TESIS^ APPROVAL STATUS FORM

JUDUL: DEVELOPMENT OF SECURE WINDOWS ENVIRONMENT AND APPLICATION BLOCKER (SWEAB)

SESI PENGAJIAN: 2003/2004

Saya LAI YEN WEI

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Kolej Universiti Teknikal Kebangsaan Malaysia.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

_____ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

_____ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

_/_ TIDAK TERHAD

(TANDATANGAN PENULIS)

Alamat tetap : 1563 , JLN SJ 10/113
TMN SBAN JAYA
70450 SEREMBAN

Tarikh : 21/10/2004

(TANDATANGAN PENYELIA)

SHEKH FAISAL BIN ABD LATIP

Tarikh : 21/10/2004.

CATATAN: ** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.
^ Tesis dimaksudkan sebagai Laporan Projek Sarjana Muda (PSM)

DEVELOPMENT OF SECURE WINDOWS ENVIRONMENT AND APPLICATION BLOCKER (SWEAB)

LAI YEN WEI

This report is submitted in partial fulfillment of the requirements for the Bachelor of Information and Communication Technology Technology (Software Development)..

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
KOLEJ UNIVERSITI TEKNIKAL KEBANGSAAN MALAYSIA
2004

ADMISSION

I admitted that this project title name of

DEVELOPMENT OF SECURE WINDOWS ENVIRONMENT AND APPLICATION BLOCKER (SWEAB)

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : _____ Date : 21/10/2004
(LAI YEN WEI)

SUPERVISOR : _____ Date : 21/10/2004.
(SHEKH FAISAL BIN ABD LATIP)

DEDICATION

"To my lovely parents, familys and all my freinds"

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my gratitude to KUTKM for giving me this well planned final project, especially my faculty supervisor, Mr. Shekh Faisal bin Abd Latip who has given information about PSM Project via email, telephone and personal visit, supportive, ideas, comments and suggestions have been invaluable.

My greatest appreciation towards Cosmopoint Seremban Centre Manager, Mr. Abdul Razak and IT Exec, Mr.Nuyussaini who have been very understandable provided me the actual working environment. Thanks also for their kindness and willingness to teach and guide me will be remembered. Last but not least, I would like to thank those who are not mention in here but have directly or indirectly helping and guiding me towards completing my final project their efforts and time are much appreciated.

Finally, to all my family members and friends that have given me moral support, a million thanks. Without all of them that I have mentioned, I would not be able to undergo my final project successfully and meaningfully. All the experiences and knowledge that I have gained are their efforts and time spent.

ABSTRACT

Generally, with the inclusion of new features in each successive generation of Windows, it was discovered that its security decrease. Therefore this research was carried out to overcome this problem which results with the development of Secure Windows Environment and Application Blocker (SWEAB). SWEAB is a Windows resources restriction security application. The goal of this project is to develop a security application for home users, IT colleges, universities or private companies by providing tighter security implementation for Windows XP operating system. SWEAB system was programmed to edit the Windows Registry to restrict user from accessing the Windows resources. The prototyping method is used in developing the project as it is an essential element of an iterative design approach, where designs are created, evaluated, and refined with the results of testing at each cycle feeding into the design focus of the next cycle. The waterfall model has been chosen as project methodology because its deliverables of every stage matches the project milestone requirement. The SWEAB project development is grouped into five major phases: Planning, Analysis, Design, Implementation and Design. The SWEAB system supports the following scopes: Program blocker to block Instant Messaging, restrict access Windows resources and provides folder protection. SWEAB system will increase the Windows XP security and provides easy usage. It is efficient to use as it "Windows Configurator", "Folder Guard" and chat blocker features.

