International Journal of Engineering Inventions
ISSN: 2278-7461, www.ijeijournal.com
Volume 1, Issue 7 (October2012) PP: 20-21

ATTACK MODEL OF VERSION BASED SOFTWARE WATERMARK

D.Seetha Mahalaxmi[1], Dr. S. Viswanatha Raju[2], Dr. A. Vinay Babu[3],
[1]Associate Professor, Dept. of CSE, JNTUHCEH, Hyderabad - '85
[2]Professor, H OD of C S E, JNTUHCEJ, Wrarangal
[3]Principal, JNTUHCEH, Hyderabad – '85

Abstract:—Software Watermarking is an important tool for combating the Software Piracy. Software Watermarking is an approach to the problem of copyright protection that involves embedding ownership information in an executable program. The software watermark acts like an identifier and helps in proving the ownership of the owner. In this paper an Attack Model of VBSW, a brief account on Version attack, and LOC are discussed.

Keywords:—VBSW, version attack, LOC attack

I. INTRODUCTION

Software Watermark is a technique where a watermark W, is embedded into a program such that W can be reliably located and extracted from P even after P is subjected to semantic preserving transformations such as code optimization and obfuscation. The utility of a software watermark depends on its resilience against semantics-preserving code transformations: it is easy to destroy the watermark via simple transformations. The goal of the Software Watermarking is to come up with watermarking techniques that are "expensive enough" to break in terms of time, effort, or resources.

Embedding Techniques

A lot of research is done in order to embed a given watermark into a program, such as Basic Block sequence[1] in which a software serial number is encoded in the basic block sequence of a program's control flow graphs, register interference graphs [3], watermark is embedded in a control flow structure [5]of a designed piece of a program, Stern et al [4] embeds the watermark in the relative frequencies of instructions throughout the entire program using a spread spectrum technique.

Attacks on Software Watermark

Davidson's method is easily destroyed by many locality-improving optimizations, Davidson [2]. This method provides no protection against additive attacks; if the basic block structure to encode the watermark is reorganized, it is clear that the original watermark can no longer be retrieved. reordering of the block sequence [3] . The main limitation of this is addition of new nodes[5]. But these watermarks [4] are relatively vulnerable to relatively simple automated transformative attacks that do not have too great impact on program performance.

Version Based Software Watermark

It is observed that a lot of research is done on various embedding techniques, and the attacks that are possible on these embedded software watermarks. The main theme of the paper is to opt for a new method of obtaining the watermark which is known as Version Based Software Watermark.

Version Based Software Watermark, also known as VBSW, is a method to evaluate the value of Version watermark. The version watermark can be computed by making use of Lines of code and Version number of software. Since it is fact that LOC and version number plays a vital role in the software, these two terms are used for computing the version watermark.

Attack Model of Version Based Software Watermark

A Model is a frame which shows the pictorial representation of the sequence of actions. An attack model of the Software Watermark gives the various attacks that are possible on software.

Alice the author of the software has embedded secret information, known as watermark, and uploaded into the server, for the use by all other members of her organization. Danny, an attacker, has performed various transformations on Alice's software so that Alice is unable to prove her ownership.

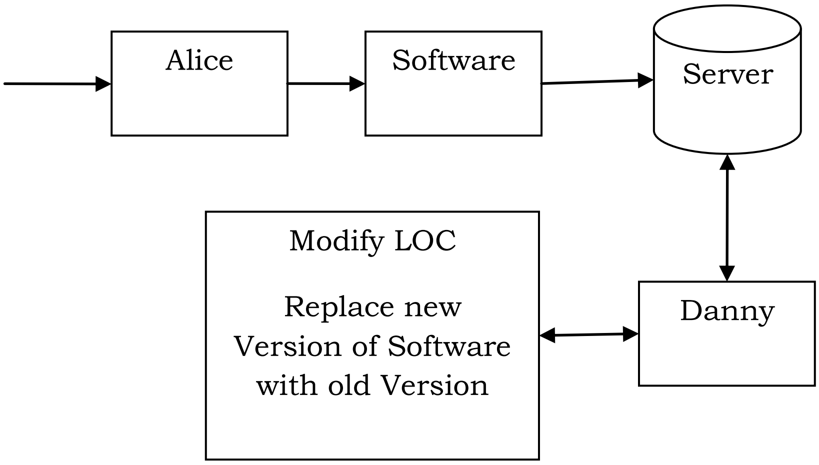

Fig. 1. Attack Model of Version Based Software Watermark

Two types of attacks are shown

i. Updating the LOC, i.e insertion of new lines or deletion of existing lines so that some of the functionality of the software is missing,

ii. Replacement of new version software with old version software.

Definition of Version Attack and LOC Attack

Definition 1 (Version Attack): An attacker replaces the current version software with the old version software is known as Version attack.

$$VA\colon S'''(z) \neq S(z)$$

Definition 2 (LOC Attack): The updation of the lines of code of the original software by the attacker is known as LOC Attack.

$$LA\colon S'''(l) \neq S(l)$$

Quality of VBSW

It is observed that the watermark is extracted effectively even after subjecting it to various attacks.

II. CONCLUSION

In this paper the purpose of Software watermark its definition, various embedding techniques of software watermark, attacks that are possible on these embedded software watermark are discussed. Finally a new method for creating a watermark known as Version Based Software Watermark, also know as VBSW is introduced. The attack model of this VBSW and the two different attacks are identified and defined.

REFERENCES

1. R. L. Davidson and N. Myhrvold. Method and system for generating and auditing a signature for a computer program. US Patent 5,559,884, September 1996. Assignee: Microsoft Corporation.
2. Robert L. Davidson, Nathan Myhrvold, Keith Randel Vogel, Gideon Andreas Yuval, Richard Shupak, and Norman Eugene Apperson. Method and system for improving the locality of memory references during execution of a computer program. US Patent 5,664,191,September 1997. Assignee: Microsoft Corporation.
3. G. Qu and M. Potkonjak. Analysis of watermarking techniques for graph coloring problem. In IEEE/ACM International Conference on Computer Aided Design, pages 190{193, November 1998.
4. J.P. Stern, G. Hachez, F. Koeune, and J.-J. Quisquater. Robust object watermarking: Application to code. In Information Hiding, page 368
5. R. Venkatesan, V. Vazirani, and S. Sinha. A graph theoretic approach to software watermarking. In 4th International Information Hiding Workshop, Pittsburgh, PA, April 2001.