D.Seetha Mahalaxmi, Dr. S. Viswanatha Raju / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 1, Issue 4, pp. 1579-1582

Revolutionary Approach for Protecting the Software

D.Seetha Mahalaxmi,
Associate Professor,
Department of Computer Science,
JNTUHCEH, Kukatpally,
Hyderabad.

Dr. S. Viswanatha Raju
Professor,
School of Information Technology
JNTUH, Kukatpally,
Hyderabad.

Abstract

In this paper a revolutionary approach to protect the software were discussed. Software watermarking techniques was discussed. The various types of watermarking techniques such as static software watermarking and dynamic software watermarking were given. At the end, a more mathematical approach fro embedding a given watermark into software using logical inference were briefed.

Keywords

Software watermark, static software watermark, dynamic software watermark.

1. Evolution of Watermarking

In the advanced development of Internet, the software program can be transmitted from one location to another location. While the program is transmitted the attacker tries to conceal the contents of the program. A software program can migrate from machine to machine in a heterogeneous network. The program chooses when and where to migrate. In this course the attacker even to tamper the contents of the software program. In order to protect the software program from unauthorized modifications, there are various techniques that are available. A new technique called Software Watermarking is used to protect the Software program from the unauthorized access [1].

2. Importance of Watermarking

In addition to malicious attacks, agent reverse engineering process of de-compilation the source code is also a great threat from any software-based program. It is rather easy to reverse code the source code, which is a great threat for any software dealer. The code can be illicitly modified, or secret data can be revealed, or intellectual property stolen. All of the information attacks become much easier based on the analysis of the Software Agent's source code.

3. WATERMARKING TECHNIQUES

Watermarking is a technique where we embed a secret message into a code message. It is an object that discourages intellectual property theft, or while such theft has occurred allows us to prove ownership. There are various watermarking techniques that are available such as digital watermarking and software watermarking.

3.1 Digital Watermarking

A Digital Watermarking [3], has emerged as an enabling technology for protecting intellectual property rights of digital information. Digital Watermark provides an efficient solution. A digital watermark travels from host to host on a network and acts like a "detective" that detects watermarks and collects evidence of any misuse.

3.2 Software Watermarking

Software Watermarking is a technique to embed a secret message into a cover message [1][2]. Fingerprinting is a similar to watermarking, except a different secret message is embedded in every distributed cover message. This

may allow us not only to detect when theft has occurred but also to trace the copyright violator. There are two different types of software watermarking, they are static software watermarking and dynamic software watermarking.

3.2.1 Static Software Watermarking

Static Watermarks [1] are stored in the application execution itself. There are two types of Static Software Watermarking. They are Code Watermarks and Data Watermarks.

Code Watermarks

Code Watermarks are stored in sections of the executable that contains instructions.

Data Watermarks

Here Watermarks are stored in any other section, including headers, string section, debugging information section and etc.

Advantages of Static Data Watermarks are:

They are easy to construct and recognize.

Disadvantages:

They are susceptible to distortive attacks by obfuscation. In simplest way it breaks all strings into sub strings, which are then scattered over the executable. This makes the watermark recognition nearly impossible.

3.2.2 Dynamic Software Watermarking

Dynamic Watermarks are stored in a program execution state, rather than code itself. There are three kinds of Dynamic Watermarks. In each case the application is run with a predetermined input sequence which makes the application enter a state which represents the watermark. The method differs in which part of the program state the watermark is stored, and in the way it is extracted.

Easter Egg Watermark

A piece of code that gets activated for a given input. The defining characteristics of an Easter Egg Watermark is that it performs some action that is immediately perceptible by the user, making watermark execution trivial. The main problem with Easter Egg Watermark is that they seem to be easy to locate. Once the right input sequence has been discovered, standard-debugging techniques will allow us to trace the location of the Watermark in the executable and then remove or disable it completely.

Dynamic Data Structure Watermark

Here Watermarks are embedded within the global declaration of a program. The watermark is extracted by examining the current values held in a variable, after the end of the input sequence has been reached. This can be done using either a dedicated watermark extraction routine, which is linked, with the executing program or by running under a debugger.

Dynamic Execution Trace Watermark

A Watermark is embedded within the trace of the program as it is being run with a particular input. The watermark is extracted by monitoring some property of the address trace or the sequence of the operation executed.

4. Characteristics of Software Watermarking

The characteristics of any steganograhy can be given by taking data rate, stealthy and resilience into consideration.

Data Rate

The quantity of the hidden data that can be embedded within the cover message.

Stealthy

Expresses how imperceptible the embedded is to an observer.

Resilience

Expresses the hidden messages degree of immunity to attack by the adversary.

5. Attacks On Watermarking System

In order to evaluate the quality of watermarking scheme we must also know how well it stands to the various types of attacks. There are mainly three kinds of attacks that are possible. They are:

Subtractive Attack

An effective Subtractive attack is one where the watermark can be successfully removed.

Distortive Attack

An effective Distortive attack is one where additional watermark can be transformed in such a way that cannot be detected.

Additive Attack

An effective Additive attack where additional watermarks are embedded in order that original message can never be identified.

6. Designing Issues

There are mainly three issues that we have to consider while designing the Software Watermark Technique.

Required Data Rate:

The size of the watermark must be irrespective when compared to the size of the original program.

Form of Cover Program:

The transmission of a program on a heterogeneous network.

Expected Threat Model:

The threats that are expected are reverse engineering, tapering on a given piece of software program, and so on.

7. Conclusion

In this paper we have discussed the requirement of software watermarking. The various types of watermarking technique, such as, digital watermarking, and software watermarking, the characteristics of software watermarking and the attacks those were possible on software watermarking.

REFERENCES

[1] Christian Collberg, Clark Thomberson, "Software Watermarking: Models and Dynamic Embedding", In ACM SIGPLAN – IGACT Symposium on Principles of Programming languages (POPL98), San Antonio, Texas

[2] C.Colleberg and C.Thomberson, and D.Low, "On the limits of software watermarking", in Technical Report #164, Dept. Of Computer Science, University of Auckland, 1998.

[3] Jian Zhao and Chengui Luo, Digital Watermark Mobile Agents, Fraunhofer center for research in computer graphics, Inc.