component has to be added to the cost of software. At first glance it seems to be unreasonable, but on the other hand the protected software can be sold at a considerable low price because there will be almost no loss due to piracy.

Although nowadays they can be applied to some commercial software, they are still at high cost to apply to the personal computer users. One way around this is that software vendors can share burden of this cost for exterior component such that the exterior component can be used for different programs of different software vendors [5]. Another way to solve this problem is that it could be possible to integrate the exterior component in the terminal [3].

There are remaining issues that require further consideration to implement the two schemes discussed above. These other details can not be discussed here due to limited space. In the final analysis the protected software in combination with the use of hardware component is realized when the schemes can bring us with high level of security to prevent against piracy.

Acknowledgments:

I would like to thank my friend Steven Lim for his effort to help me to correct my English grammar.

References:

[1]Moores T. Dhillon G. Software piracy: “A view from Hong Kong” [Journal Paper] Communications of the ACM, vol. 43, No. 12, Dec. 2000, pp.88-93. Publisher ACM, USA

[2]Aladdin Company, white paper for software vendors, “Software Protection-The Need, the Solutions, and the Rewards.” Available on http://www.cuj.com/documents/s=8254/cuj1053119171067/hasp_softwareprotection.pdf

[3]Tim Maude and Derwent Maude, “Hardware protection against software piracy,” Communications of the ACM, 27(9):950-959, September 1984.

[4]Antonio Mana, Ernesto Pimentel, “An Efficient Software Protection Scheme,” in Michel Dupuy, Pierre Paradinas (Eds.): Trusted information: The New Decade Challenge, IFIP TC11 Sixteenth Annual Working Conference on Information Security (IFIP/Sec’01), June 11-13, 2001, Paris, France. IFIP Conference Proceedings 193, ISBN 0-7923-7389-8, Kluwer, pp. 385-402, 2001.

[5]Ingrid Schaumueller-Bichl and Ernst Piller, “A Method of Software Protection Based on the Use of Smart Cards and Cryptographic Techniques”, Proceedings of Eurocrpt’84. Springer-Verlag. LNCS 0209, pp. 446-454. 1984.

[6] Gareth Cronin, “A Taxonomy of methods for software piracy prevention”, Department of Computer Science, University of Auckland, New Zealand, Available on http://www.croninsolutions.com/writing/piracytaxonomy.pdf