A RESEARCHING OF THE PROCESS OF BINDING SOFTWARE TO HARDWARE

A. Yu. Piletskaia, Yu. V. Kobenko
Tomsk Polytechnic University

Information security is one of the most important sphere in Cybernetics. And for Russia this problem is state-of-the-art because of the wide-spread internet piracy and a huge number of hackers. This article explores the commonest ways to protect software using binding to hardware, with a focus on the main approaches to a collection of data from hardware and ways of data processing. As a possible method of solution it is accepted to collect data from main parts of hardware using .Net Framework and further process it using hash-function. The preliminary results reveal that standard facilities of .Net Framework and programming language C# allows gathering information from hardware in simple way. Thus, as a result of research the special software for getting protection code was developed.

Key words: protection software, hardware, hash-algorithms

Introduction

In today's world, wide spreading of Internet arousesconcern about data. The integration of IT technologies in all spheres of life so great, that it is enormously difficult to keep the information private. It is all about not only a different content but also the software. This problem is up-to-date for Russia. Despite the legislation protecting copyrights, a pirated software is available to download. By pirated software is meant the software, which using leads to the intellectual property rights violation.This problem has led to rise of approaches to secure the software from the illegal use. The purpose of this paper is to consider one of the approaches – binding software to hardware. The thesis consists of three parts. The first part includes basic technical methods to protect software. The second part describes the process of binding software to hardware and includes an example of program as a result of researching. The thirdpart concludes.

Methods

Most known methods are described further.

1. Local software protection.

This type of protection was one of the first methods of protection. It's used up to now. The method requires entering a serial number of a product while installation or first running. But wide spreading of networks reveals the main disadvantage of this method. It's very easy to distribute disk images and serial numbers via networks. That is why the method is used in conjunction with other methods.

2. Network software protection

This type of protection is divided on two types: local and global.

Local

A local network is scanned in order to eliminate simultaneous running of programs with identical registration keys on two or more computers within one local network.

Global

This method is used in case if software works with a host-centric server and useless without it.Software can transfer its own serial number to a server. If the number is incorrect, server will refuse to serve. There is the disadvantage in possibility to create a server without verification serial numbers [1].

3. Protection via CD

Method was popular in the early 20th century but now it is old-fashioned.

Recorded program asks for the original CD. Without CD it doesn't work. The main disadvantage is a bypass of protection using special programs for making disk images.

This method is used to distribute games [1].

4. Protection via hardware key

Today hardware key is the most efficient protection tool. Hardware key is a small device connected to computer via USB- or LPT- port.

Algorithm of protection

a) Program is bound to a key using special software;

b) While in operation secured program recognizes the key;

c) If the key if missing or incorrect, program will not work.

Therefore, there is no point in copying secured software because it's useless without hardware key [2].

5. Binding to computer's parameters and activation

Binding to user's information or serial numbers of computer's units and following activation is wide-spread nowadays (e.g. OS Windows).

While installing program computes an activation code–a control value based on units and software of the computer.Then the activation code is transmitted to software developer. Developer generates an activation key fit only certain computer. The advantage is that special hardware is not required. However, if user upgrades configuration of computer, protection will become unsecured. To protect software serial numbers of motherboard's BIOS and hard drives are used generally.

This type of protection will be considered more detailed in the next part of the paper [1].

6. Protection via SaaS

SaaS (Software as a Service)is a software licensing and delivery model in which software is licensed on a subscription. Executable code is located and executed on a server, and available via a thin client.

Software stays protected because it's located on trust side.But this model requires greater attention to protection of servers and transmitted data. There are some other methods of software protection such as, for example, protection of code from analysis [1, 3].

The process of binding software to hardware

This method is based on the fact that each device, included in a system unit, has its own unique number so-called identification number or serial number. The flowchart of the binding process is shown in Figure 1.

