ONLINE MODULES:
NOVEL MODEL IN SERIAL-BASED METHOD OF SOFTWARE COPY PROTECTION

AHMAD GHADIRI HAKIMI

A project submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Science (Computer Science)

Faculty of Computer Science & Information Systems
Universiti Teknologi Malaysia

JANUARY 2013

This project is dedicated to my family for their endless support and encouragement.

ACKNOWLEDGEMENT

In the name of Allah, Most Gracious and Most Merciful.

I take this opportunity to express my profound gratitude and deep regards to my guide Dr. Imran Ghani, my supervisor for his exemplary guidance, monitoring and constant encouragement throughout the course of this thesis. The blessing, help and guidance given by him time to time shall carry me a long way in the journey of life on which I am about to embark.

I am obliged to Information Security students in UTM that cooperated with me to filled questioners about the proposed model.

ABSTRACT

One of the most significant concerns of software corporations is protect their products against unauthorized copying. Since now the researchers proposed some copy protection models that all of them have weakness to protect against unauthorized copying. The goal of this project is propose new model of serial-based method that more security against illegal usage. This project offered Online Modules model in serial-based method that it spilt the software to two parts. Fist part run in client and second part run in web service, when the software needs to use the second part then the software connect to the web service and the server check the software license. If the license has been valid then run the second part. This model compares with online activation model in serial-based method and the results show the proposed model has more secure against unauthorized copying.

ABSTRAK

Salah satu masalah yang paling signifikan dari perusahaan perangkat lunak adalah melindungi produk mereka terhadap penyalinan yang tidak sah. Sejak sekarang para peneliti mengusulkan model copy perlindungan bahwa semua dari mereka memiliki kelemahan untuk melindungi terhadap penyalinan yang tidak sah. Tujuan dari proyek ini adalah mengusulkan model baru dari seri berbasis metode yang lebih keamanan terhadap penggunaan ilegal. Disertasi ini menawarkan model yang online Modul dalam serial berbasis metode yang tumpah perangkat lunak untuk dua bagian. Bagian Fist berjalan di klien dan bagian kedua dijalankan dalam layanan web, ketika perangkat lunak perlu menggunakan bagian kedua maka software terhubung ke layanan web dan server memeriksa lisensi perangkat lunak. Jika lisensi telah berlaku kemudian jalankan bagian kedua. Model ini dibandingkan dengan model Aktivasi online di serial berbasis metode dan hasilnya menunjukkan Modul Online memiliki keamanan yang lebih terhadap penyalinan yang tidak sah.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Protection of software against cracking is one branch of software security. Usually, developer software use complex codes for enhancing security in order to crackers have problems to cracks the software. But they can do it just with spend more time. In this paper reviewed the popular and strong algorithm about crackproofing and bring up an idea for enhance crackproofing. (Cerven, 2002)

1.2 Problem Background

Nowadays, the people life involved to the technology as continue life without technology is so unbelievable. Also, technology caused people have a more time for do their works and it can avoided of duplication work and day by day people more need to new technology. One of the most important parts of technology is software that it can useful for people to all fields such as business, education, entertainment, health, communication and daily routine.

For creating software need to spend substantial money and software developer to make powerful application for attracting more customers and earn more money. Because of this they should spend more money, time and use expert groups of software engineering for preparing the software. Unfortunately, when the software enters to markets for selling, crackers start to crack the software in order to other users allow use it without pay money. Some users buy it but other users use illegal software by the crack. It makes a great loss to the software developer because of this the developers do not have enough motivation for create a costly software. At first the developers estimate that how many of license will sell with what price, after that they spend money and time for creating the software. Imagine, the users cannot use cracked software, what happens? It's clear; the developers can more sell of their software so they can spend more money for preparing software and every day we will see powerful applications come to markets that they can more useful for us. (Djekic , *et al.*, 2007)

1.3 Problem Statement

In today's world, piracy accounts for $35 billion in lost revenues to software companies. Software developers usually have a strategy for protecting software against illegal usage of their applications. The developers often sell a license with software for activation the application. When user enters the license code, application investigates the license validity and if the entered serial number has been correct then application been activated and user can use it. Crackers can open and change software codes in order to misuse the application as illegal access. A general trend that appears is software from a large company is usually more secure while smaller start-up companies seem to lack the necessary means to protect their software. But almost all models of software copy protection have some breaches to bypass licensing because crackers allow to all machine code of the software. (Ankit, et al., 2007)

1.4 Project Goal

The main goal of this project is to propose the new model which is capable to improve the weakness of software copy protection models. The model doesn’t allow to crackers to have all the machine code of software. Another goal of this study is to research on some models’ trends of software copy protections and to understand the vulnerabilities of their methods.

