Research Article

Engineering and Technology Journal

A Survey on Program Code Obfuscation Technique

Gaurav Kumar[1]
Department of Information Technology, Bengal College of Engineering and Technology, Durgapur, West Bengal, Email- Kgaurav226@gmail.com

ARTICLE INFO

[1] corresponding Author:
Gaurav Kumar

ABSTRACT

Program code are distributed through internet and suffering from the program theft. Means a program is sold to user and user make own copyright of program called program theft. This is happen because program are easily decomposed into reusable class file and also decomposed into source code by the program users. In this paper practical work show that theft program can easily findable and also proposed a method that shows that if starts working on the method theft program are easily findable. Original developer of program can easily find the program theft and one another technique is watermarking technique that is also a successful technique help the original developer of program to finding program theft, some concept of watermarking also discuss in this paper. With the help of this paper people knows the actual power and use of obfuscator technique. Experimental result in the paper show that approach work successfully.

Keywords: *Obfuscation Technique, Obfuscating Software, Obfuscation Properties, Method of Code Obfuscation and Watermarking Technique*

1. INTRODUCTION

Obfuscation is a basically a term that is used in software engineering and describe the intentional correction of program source code. So that source code is difficult to understand by humans being. In the more prescribed language obfuscation is intentional act of creating obfuscated code such that which is difficult to understand by us basically the aim of the obfuscation is effort of reverse engineering to increase suddenly to the theft part of program.

In the some programming language like scripting languages in that source code is delivered it means that delivered copy of source is unrecognizable and it make more hardly to read. In a compiled program is scrambled and obscured an obfuscator not the source code but directly the copy of source code immediately before compiling [1, 2].

Program code Exchanges of information in now these days become important part of modern society. Some examples of real life like book a ticket online, we communicate with another person using email and embedded system software in car these applications are make use of program code. In now this era in software industry competitions is one of the important factor means do well from another. The revenue of Software Company is huge mainly in the professional level and consequence illegal use of software emerged and with a just click downloads software through internet and user have full control on their physical devices. In some case it seen that famous application is

[1] **Gaurav Kumar**
Department of Information Technology, Bengal College of Engineering and Technology, Durgapur, West Bengal

volume1 issue 2 2016
DOI: 10.18535/etj/v1i2.05
ETJ ,2016, 1, 70-74

attempt to attack [6] such as reverse engineering and program theft is part of reverse engineering. In the last decades it seen that program code are distributed through internet examples range from the games to online banking and many more and it seen that causes problem of program theft. This is happen because program are easily decomposed into reusable class file and also decomposed into source code. Example in the case of java program user knows how to change class file without knowledge of original developer of program and java is platform independent and easily make own copyright of program of another developed program. In this paper proposed method using obfuscation technique help original developer of program to the program theft [2, 3].

Watermarking- Is a technique in which a pattern of bit inserted audio, video, images file that find the copyright information as well as author, right etc or common language you can says that the hiding a message within a image or audio such as it can video also and sometimes it also called data embedding or information hiding. Digital watermark design to be completely invisible in case of image or in the case of audio file it is inaudible [7]. Such as traditional watermarking technique the digital watermarking technique only perceptible under some condition such as using some algorithm otherwise it is imperceptible [5]. Now these days watermarking is used in various application and it is mainly used for security purpose. In this an images is used as a cover to hide the message which is intended for transfer. Since the digital watermarking is the passive protection tool. One of the famous application of watermarking is source tracking in which watermark is embedded into a digital signal at each point of distribution. In this case if the copy of the work found later in that case watermark may retrieve from the copy and the source of distribution is known. The source tracking technique mainly used to detect the source of illegal copied movie [4]. Watermarking technique in now the era is a successful technique in the field of technology as well as computer science and it is widely used in the field of computer science. Watermarking does not reduce execution efficiency of program, user can hardly find location of watermark thus erasing and tempering with watermarking are very hard for user. In the case of stolen of a program means a part of program is copy and make a program then in the case watermark can easily decoded if it presents in the program. It seen that most of embedded watermark in class file are attempt to attack of two type attack to erase watermark such as obfuscator attack and decompile – recompile attack [8].