ABSTRAK

Secara umumnya, dengan pernambahan fungsi baru dalam setiap generasi Windows yang berjaya, keselamatannya akan berkurang. Oleh itu, kajian ini dijalankan untuk mencari satu penyelesiaan bagi masalah tersebut. Maka, Sistem SWEAB telah dibangunkan untuk menyelesaikan masalah ini. Sistem SWEAB merupakan satu aplikasi bagi menyekat pencapaian sumber *Windows*. Tujuan projek ini adalah untuk membangunkan satu aplikasi selamat bagi pengguna di rumah, kolej, universiti atau organisasi persendirian untuk keselamatan bagi sistem pengoperasian *Windows XP*. Sistem SWEAB diprogramkan untuk mengedit *Windows Registry* untuk menyekatkan pencapaian sumber *Windows*. Kaedah prototaip digunakan dalam membangunkan projek ini dimana kaedah ini merupakan elemen asas dalam rekabentuk iteratif iaitu merekabentuk, menilai dan manapiskan keputusan setiap fasa pengujian ke dalam rekabentuk yang menfokuskan fasa berikutnya. Model air terjun dipilih sebagai methodologi projek kerana penyampaian setiap peringkatnya berpadanan dengan kehendak projek. Pembangunan projek SWEAB dikategorikan kepada 5 bahagian fasa yang utama iaitu perancangan, analisis, rekabentuk, perlaksanaan dan implikasi. Sistem SWEAB menyokong skop seperti berikut *"Program Blocker"* untuk menghalangkan *Instant Messseger*, menyekat pencapaian sumber *Windows* dan menyediakan perlindungan folder. Sistem ini akan meningkatkan keselamatan *Windows XP* dan memudahkan penggunaan. Ia adalah efisyen digunakan kerana ia merupakan kombinasi fungsi "*Window Configurator*", "*Folder Guard*" dan "*Chat Blocker*".

TABLES OF CONTENTS

LIST OF TABLE

LIST OF FIGURE

LIST OF TERMS AND ABBREVIATIONS

ABBREVIATIONS	DEFINITION
AIM	AOL Instant Messenger
API	Application Program Interface
AUT	Application Under Testing
BASIC	**B**eginners' **A**ll-purpose **S**ymbolic **I**nstruction **C**ode
CASE	Computer Aided Software Engineering
DoS	Denial of service
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
DWORD	A DWORD is similar to a binary value, except that it can't exceed 4 bytes in size. It is used to store large integer value
GUI	Graphical User Interface
ICQ	AOL Time Warner
ISS	Internet Security Systems
MD4, MD5	message digest
MSN	. NET Messager and Windows Messager
OOD	Object-oriented design
OS	Operating System
P2P	Peer-To-Peer
PC	Personal Computer
PERT	Program Evaluation Review Technique
PSM I	Bachelor Degree Project I
PSM II	Bachelor Degree Project II
SHA-1	Secure Hash Algorithm
SHS	Secure Hash Standard
WBS	Work Breakdown Structure
SWEAB	Secure Windows Environment And Application Blocker
WSH	Windows Script Host

LIST OF APPENDIX

CHAPTER I

INTRODUCTION

1.1. Preamble/Overview

In just a few years, the world has learned terms such as "virus", "worm" and "Trojan horse" and now appreciates concept such as "unauthorized access", "sabotage" and "denial of service". At the same time, the number of computer users has increased dramatically. Thus, it is unsurprising that threats to security in computing have increased along with its users and uses.

Security in computing addresses three very important aspects, confidentiality, integrity and availability. Confidentiality is the prevention of unauthorized disclosure of information. Integrity is the prevention of unauthorized modification of information (Pfleeger, 2003). In this context, modification includes writing, changing, changing status, deleting, and creating. Availability is the prevention of unauthorized withholding of information or resources.

"In 2001, Information Week Magazine commissioned global information survey of 4,500 security professionals. As part of the survey, the respondents were asked to name the primary methods of attack used by intruders against their organizations, which multiple responses were allowed. The top method was exploiting know operating system vulnerabilities; almost one-third of the respondents had experienced this kind of attack. The next most popular method was exploiting an unknown application (27%). Other commonly used attacks were guessing passwords (22%), abusing valid user accounts or permissions (17%), and using an internal denial of service (12%). Breaking through the defenses of operating systems gives access to the secrets of computing systems. Microsoft did not made Windows 95/98/Me a secure operating system. The only security tool included in Windows

98/95 is the System Policy Editor, which was very limited in use, confusing to set up and can be easily bypassed (Pfleeger, 2003)."