The algorithm is following:

1. User starts a special program – information collector;
2. Collector gets ID numbers of devices. For this purpose there is the special class WqlObjectQuery in language C#. Objects of this class is a query in WQL (WMI Query Language; WMI – Windows Management Instrumentation) format;
3. Obtained information is transformed into a single string variable. The hash function is applied to this variable (using SHA-1 or MD5 algorithms). Encoding string is transmitted to the server via Internet;
4. On the server the encoding string is written into the memory of a copy of the program;
5. The copy of the program with hash code is sent to end user as an installation package;
6. During installation process, there are recollection of IDs from devices and encryption of them.
7. Old and new hash codes are compared. If codes are the same, the installation process will be continuing. Otherwise, the process of installation is canceled and user get the error message. The main advantage of given method is the exclusion of recycling the copy of the program because it is impossible to assemble the set of devices with the same IDs like in the original system unit.
8. The disadvantage is that this method exclude the opportunity to replace some devices in the system unit in time between sending encoded string and installing the software on a computer. The given algorithm was successfully implemented within course project [4].

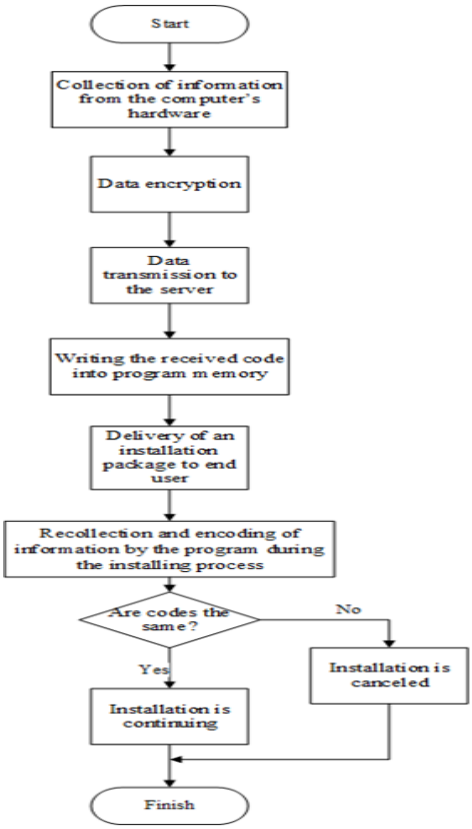

Figure 1. Flowchart for the process of binding software to hardware

Screen shots of working application are shown in figures 2-4.