1.5 Project Objectives

This project follow the below objectives:

1. To study software copy protection methods for problem analysis
2. To propose and implement a novel model in serial-based method of software copy protection that called “Online Modules” model.
3. To test software copy protection in Sales Invoice software.
4. To compare Online Modules model with Online Activation model

1.6 Project Scope

This project is limited to review some methods and models of software copy protection and propose Online Modules model. Also it tested on an application.

1.7 Significance of Study

This subject helps to investors that they can get more benefit of invest in software which cause software industry grow up faster and more powerful than past.

1.8 Project Organization

This study consists of four chapters. The chapters are organized according to different works that involved in this study. The detailed organization of this report is described in following paragraphs. This section presents how this report is organize in different chapters.

Chapter 1 of this report consists of overview of the study, problem background, problem statement, objectives, scope and significance of this study.

Chapter 2 is about a review of the literature related to the research area. It discusses some methods and models in serial-based of software copy protection.

Chapter 3 consists of the research methodology that it used in this project.

Chapter 4 is about the analysis and design of the project.

Chapter 5 is about implement the project and analyzes its performance. Also this model compares with Online Activation

Chapter 6 is about discussion, conclusion and the model future

REFERENCES

Bobba, J. et al., 2009. StealthTest: Low Overhead Online Software Testing using Transactional Memory. *Appears in the Conf on Parallel Architectures and Compilation Techniques (PACT)*, september.

Djekic, P. & Loebbecke, C., 2007. Preventing application software piracy: An empirical investigation of technical copy protections. *Journal of Strategic Information Systems 16*, 12 july, p. 173–186.

Madou, M., Anckaert, B., Sutter, B. D. & Bosschere, K. D., 2004. Hybrid Static-Dynamic Attacks against Software Protection Mechanisms. *Ghent University*.

Ankit, J., Kuo, J., Jordan Soet, J. & Tse, B., 2007. Software Cracking.

Cerven, P., 2002. Crackproof Your Software. In: San Francisco: William Pollock, pp. 3-6.

Corporation, A., 2012. *Home Page.* [Online]
Available at: http://www.acunetix.com/
[Accessed 23 December 2012].

Eberhardt, G. & Nagy, Z., 2006. Copy protection through software watermarking and obfuscation. *Department of Measurement and Information Systems Budapest University of Technology and Economics Budapes*.

Genov, E., 2008. Designing Robust Copy Protection for Software Products. *International Conference on Computer Systems and Technologies*.

Ionescu, A., 2004. Introduction to NT Internals, Part 1: Processes, Threads, Fibers and Jobs, Relsoft Technologies.

Joye, M., 2008. On White-Box Cryptography. *Security of Information and Networks,,* pp. 7-12.

Linn, C. & Debray, S., 2003. Obfuscation of Executable Code to ImprovenResistance to Static Disassembly. *Department of Computer Science University of Arizona*.

Li, S., 2004. A Survey on Tools for Binary Code Analysis. *Stony Brook University*, pp. 37-52.

Merckx, G., 2006. *Software Security thirough Targetted Diversification,* s.l.: Katholieke University IT Leuven.

Nigurrath, S., 2005. Cracking with loaders: theory, general approach and a framework. *ARTeam*.

Nützel, J. . & Beyer, A., 2006. Towards Trust in Digital Rights Management Systems. *ACM workshop on Digital rights*.

Razeen, M., Ali, A. & Sheikh, N. M., 2003. Software protection: The Last Line of Defense against Piracy.

Schneier, B., 1996. Applied Cryptography. In: s.l.:John Wiley & Sons, pp. 39-44.

Shi, W., Lu, C. & Zhang, T., 2004. Attacks and Risk Analysis for Hardware Supported Software Copy Protection Systems. *College of Computingy School of Electrical and Computer Engineeringz Georgia Institute of Technology Atlanta*.

Stallman, R., 2003. Stallman and the GCC Developer Community. *Using the GNU Compiler Collection, GNU Press*.

Sutter, D., Bus, D., Bosschere, D. & Demoen, K., 2000. On the Static Analysis of Indirect Control Transfers in Binaries. *Ghent University and Katholieke Universiteit Leuven*.

Tanenbaum, A. S., 2002. Computer Networks. In: 4th ed. s.l.:Prentice Hall, pp. 156-165.

techtarget.com, 2009. *digital signature (electronic signature).* [Online] Available at: http://searchsecurity.techtarget.com/definition/digital-signature [Accessed 22 December 2012].

Usama, M. & Sobh, M., 2011. Software Copy Protection and Licensing based. *IEEE,* pp. 856-861.

Zhao, J. & Yao, N., 2009. A New Method to Protect Software from Cracking. *World Congress on Computer Science and Information Engineering*.