IPR: An Intellectual Property Right of Software Codes

Ritesh Rastogi Sahi Srivastav Kuldeep Kumar

Abstract

Today an Intellectual Property Right (IPR) of software codes is very challenges task for software developers or companies. A variety of prevention techniques have been developed for intellectual property rights using both hardware and software. But, unfortunately no single technique is currently strong enough to protect the software codes. However, through a combination of techniques software developer can better protect their software codes.

Introduction

Software piracy is one of the main direct threats to software industry, which will bring serious damages to the interests of software developers. It directly affects the revenue of software vendors. As a prevention technique, one of the most promising attempts to protect intellectual property rights includes software water marking. Software water marking is a new research area that aims at providing copyright protection for commercial software. It is relatively new software protection technique appeared in recent decade, whose basic principle is to embed secret information as the evidence to identify an owner, track pirated software. This technique is also used in other kinds of protection and enforcement of intellectual property rights such as text, digital images, digital audio, digital video etc. The software can be protected by two main approaches namely hardware-based and software-based [2].

In the hardware-based technique, the developers or providers used additional hardware components such as a specific CD, smart card etc to execute the software. It is impossible to execute the software without the presence of a trusted hardware component. In the software-based technique, the developers used earlier registration codes, license files, shelling of the codes and many other methods, which protect the software merely via the software itself. The most common implementation technique is to put the registration on the client. It requires a legal token so as to give the user permission to use. The token may be a license key, a license file or an activation code and so on. The software codes are copied by most of the people due to the following reasons :

- Software is intangible or non-exclusive
- Everyone does it
- It is very easy to copy software codes
- It does not harm anyone
- The low quality of software
- Software is expensive
- The risk is minimal

2. Protection:

Techniques of copyright

Various techniques of copyright protection of software codes have been defined. These techniques are categorized into two ways: static watermark and dynamic watermark

2.1 Static water marking

In static watermarking the watermark is stored in the source code, either in the data section or in the code section. The one kind of static watermarking is naming convention like variable name always starts with VAR or numeric is appended at the end of the variable name [1]. Infosys Company is using these concepts [5]. This company is using these concepts at the time of declaring variables. In each variable first letter always starts with their data types like integer variable start with letter i, float variable starts with letter f, double variable start with letter d etc [3]. The other static watermarking recursively applies mathematical operations on a variable, which has no effect in over execution of the program. The extraction of such watermarks does not need to run the software.

2.2 Dynamic water marking

In dynamic water marking the watermarks are generated during program execution and stores in the program execution state. The dynamic water marking hides the watermark in data structures that is built specially for embedding purpose during execution of the program. The Semblance Based Disseminated Software Water marking Algorithm (SDSW) [6] describes the watermarking techniques for the virtual environment like JVM. This is based on java-based applications. SDSW is designed to encode the secret information, which is added to the program after compilation. This encoding of secret information within the program is achieved by adding dummy instructions, which are hard to identify and to replace.

The SDSW is divided into four steps

- Watermark Encoding
- Dictionary Mapping
- Instruction Embedding
- Watermark Recognizer.

These four steps are briefly defined as below:

Watermark Encoding

Watermark encoding for JVM works by manipulating the classes of program. Every class of the program is represented by smaller representation which is calculated by hashing or by manipulating the local variables or instruction of methods

Dictionary Mapping

Dictionary mapping maps the set of possible dummy instructions or variables, which are inserted in the program to encode watermark. Instruction

Embedding Instruction

Embedding explains various techniques for watermarking like watermark the whole class, every method or selected methods.

Watermark Recognizer

Watermark Recognizer recognizes the method to extract the watermark by tracing the dummy instructions. The dummy instructions are scrutinized by scanning the program and each time instruction counterparts to the one in dictionary its corresponding binary is recorded. The recorded binaries are used to reveal the Key to unmask the legitimate buyer

3. Threat Analysis

Any watermark is considered robust if it stands various attacks and distortion attempts. Attacks against watermarks fall in three main categories.

Subtractive attacks

The subtractive attacks try to remove the watermark from the software codes. By this the software code might damage some functionalities or parts of the program. If the software codes are still able to retain enough original content then watermark is considered successful.

Distortion attacks

The distortion attacks will not remove the watermark but might be able to damage or distort it in a way that the owner cannot prove the ownership of the software codes.

Additive attacks

The additive attacks can insert own watermarks in the software codes. The new watermark can either replaces the original watermark or be inserted in addition to the original watermark and thus it would be difficult to prove which watermark was inserted first.

4. Conclusions

of the information society, and thus it is important to capture, store and apply it without any piracy. Through this approach we can show IPR of our s/w codses.

References

[1] Zeeshan Pervez, Noor-ul-Qayyum, Yasir Mahmood, Hafiz Farooq Ahmad, "Semblance Based Disseminated Software Watermarking Algorithm" IEEE 23rd International Symposium on CIS, 27-29 Oct. 2008, PP 1-4

[2] Xuesong Zhang, Fengling He, Wanli Zuo, "Hash Function Based Software Watermarking" IEEE International conference on ASEA 2008, 13-15 Dec. 2008, PP 95 - 98

[3] Siva subramanyam Y, Deepak Ranjan Shenoy, "Computer Hardware and System Software Concepts" Vol -1, Version 1.0, March 2007.

[4] Mikko T. Siponen, Tero Vartiainen, "Unauthorized Copying of Software - An Empirical Study of Reasons For and Against",SIGCAS Computers and Society,Volume 37, No.1, June 2007, PP 30 -43

■ ■ ■

Ritesh Rastogi
Assistant Professor

Sahil Srivastav
MCA Student, NIET

Kuldeep Kumar
MCA Student, NIET