Therefore, the purpose of this project was to develop a new Windows secure application calls Secure Environment and Application Blocker (SWEAB) by using Microsoft Visual Basic 6.0 and Windows Scripting. SWEAB is a Windows resources restriction security application. It enables restricted access to several Control Panel applet functions, including Display, Network, Printer, and System. SWEAB provides the function in disabling Start Menu items, disable drives, disable the command prompt and hide task manager. It is also the administrator, which has the ability to prevent the opening of some Windows on the user's desktop. In addition, SWEAB also enables the folder protected feature.

Furthermore, this program is also a program blocker. It provides administrator to block Instant Messaging such as ICQ, MSN, and Yahoo! Messenger. SWEAB can be used by people at home, in schools, colleges, and university event offices as a System Administrator for security purpose.

1.1.1. Cosmopoint IT College – A Case Study

Cosmopoint Sdn Bhd is a leading Bumiputera IT company interoperated in October 1991 with an aim to build the Malaysian people towards becoming an information rich society. It hopes to achieve the goal by developing an IT literate nation that would embrace sophisticated technology at ease. Cosmopoint Institute of Information Technology Seremban Center was incepted in April 2001. Cosmopoint Seremban tries to keep its computer, hardware and software with tight security implementations and ease of use.

In the past few months, IT Executive had used the "Windows Configurator" to secure the Windows resources such as Control Panel applet function, disable network properties, disable start menu properties and desktop settings. As a result, he comments "I found that event this software protected by password but it can

retrieve the password by other third-party software. Have some student successful breaking into the network property and change the network settings." The one complain that recurred continuously from the lecturers. For example, the lecturers complained that "Can block the chatting program running in lab computers? Students always chat online in the lab and causes viruses and worms to attack the lab computers." Center Manager has discussed this suggestion with the IT Executive to search for freeware security application with features of "Windows Configurator", "Folder Guard" and "Chat Blocker".

1.1.2. Methodology

The Waterfall model has been chosen as the project methodology because its deliverables of each stage matches the milestone requirement. Multiple techniques such as fact-finding, modeling and prototyping were applied during project development. Waterfall model is an organized set of activities used in guiding the development of SWEAB system. The activities can be grouped into five major phases: Planning, Analysis, Design, Implementation and Maintenance.

1.2. Problem Statement

The following problems have been identified from Cosmopoint Seremban's lab:

i. The constant network setting change had led to the network secure problem. It had caused the college network to be easily attacked by hackers, viruses, and worms or spy ware.

ii. The students like to change the system settings, edit the registry and remove hardware and software from the Control Panel applet. This action can damage the system file and is able to cause the hard disk bad sector and missing Windows file.

iii. Students can change the wallpapers through the set up of wallpapers background by using the paint program-set as wallpaper.

iv. They do no have any chat blocker to block the students from chatting in the Yahoo! Messenger. Students can easily download the messenger and install it in the Lab PC through yahoo homepage. http://www.yahoo.com.

v. "Windows Configurator" network setting can be enabled by using third party software such as "Net Time Client.

vi. Hard to detect the insider hackers.

1.3. Project Goal

The goal of this project is to develop a secure application for home users, IT colleges, universities or private companies to provide tighter security implementation for Windows XP operating system.

1.4. Project Objective

This project develops a new window secure application to secure the Windows and block the chatting program in the user workstations. It is anticipated that the application will provide tighter security implementations and ease of use. It is anticipated that this project will result in one of the following:

i. Development of a Windows secure application for IT Colleges, Private Companies or Home Users to provide tighter security implementations for the system settings that only can be changed by the System administrator.

ii. To integrity the "Windows Configurator" secure feature, chat blocker and folder protections secure functions for release new Windows secure software in a highly competitive market.

iii. A solution to overcome the Windows XP security problem.

1.5. Project Scope

This project is supports the following scopes:

i. **Block program**

It enables user to block the chatting program such as MSN, ICQ, MIRC, Yahoo!Messenger, and AOL Instant Messenger.

ii. **Restrict access to several Control Panel Applet**

It offers the administrative support for controlling user's access the control panel applet functions, including the Display, Network, Passwords, Printer and System.

iii. **Folder Protection**

It enables user to lock the folder and protected by password. Searching folders/files and provides change the folders/files properties options.

iv. **Disable and hide the Windows resources**

It can disable the command prompt, disable the start menu items, disable the desktop settings, disable the networks settings, disable the system options and restrict access certain drives.