2. OVERVIEW

Obfuscation

2.1 Properties

Obfuscation change the executable code of program but the only function of program is come to original name means that function and variable comes in original named, unless they would be recoverable from the program. Also the machine or bytecode are so scrambled that the command section that means the high level language command correspond to mingle with those of previous high level instruction often addition unwanted are inserted commands.

2.2 Delineation

The obfuscation only changes variable name, control flow and not the whole program. Means the whole program is not encrypt mainly in this stenography is not applied.

2.3 Method of Code Obfuscation

Changing the control flow- the orders are executed in the program instruction can be rearranged without affecting the functionality.

Variable substitution- Simply renames the name of changed variable.

Change the function hierarchical- specific block in contrary to subroutines logical structure is

volume1 issue 2 2016
DOI: 10.18535/etj/v1i2.05
ETJ ,2016, 1, 70-74

copied from the subroutines to calling point.

Coding-Encryption is mainly important for the camouflage of individual by string as code hardcoded password stored.

Difficult inserting code decompiling-In this case inserted code after end of method mainly which is bringing some decompilierer crash. Mixing of two functions- In this case statement of two functions written alternatively. Columns of variable In this case reconstructing of array or list such as a one dimensional array divided into several one dimensional array, a one dimensional array can be expanded into a multidimensional array etc.

2.4 Obfuscating Software For Program

Obfuscating software depends upon the program language and platform which are used by us and size of obfuscator depends on the program language and platform. Many of them are direct application to the source code. For C/C++ StarForce C++ Obfuscate, Morpher C/C++ Obfuscator etc are actively maintaining C/C++ obfuscators.

For Java ByteCode and Common Intermediate language for .NET there are number of open source obfuscator available such as for java bytecode Java Guard, DashO, ProGuard etc are actively maintained. Mainly ProGuard is suggested by Google for the Obfuscation of android program.

JavaScript – for the obfuscating of JavaScript there are large number of obfuscating software is available such as JSrambler, JSObfuscator etc are used for JavaScript source code and it is main feature of obfuscation of JavaScript code.

Windows Script Encoder- To various scripts such as Jscript, VBScript Specially ASP to conceal files and Microsoft suggest user to use windows script encoder.

2.5 Disadvantage

Mainly in the obfuscation technique can reverse engineering complicate a program time consuming, but not compulsory make impossible and it is limited version of application for the change of obfuscated code.

Watermarking

2.1.1 Encoding procedure

In this procedure we inject a watermark into the program and watermark are encoded into the source code then after the theft of program use of decoding technique we can easily find the theft program.

2.1.2 Decoding procedure

In the decoding procedure it can be automated so that in this case if program are theft it easily decoded and original developer of program can easily find theft program and if the a part of program are stolen then also it easily find.

2.1.3 Application

Digital watermarking is now these era wide range of application such as copyright protection, source tracking, broadcast monitoring, software crippling etc.

3. RELATED WORK

3.1 Solution for finding program original Developer

This is done with the help of Obfuscator-basically in this obfuscation is the intentional act of creating obfuscated code such as which is difficult to understand for human. Mainly in the obfuscator tool

Encode the variables and method names so that the decompiled source code is unintelligible gibberish.

There are many obfuscator tools are available in the market such as for Java bytecode DashO, JavaGuard, for the C/C++ source code StarForce C/C++ obfuscate, Morpher C/C++ obfuscators, for Window Script Encoder Jscript, VBScript and Microsoft also suggest user to use window script encoder and for the JavaScript source code JSObfuscator, JSrambler etc. In some case it also seen that the effective protection of program to the program theft using these obfuscators. In general term Obfuscator is a term which is used

volume1 issue 2 2016
DOI: 10.18535/etj/v1i2.05
ETJ ,2016, 1, 70-74

in Software engineering that is describes the intentional correction of program code that lie the source code is difficult to understand for human and also difficult to defensive. The aim of the obfuscator is the attempt of reverse engineering to increase of theft part of program.

3.2 Digi Cert

In this method a sign related with the applet that indicates the true developer of the applet same like as the watermarking technique and the user whether it worthy reliable or not by checking the sign. The sign also give guarantee of that is original one and never used by anyone and never tempered with anyone else and also signing certificate conform the legitimacy of code and ensure user it has been tempered with digicert. DigiCert is digitally certificate.