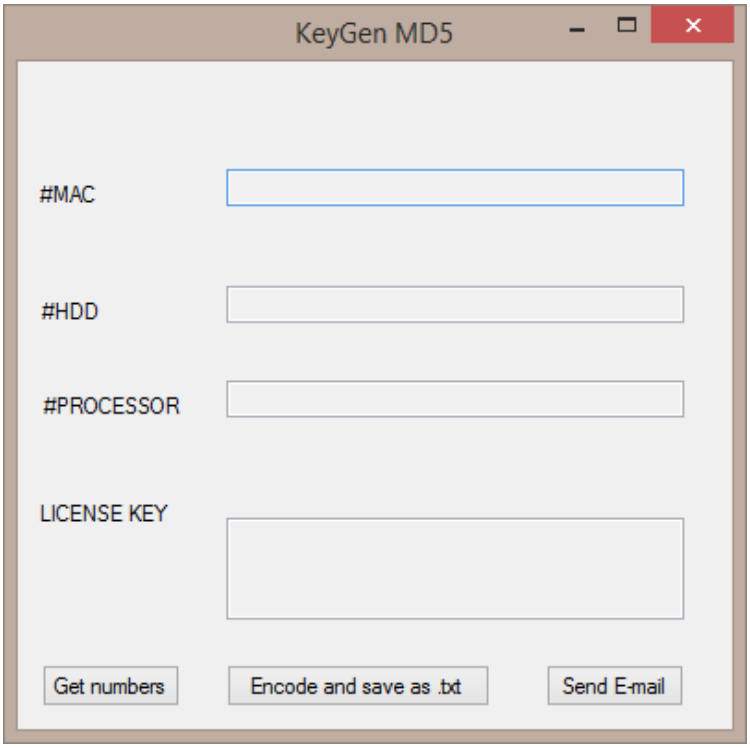

Figure 2. Start screen of the application

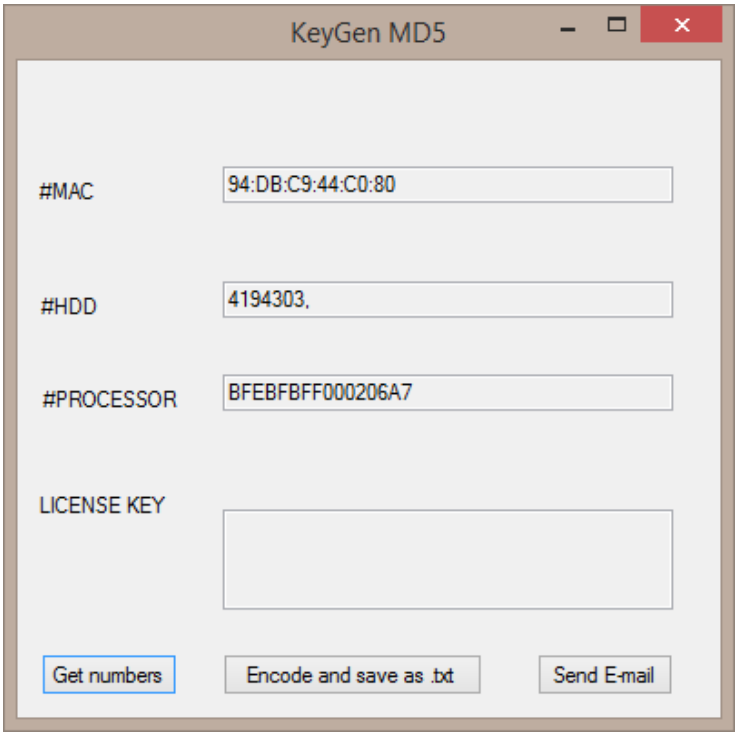

Figure 3. Collected serial numbers of devices

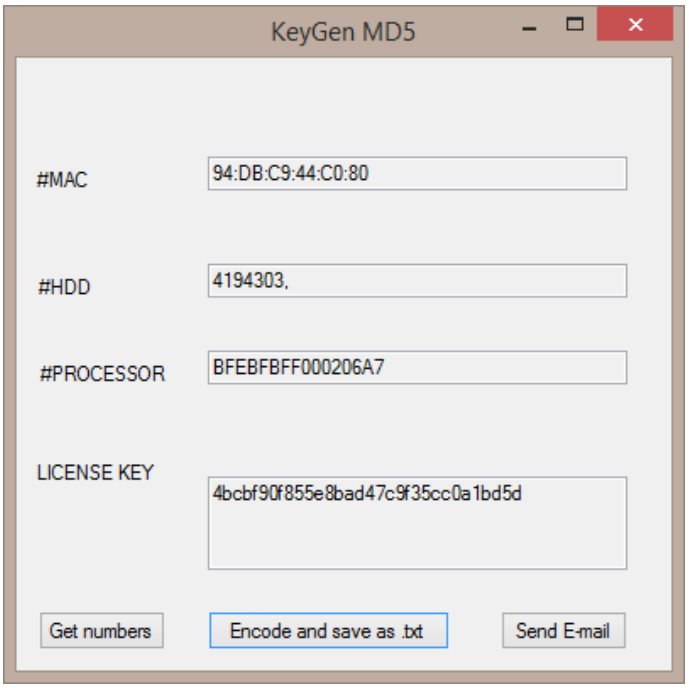

Figure 4. Encoded data in the field "LICENSE KEY"

Conclusion

In short, the software protection methods were considered according to the aim of the paper. One of the methods was considered more detailed and implemented as an application.Basing on this method it is possible to combine it with other existing methods in order to obtain new tools to secure software.

REFERENCES

1. Защита программного обеспечения. Технические, Юридические, Организационные средства защиты // Академик – 2014 – URL: http://dic.academic.ru/dic.nsf/ruwiki/639227 (date: 05.05.2015);
2. Защита с помощью электронных ключей. Технология защиты // Научно-производственная фирма «ЛОГОС» - 2014 – URL: http://logosnsk.ru/guardant/zashhita/ (date:05.05.2015);
3. Безопасный доступ для SaaS. Защитите доступ к облачным приложениям с помощью централизованной аутентификации // SafeNet. The Data Protection Company – 2015 – URL: http://ru.safenet-inc.com/data-protection/virtualization-cloud-security/saas-security-cloud-access-control/ (date: 06.05.2015);
4. Пилецкая А.Ю. Привязка программного обеспечения к аппаратным средствам компьютера // Технологии Microsoft в теории и практике программирования: сборник трудов X Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных, Томск, 19-20 Марта 2013. - Томск: ТПУ, 2013 - С. 341-343.