1.6. Significance of the Project

This project increases the Windows XP security and blockes the Instant Messaging. SWEAB provides with tighter security implementations and ease of use. It is more efficient to use as it integrity "Windows Configurator", "Folder Guard", and "Chat Blocker" features. SWEAB is more economical compared with other commercial softwares such as Chat Blocker and Firewall.

The following benefits could be realized if this project was developed:

i. The blocking of chatting program can avoid the employees or students from chatting. This can increase the quality and quantity of works. In additional, attacks by hackers, viruses, worms and spy wares can be avoided.

ii. Folder protection feature can disable the folders access by unauthorized users. Advanced folders/files search by certain criteria and folders/files properties change was provided.

iii. Restricts the Windows resources such as control panel applets and system file can avoid system files and Windows file damage. Furthermore, system administrator may easily maintains the security purpose.

iv. When command prompt is disabled, the hackers can be prevented from hacking the system and accessing the files in the user PC.

1.7. Expected Output

SWEAB is a solution to overcome the Windows XP security problems. The SWEAB system was programmed to edit the Windows Registry to restrict user from accessing the Windows resources. It has "Windows Configurator" feature which can restrict user from accessing the Windows resources such as control panel applet functions, system options, desktop settings, start menu items, networks settings, restriction explore certain drives in the Windows Explorer. Furthermore, folder protection functions is also provided by SWEAB and blocks the chatting program such as ICQ, MSN and Yahoo!Messenger. SWEAB system will be protected by password and the password data is encrypted.

1.8. Organization of Project Report

This report is organized into 8 chapters, followed by a resources section that contains bibliography and appendixes. Chapter 1 gives an overall introduction of the project. It describes the project's goal and organizations that play an important role in case studies, suggestion of problem solving, methodology that was used in the project, project objectives, project scope and project significance.

Chapter 2 presents literature reviews of the project that focused on security holes, Windows Registry, risk of Instant Messaging, Windows XP and SHA encryption algorithm. Furthermore, this chapter discussed the solution used in the researches and gives suggested approaches to solve the problem. Chapter 3 was discussed in detail on the project planning, project development and project methodology used in meeting project objectives, scope and requirements. Work breakdown structure, Gantt chart, PERT chart and milestone was used to monitor the project planning and schedule.

Next, Chapter 4 presented an analysis of the project. Business review, problem analysis and requirement analysis was discussed detail in this chapter. Chapter 5 was described in detail on initial system design and prototype of SWEAB system. This chapter described the system architecture, system design, specifies the input/output and user interface system. Chapter 6 discussed about the project implementation, include software development environment setup and implementation status. Chapter 7 described the project testing activity involved in testing phase. Chapter 8 is a brief conclusion of project PSM, such as observation on weaknesses and strengths and propositions for improvement.

Finally, the resources section at the end of the report contains a wealth of information such as screenshot of the "Windows Configurator" and "Terminator-X" , Gantt chart, PERT chart, work breakdown structure, use case diagram and sequence diagram of SWEAB system, detail design system, flow chart, module source code, system implementation status, test script, test data, test case result and bibliography.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

The purposes of literature review are to provide the background and justification for the undertaken research. The literature review provides examples, case studies and other relevant works that has been done in the past. The significance of the literature review is to allow the researcher to gain more information based on their subject area. It also provides the researcher with the objectives, problem statements, scopes and other information from the previous system. Theoretically, the researcher will produce a more efficient new system which fulfills the user requirements of the previous system. The researcher will also know the limitations of the previous system which helps the development of a new and more advance system.

This chapter is a review of studies and information related to the Win32 API, Windows XP Registry, SHA-1 algorithm and studies the current system "Windows Configurator" and "Terminator-X". The objective of this task is to synthesize available knowledge from existing literature and ongoing research. SWEAB is an idea gathered from the study of the existing literature reviews discussed in this chapter.

2.2 Fact and finding

An effective literature review informs the researcher not only of the particular conceptual area, but also of the appropriate strategies and methods for investigating