Muhammad Azwan Ibrahim

SOFTWARE MANIPULATIVE TECHNIQUES OF PROTECTION AND DETECTION: A REVIEW

INTRODUCTION

In the digital era, everything is now relies on software. Software plays an important part in banking, trades, medical, production, entertainment and education. Software vulnerability leads to software piracies, code stealing and software tampering. This does not only affecting the software industries, but can caused more troubles such as in economic and legal situation, where people nowadays tend to tamper or manipulate software in the favours of their purposes in every sectors.

Illegal manipulation of software is one of the biggest issues in software security. There have been a lot of extensive studies related to the software security such as steganography, obfuscation, watermarking, birthmarking and many more. Some of them have existed in literatures from the studies done years ago, but are still being practiced until today.

There are numbers of real life cases where tampering could be a serious threat to community, for instance; a case as of petrol station in Silibin, Ipoh has been reported in the year of 2013 by the Malaysian enforcement authority where the owner had manipulated their fuel pumps to gain more profit. Similar cases also had been reported in India in the year of 2008.

Several studies and techniques are applicable to prevent such problems. This article summarizes techniques applicable conducted from the previous studies.

STEGANOGRAPHY

Steganography defined as the method of hiding information by using innocuous carriers by means of covering the existence of the secret information. The word steganography itself was derived from ancient Greek, which means to cover or hide. It is not intended to replace cryptography but rather to complement it. By concealing information with encryption, it will reduce the chances of the information being revealed.

CRYPTOGRAPHY

Cryptography is the method of scrambling data into something that is not understandable. Normally steganography and cryptography are used together as both of them complementing each other. Usually, a message that is going to be hide using steganography technique, first has to be encrypted so that even if the hidden information is successfully revealed; it would still be very difficult for the unintended party to understand the actual meaning of the message.

OBFUSCATION

Obfuscation is a technique to complicate the control flow of an instruction stream and data structures which contain sensitive information to mitigate from code reverse engineering. Although an adversary has successfully revealed the code, whether in the form of original source code or

assembly, it would be very difficult to understand the flow and thus reduce the likelihoods of the code being reverse-engineered.

SOFTWARE WATERMARK

Software watermarking can be defined as the process of embedding additional information into software, without interrupting the functionality of the software itself.

The first patents based on the concepts of software watermarking were filed in 1994. The watermarking proposed was used to identify unauthorized copies along with the source.

In 1996 Microsoft Corporation has filed a patent which utilizes software watermarking concepts. This was done by reorganizing blocks of codes so that the code blocks become a unique identification on each software distribution.

FINGERPRINTING

Fingerprinting concepts is basically same as watermarking, except that fingerprinting embeds unique identifier information on each distribution copies of software. This may not only detect an occurrence of software violation copies, but also able to trace the violator. A fingerprint may include vendor, product or customer information.

SOFTWARE BIRTHMARK

Software birthmark is one of the rarely used methods on securing a copy of software. It has quite a different approach compared to software watermark. The general concept of software birthmark is as found in the computer virus signature concepts; to produce a unique identification of the software. There are two important characteristics to differentiate between the software watermark and software birthmark;

(a) In software watermark, it is often necessary to embed external information, data or code within carrier software, whereas it is not required in software birthmark.

(b) Birthmark could not be used to identify ownership, or source of distribution but rather to confirm that software or code whether it is in partially or in fully, is a reproduction of others.

CONCLUSION

The aim from this research is to propose an effective method and framework in the future for detecting and securing software by utilizing some of the methods discussed above. The application would be on the protection of software based instruments that relate with trade and consumer activities. This would directly benefit both business and consumers community by means of trustworthy transaction.