MIGRATION VIRTUAL TRUSTED PLATFORM MODULE STATE USING TPM EMULATOR

KILAUSURIA BT ABDULLAH

A thesis submitted in fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information System

APRIL 2010

To my beloved mother and father

ACKNOWLEDGEMENT

In the name of ALLAH , The Most Gracious and the Most Merciful.

Immeasurable gratitude to Allah S.W.T for giving this servant an opportunity to undertake and complete this piece of work. The hard work and pains or researching this study bear the fruits in-depth and invaluable knowledge, indeed.

In particular, I wish to express my sincere appreciation to my main thesis supervisor, Dr.Rabiah Ahmad, for encouragement, guidance, critics and friendship. Also, in preparing this thesis, I was in contact with many people, researchers, academicians, and practitioners. They have contributed towards my understanding and thoughts.

To my passionate husband and family, thank you for this golden opportunity that has open the horizon of my limited knowledge in Security Information. I would like to dedicate this report to them for their encouragement, love, tolerant, understand and support.

Lastly, to all colleagues of the CASE, I extend my gratitude for the support; priceless contribution and the time they have sacrificed in making this report a success.

ABSTRACT

The purpose of this study is to investigate the application of Virtualization Trusted Platform Module (vTPM) and migration of vTPM states and develop a simulation migration model between platforms. TPM Emulator, software based TPM was used as the benchmark for the proposed vTPM. A vTPM instances between platforms based on modified TPM Emulator has been proposed in this study to reduce problem of migration vTPM states between platforms. The effect of different combination of UNIX domain socket and TCP socket on the platforms of the developed simulation migration model was studied and the effectiveness and shortcoming of TPM Emulator were highlighted. Results were compared between previous TPM Emulator running instances on single host platform and between platforms. It was discovered that modified TPM Emulator can perform the vTPM instances not only in single host platforms however includes between platforms. In addition, the use of simulation migration model was also proposed and investigated, named as Virtual Machine Monitor Management (vTPM Manager) to handles vTPM state life cycles. Simulation migration vTPM states results demonstrated that vTPM instances are able to be created and saved between platforms. Furthermore, from the case studies of vTPM challenges showed that the proposed simulation migration could be used as an alternative platform to adequately identify adequate and complete models for vTPM states life cycles.

ABSTRAK

Kajian ini dilakukan bertujuan mengkaji penggunaan Virtualisasi Kebolehpercayaan Modul Platform (vTPM) dan migrasi situasi Virtualisasi Kebolehpercayaan Modul Platform (vTPM) dan membangunkan model simulasi migrasi antara platform. Emulasi Kebolehpercayaan Modul Platform (TPM Emulator), yang berdasarkan kepada perisian digunakan sebagai bandingan bagi kaedah yang dicadangkan, Virtualisasi Kebolehpercayaan Modul Platform (vTPM) yang berdasarkan pengubahsuaian terhadap Emulasi Kebolehpercayaan Modul Platform (TPM) dicadangkan dalam kajian ini bagi mengurangkan masalah migrasi situasi antara platform. Kesan penggunaan gabungan soket utama UNIX dengan soket Penghantaran Kawalan Protokol (TCP) ke atas platform simulasi model migrasi yang terbentuk dikaji dan keberkesanan serta kekurangan Emulasi Kebolehpercayaan Modul Platform diutarakan. Kajian simulasi dilakukan untuk membanding Emulasi Kebolehpercayaan Modul Platform yang dijalankan pada satu hos platform dan beberapa platform. Dengan menggunakan pengubahsuaian Emulasi Kebolehpercayaan Modul Platform, Virtualisasi Kebolehpercayaan Modul Platform (vTPM) boleh dijalankan bukan terhad kepada satu hos platform, tetapi beberapa platform. Di samping itu, penggunaan Pengurus Mesin Pemerhatian Virtualisasi (VMMM) telah dicadangkan untuk menguruskan situasi kitaran hidup Virtualisasi Kebolehpercayaan Modul Platform (vTPM). Hasil simulasi migrasi situasi vTPM, menunjukkan vTPM berkeupayaan untuk dibina dan disimpan di antara platform . Tambahan pula, daripada kajian kes kekangan vTPM menunjukkan hasil cadangan simulasi migrasi boleh digunakan sebagai platform alternatif untuk memperolehi model yang lengkap bagi kitaran situasi vTPM.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

TC	Trusted Computing
TCG	Trusted Computing Group
TCB	Trusted Computing Base
TPM	Trusted Platform Module
vTPM	Virtualization Trusted Platform Module
VMM	Virtual Machine Monitor
VMMM	Virtual Machine Monitor Management
VM	Virtual Machine
TCPA	Trusted Computing Platform Alliance
NGSCB	Next Generation Secure Computing Base
ETS	Embassy Trust Suites
TSS	Trusted Software Stack

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

This chapter describes the introduction of this project including all the related information regarding the trusted platform modules. The next section (Section 1.2) will present the background of the problem that will be solved in this project. Section 1.3 will explain in detail the problem statements that became issues to be solved in migration vTPM states using TPM Emulator. Section 1.4 provides the project objective, the step by step guide on what is required at the end of this project. Section 1.5 will explain the limitation or boundaries within the project scope. Section 1.6 will discuss about the significance of this project, including the importance why a research is required in this area. The final section provides a summary of this chapter.

1.2 Background of the Problem

Development in Trusted Computing (TC) technology have impacted all sectors such as e-services, online banking, grid computing, digital right management, secure supply chains and mobile computing. To ensure TC will continue a great significance for constructing a secure information system, the Trusted Platform

Module (TPM) is the trusted root of platform [1]. This means TPM transfers trust successively from trusted root to BIOS, operating system (OS), and TC application environment. The application of TC to Grid Computing is widely discussed. However, much of this works aims to prevent or detect provider misbehavior.

