A STUDY OF TRUSTED COMPUTING IMPLEMENTATION IN PUBLIC SECTOR INFORMATION, COMMUNICATION AND TECHNOLOGY (ICT) DOMAIN

RUSNITA BINTI ISNIN@HAMDAN

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

Centre for Advanced Software Engineering (CASE)
Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

APRIL 2010

To my husband Mohd Fauzi Haji Ismail, and
children Aida Shaheerah, and Aida Thurayya and
also to my beloved mother for their patience, understanding and dedication

ACKNOWLEDGEMENT

The highest gratitude to Allah the Almighty with whose blessings and permission I have, alas, been able to complete this project report for my Masters Degree.

I would like to take this opportunity to express my deepest gratitude to my project supervisor, Dr. Rabiah Ahmad for her encouragement and guidance. Special thanks goes to all lecturers and staffs at Centre for Advanced Software Engineering (CASE) for their cooperation and support throughout my course at CASE.

I am also very thankful to my husband En. Mohd Fauzi Ismail for his everlasting support throughout this entire period of this project. A million thanks to my family and friends too who always encouraged, motivated and gave me full support to finish this project.

ABSTRACT

The Trusted Computing evolution has introduced a lot of opportunities for Information, Communication and Technology (ICT) that enhance the protection approach to the ICT environment towards computer threats. With time the changes in technology have influenced many giant ICT companies worldwide to get involved in research and development (R&D) in order to simultaneously provide better solutions on leveraging ICT usage in business. The public sector is also not excluded from this influence of developing as a R&D platform provider and implementer. The Malaysian Public sector already made a statement that allows companies in Malaysia to do further R&D in trusted computing. However the implementation level in general in Malaysia and more specifically the Malaysian Public Sector has never been explored. Therefore this study has been conducted to discover the depth of implementation of trusted computing in the public sector ICT Domain. This study attempts to reveal trusted computing usage levels according to its revolution in the public sector agencies. As a result of this study, guidance will be provided for ICT officers to attain better implementation of trusted computing in their organization.

ABSTRAK

Evolusi Trusted Computing telah memberikan peluang kepada Informasi, Komunikasi dan Teknologi (ICT) meningkatkan pendekatan untuk mengatasi ancaman keselamatan komputer. Dari semasa ke semasa, teknologi ini telah mempengaruhi syarikat-syarikat besar ICT terlibat di dalam kajian dan pembangunan (R&D) dalam memberi penyelesaian terbaik sejajar dengan peluasan penggunaan ICT di dalam urusan seharian. Kerajaan juga tidak terkecuali daripada terlibat di dalam perkembangan teknologi ini dari segi menyediakan platform untuk R&D dan sebagai pengguna. Kerajaan Malaysia telah mengeluarkan kenyataan bahawa syarikat-syarikat ICT di Malaysia dialu-alukan untuk menjalankan kajian terhadap teknologi ini. Walaubagaimana pun, pelaksanaan teknologi ini di Malaysia umumnya dan Kerajaan khususnya masih belum diteroka. Oleh yang demikian, kajian ini dijalankan untuk mengetahui tahap penggunaan Trusted Computing mengikut perubahan evolusinya di dalam agensi Kerajaan. Sebagai keputusannya, panduan penggunaan Trusted Computing bagi pihak pengurusan akan dibangunkan agar penggunaannya dapat dilaksanakan dengan lebih sistematik.

TABLES OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

CPU	-	Central Processing Unit
I/O	-	Input/Output
ICT	-	Information, Communication &Technology
IDs	-	Identities
IT	-	Information Technology
MAMPU	-	Modernization and Management Planning Unit
MIMOS	-	Malaysian Institute of Microelectronic Systems
NGSCB	-	Next-Generation Secure Computing Base
PCs	-	Personal Computers
PDA	-	Personal Data Assistant
RND	-	Research and Development
TC	-	Trusted Computing
TCG	-	Trusted Computing Group
TCPA	-	Trusted Computing Platform Alliance
TNC	-	Trusted Network Connect
TPM	-	Trusted Platform Module

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

This chapter will briefly explain the aim of this project. The problem background, objectives, scope of study and its significant will be briefly explained in order to give the reader a basic understanding of the project.

1.2 Problem Background

"The Top Cyber Security List" as published in the SANS website in September 2009 mentioned the most prevalent attacks. This data was brought about through featuring attack data from TippingPoint intrusion prevention systems protecting 6,000 organizations, vulnerability data from 9,000,000 systems compiled by Qualys, and additional analysis and tutorial by the Internet Storm Center and key SANS faculty members. The top most attacks are Application vulnerabilities which exceed OS vulnerabilities, Web application attacks, Windows: Conficker/Down up and Apple: QuickTime and six more.

SANS also announced that the number of attacks is now so large and their sophistication so great, that many organizations are having trouble determining which new threats and vulnerabilities pose the greatest risk and how resources should be allocated to ensure that the most probable and damaging attacks are dealt with first.