4. EXPERIMENT

4.1 Experimental Theory

First ready theft program source code and apply the obfuscating software according to choose programming language source code such as for java bytecode JavaGuard is use for finding theft program it can easily rename the name of variable and function and original developer easily find the own develop program.

Watermarking technique is also successful in the case of theft program in this case watermarking encoded into source code and after the attack it decoded then if watermark present in the previously source code and then it easily show it also help copyright information.

4.2 Experiment Process

First preparing of source code – I select five source files of java and C++ and prepare it to program theft.

Attack – After the preparing source code some of code are taken and make a new program code of Java and C++.

Compile- After making a new program of using the theft code and then compile it for java program jdk 1.7 and a new bytecode is created for new program of java and a new source file is also created for the java program. For C++ code compile into Turbo C compiler and a new source code created for the program.

Apply Obfuscator Software- After the attack JavaGuard is applied to the theft program of java bytecode and StarForce C++ obfuscate is applied to the C++ theft program.

And another is watermarking technique in this we first encode the watermark then after program theft decode the code it easily show that theft code.

4.3 Experimental Result

After the apply obfuscator software it seen that the theft program of variable and function rename as previous one that lies original program and it seen that the theft program are easily findable.

The obfuscating software helps original developer of program to the program theft.

Some of organization suggests that use of obfuscating software such as in case of windows Script Encoder Microsoft suggest user to use obfuscating software.

Watermarking technique is also used in widely to find the program theft in such case watermark are encoded in the source and after the attack decoded the theft program easily find.

5. CONCLUSION

From the above experiment result it seen that theft program can easily find and proposed method also show that it help original developer of code to the program theft and the obfuscation technique now this era widely used in the field of computer science and information technology and watermarking technique also help to find theft program that present in the Paper. From result it's good for original developer of program use of obfuscating software.

volume1 issue 2 2016
DOI: 10.18535/etj/v1i2.05
ETJ ,2016, 1, 70-74

6. REFERENCES

1. https://de.wikipedia.org/wiki/Obfuskation.
2. Kumar, Gaurav. "Novel Method and Procedure for System Security."International Journal of Advance Engineering and Global Technology 3 (2015).
3. Jan Capparat. “Code Obfuscation technique for Software Protection” Pdf.
4. https://en.wikipedia.org/wiki/Digital_watermarking.
5. Frank Y. Shih: Digital watermarking and steganography: fundamentals and techniques. Taylor & Francis, Boca Raton, FL, USA.
6. Kumar, Gaurav. "Best Plan for System Security." International Journal of Advance Research in Computer Science & Technology 3 (2015).
7. Volume 3 2015.
8. http://www.webopedia.com/TERM/D/digital_watermark.html
9. Akito Monden, Hajimu Iida, Ken-ichi-Matsumoto, Katsuro Inoue, Kojji Torri, “A practical Method for Watermarking Java Program” on 24 computer science and application conference compsac 2000.
10. Richard R. Brooks: Disruptive Security Technologies with Mobile Code and peer-to-peer networks. CRC Press,14th May 2012, 7, p 155ff.
11. http://javascript-source.com/.
12. http://stunnix.com/prod/jo/
13. https://jscrambler.com/en/
14. http://www.jsobfuscate.com/
15. http://www.codewall.net/
16. http://proguard.sourceforge.net/results.html
17. https://msdn.microsoft.com/en-Us/library/ms227229(v=vs.80).aspx
18. Kumar, Gaurav. "SKInternational Journal of Multidisciplinary Research Hub." (2015).
19. KUMAR, GAURAV. "Best Plan to Protect Against Phone Phishing Attack."American Journal of Computer Science and Information Technology *(AJCSIT)*3.5 (2015).

Author Profile

Gaurav Kumar: - He is pursuing the degree in Information Technology from the Maulana Abul Kalam Azad University of Technology (Formerly known as West Bengal University of Technology) Kolkata, India.

Him area of Interest are Information Security, Digital Watermarking, Digital Image Processing, Design and Analysis Of Algorithm, Operating System, Computer Architecture, Cloud Computing, Data structure, JAVA, C, C++, PYTHON.

DOI: 10.18535/etj/v1i2.05
ETJ ,2016, 1, 70-74