There is a critical problem addressed by products developed which includes increasing threat of software attack regarding increasingly sophisticated and automated tools, the number of vulnerabilities being discovered and the mobility of users. In addition, software with security mechanisms are not sufficient to protect information asset such as user data, passwords, certificates, identity information, keys, credit card numbers etc [2]. Therefore, the use of hardware based embedded security solution is an increasingly important approach for protecting information assets from being compromised. This is aligned with Trusted Computing Group (TCG) goal which is to make these protections available across a broad range of computing devices with common software interface to facilitate application development and interoperability.

Trusted Computing (TC) has support the spirit in which the internet was created; the Trusted Computing Group (TCG) has formed by the IT industry [3]. TCG is a consortium that made up of computer and device manufacturers, software vendors and others with a stake in enhancing the security of the computing environment across multiple platforms and devices.

Trusted Platform Module (TPM) is a hardware chip designed to the computer that provides greater levels of security previously was possible [4]. TPM currently existed in more than 15 million PCs, mostly in high end laptops manufactured by HP, Dell, Sony, Lenovo and Toshiba, amongst others. Grid Computing and distributed computing becomes generally available when utilized by TC and is likely to be more widely required. In a Grid, there is a need to expand the cloud of trust between different entities. The computing environment and reliable computational result will drive TC technology to be used by Grid and distributed computing.

Trusted Computing technology is adapted to grid computing to enhance the grid security infrastructure especially in the security modules for grid. These modules provide Trusted Computing features like integrity report and attestation, key migration for the grid through Report, Attestation and Migration modules. Migration module helps to relocate vTPM states from different platforms. It is believed that virtualization can help to significantly improve enforcement of more stringent and fine grained security policies with TC as a current Virtual Machine Monitor (VMM) provides elementary isolation [5].

Existing hardware TPM could not be shared [6]. The hardware TPM is designed for use with single operating system. Thus, it is very limited in resources such as registers, key storage space and it only meant for single owners. However, virtualized platforms include with multiple Virtual Machine (VM) but with different owners. The requirement of vTPM is, with full TPM requirement per virtual machine. Hence, the VM of the virtualized platform can be transient (relocate, saved and stored). An approach to overcome the issue of multiple owner vTPM is by emulating the TPM functionality software in multiple host platforms. Therefore, each VM has its own virtual Trusted Platform Module (vTPM).

1.3 Problem Statement

A review on the list of journal listed in *Cryptologia* [7], migration of a virtual Trusted Platform Module (vTPM) specifically to Grid computing is widely discussed. In consequences, there is a need to establish migration infrastructure necessary to support use of trusted computing in virtualization technology between platforms. Besides that, there is virtualization trusted platform module challenges which are creation, suspend, resume and destroy of the vTPM states [6]. The creation of vTPM instances must be relocate to different platforms for the purpose of virtual machine workloads and cope with hardware failures.

1.4 Project Aim

The aim of this research is to make a creation and relocate the virtual trusted platform module instances that are available to each of their virtual machines by using TPM Emulator between platforms.

1.5 Project Objectives

The objectives for the migration of a Virtual Trusted Platform Module (vTPM) states are:

1. To make a virtual trusted platform modules instances available to multiple host platform using TPM Emulator.

2. To implement the creation of virtual trusted platform module states between platforms.

3. To simulate migration infrastructure using the vTPM Manager as Virtual Machine Monitor Management.

4. To test the creation of the vTPM states between platforms using the vTPM Client.

1.6 Project Scope

The scope of this research comprise of the following:

i. Using TPM Emulator to make a virtual trusted platform module instances available to each of the virtual machine.

ii. Create vTPM Manager as Virtual Machine Manager Management to manage allocation of virtual trusted platform modules resources.

iii. Only apply the creation of virtual trusted platform states between platforms.

iv. The migration simulation infrastructure using the virtual machine (Virtual Box) not as separate physical machine.

1.7 Significance of Project

Virtualization and Trusted Computing are two technologies that complement each other. Virtualization is mending for high availability, the integrity and the isolation of each virtual machine. Meanwhile, the Trusted Platform Module is for security, the chain of trust and the remote attestation.

IaaS (Infrastructure-as-a-Service) Cloud technology is an emerging technology that will allow unlimited number of owners and multiple virtual machines without worrying about ownership cost and problems of physical hardware resources [8]. Virtual Machine technology is the essential key to an IaaS cloud. The migration of virtual trusted platform module states will improves the flexibility of resource management because the running Virtual Machines are relocated to another platform without stopping operating systems.

In addition, from the user's perspective, they can easily deploy their applications on any IaaS Cloud and can relocate to other platform easily. This will of course prevent users from being locked into certain providers and in addition, they can select the most appropriate provider based on costs and performance. Meanwhile, the service providers will also benefit via a more flexible management. Therefore, migration virtual trusted platform module states is important especially in datacenters for making site-wide maintenance easy, including air conditioning facilities and power supply facilities.

1.8 Summary

The proposed solution to make virtual trusted platform modules instances is available to each virtual machine between platforms using TPM Emulator is one of the approaches besides using the hypervisor such as XenServer and VmWareESX. The proposed simulation architecture is by developing the vTPM Manager, vTPM Client and vTPM Database to migrate the vTPM states across the network. The migration simulation architecture between platforms will become a test bed or basic setup for further operations of vTPM states besides creation and relocation between platforms.