Hence, Trusted Computing Group (TCG) has claimed that Trusted Platform Module (TPM) can assist in enhancing security levels in Information Technology tangible and intangible solutions. This is one of the options that uses hardware based mechanisms to achieve a secure environment. Although this statement has been debated since 2003 especially in terms of trustworthy, many giant information technology (IT) companies have only adopted and implemented TPM in their manufacturing to comply with industry standards. Personal computer, network equipment, mobile computing and many more IT assets have been invented using this particular technology in order to provide secure products and services for customers. Therefore conscious or unconscious, we as end users of IT facilities are already part of their target market.

The Public sector in Malaysia is not excluded. In actual fact Malaysia has got a special organization directly contributing in research and development of trusted computing in order to provide trusted solutions for Malaysian requirements. Implementation of this concept however has never been measured to verify whether it can behave according to what has been claimed by TCG; that is the enhancement of security levels in organization.

Furthermore, sometimes this implementation is only known by the organization as a security product that can help them to solve problems. They do not fully know its architecture, its purposes, actions and impacts on the organization’s privacy. In other words, they just follow the trends and put their trust in the principal that a new product with new technology will inherently have strong protection and capabilities.

1.3 Problem Statement

Information security in the Malaysian public sector has been determined as one of the very important areas in providing high profile of communication to the citizen. Leveraging of information technology application under the e-Public sector concept has been spread from urban to sub-urban and remote areas in order to deliver information and services. IT infrastructure installation and development has been progressively built for having interconnection between locations all over Malaysia. Hence just as transport online applications have also been encouraged so as to develop top management to facilitate and improve the public sector services.

This changing of the environment however does not exclude public sector application exposure to threats and vulnerabilities. Therefore a higher demand of security approaches has been raised in each IT development. Confidentiality, integrity and availability principals have also been implemented in every part of the IT solution to gain a secure IT environment.

Since trusted computing (TC) is one of security solution provided by IT vendors and has been part of compliance in industry, we would like to see whether the public sector ICT domain has implemented it or not as one of choices to enhancing security. Whatever the answer is the public sector ICT should be aware of its capabilities and take an advantage of it. Positive and negative issues related to TC also need to be addressed among ICT officer so that they can make better choices during procurement specifications of tangible, intangible services and equipment.

1.4 Research Questions

A research question is a statement that distinguishes the problem to be studied in a project. A few research questions have been determined for this project:

- Is the public sector concerned about the existing TC concept?
- Is the public sector concerned about TC positive and negative impact?
- Has TC technologies been implemented in the public sector?
- Has the public sector implemented any guidelines to achieve security, both tangible and intangible?

1.5 Objectives of the Study

This study will attempt to achieve a few objectives that have been determined in the early stages of this study. The objectives are:

- To identify the components used in analyzing TC implementation in the public sector
- To determine the level of the TC Implementation in the public sector agencies.
- To propose and validate the TC implementation guidelines.

1.6 Scope of the Study

This study was designed to get an overview of the current situation of IT security solutions directly related to TC implementation and indirectly in the public sector ICT Domain. We shall theoretically analyze TC in order to get the TC implementation levels in the public sector.

The survey will involve ICT officer in the public sector especially those who are directly responsible in planning, purchasing and implementing IT security.

1.7 Research Methodology

The research will be done by combining qualitative and quantitative methods. This is because in the public sector, the ICT organization as a whole, there are two different parties directly involved in IT security. One is the planning and monitoring unit and other is the implementation unit.

The qualitative method will be used to interview the planning and monitoring unit which is known as MAMPU. This will be done to get an overall overview of the IT Security situation that is needed to be complied with by all public sector agencies. The same interview will also need to be conducted with MIMOS officers who are directly involved in research and development (RND) of TC in Malaysia. The survey questions will then be distributed to all ministries under the public sector in order to get an overview of TC implementation.

All the data collection will be analyzed and will be used to develop a suitable implementation strategy and policy for TC. In conclusion the approach that will be used to accomplish this study is:

- Interviews
- Questionnaire
- Data Collection Procedure
- Data Analysis

1.8 Significance of the Study

This study is very significant to the public sector ICT domain especially for ICT Officers directly involved in planning and implementing ICT Security in organizations. This study will benefit the public sector in a few of the following aspects:

- Creating awareness to public sector ICT officers about TC concept as one of the IT security options for enhancing security in an organization
- Helping the public sector to have a better understanding on TC technologies that are available on the market by bringing out some security issues that are addressed in the TC.
- Proposing the TC implementation guideline for the public sector that can be used to direct organizations implementing TC in a smart and systematic manner.

1.9 Summary

This chapter primarily focuses on the objective and significance of the study that is to identify the level of use of TC in the public sector. As explained earlier, TC can be a good solution for securing information assets in the public or private sector. Availability of trusted products in the market now can present a big opportunity for the achievement of security goals. However, the integrity of TC products needs to be verified and validated by a third party to ensure none of hidden interests are planted in the tangible and intangible solution. Therefore the public sector IT officer's knowledge needs to be measured in order to provide a suitable strategy that can be referred to in procurement of information assets such as personal computers, network equipment, application development software and services.