

TESIS^ APPROVAL STATUS FORM

JUDUL: DESIGN AND DEVELOPMENT OF AN IMPROVED PERSONAL FIREWALL SYSTEM

SESI PENGAJIAN: 2004

Saya TAN HAK MENG
(HURUF BESAR)

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)

 1 TIDAK TERHAD
 /

(TANDATANGAN PENULIS)

Alamat tetap : 91-1, JALAN SUNGAI GURUP,

82000 PONTIAN, JOHOR.

Tarikh : 20/10/2004

(TANDATANGAN PENYELIA)

PROF. MADYA DR. SHAHRIN BIN SAHIB
Timbalan Dekan (Akademik)
Fakulti Teknologi Maklumat dan Komunikasi
Kolej Universiti Teknikal Kebangsaan Malaysia
Nama Penyelia

Tarikh : 20/10/2004

CATATAN: ** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

^ Tesis dimaksudkan sebagai Laporan Projek Sarjana Muda (PSM)

raf

QA76 .9 .A25 .T36 2004



0000037884

Design and development of an improved personal firewall
system / Tan Hak Meng.

**DESIGN AND DEVELOPMENT OF AN IMPROVED
PERSONAL FIREWALL SYSTEM**

TAN HAK MENG

This report is submitted in partial fulfillment of the requirements for the
Bachelor of Information and Communication Technology (Computer Network)

FACULTY OF TECHNOLOGY AND COMMUNICATION TECHNOLOGY
KOLEJ UNIVERSITI TEKNIKAL KEBANGSAAN MALAYSIA

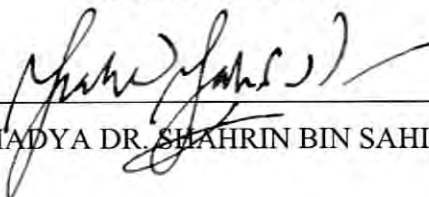
2004

ADMISSION

I admitted that this project title name of
**DESIGN AND DEVELOPMENT OF AN IMPROVED
PERSONAL FIREWALL SYSTEM**

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

STUDENT :  Date : 20/10/2004
(TAN HAK MENG)

SUPERVISOR :  Date : 20/10/2004
(PROFESSOR MADYA DR. SHAHRIN BIN SAHIB@SAHIBUDIN)

DEDICATION

I am as ever, especially indebted to my parents, Tan Boon Lee and Low Lee Sheng
for their love and support throughout my life...

ACKNOWLEDGEMENTS

I would like to show my highest gratitude and appreciation to my dearest supervisor, Professor Madya Dr. Shahrin Bin Sahib@Sahibudin who has guided me in undergoing through the Final Year Project. His constructive guidance, tireless assistance, advice and patience in helping me to complete the project are appreciated. He volunteers his valuable time to help me put my best foot forward. He is willing to share the invaluable and specific guidance, knowledge and skills with me. His kindly and friendly during every personal meeting really impressed me.

My second thanks go to all of the lecturers in KUTKM that gives their cooperation by providing me with the required needs. Without their cooperation, I would not be able to go through the phase smoothly.

I wish to express my appreciation to all my friends, especially Lau Kheh Pin, Yeow Chen Lee, Cheong Chow Sin, Lai Yen Wei and Lau Siew Chuan. They have guided me with the direction of the Final Year Project at the very beginning.

Finally, I also want to extend a special thanks to my parents, who give me the fully support and my friends who encouraged me when faced with obstacles.

Thank you for all your kind help and advice.

ABSTRACT

The Personal Firewall System (PFS) is a software application that is especially for the home users to protect their computer. There are a lot of personal firewalls can be found in the market. However, majority of the personal firewalls in the market are not able to protect the privacy violation efficiently. Therefore, the main purpose of the PFS is to provide a superior arsenal of defenses against PC infiltration by denying unauthorized access by remote hackers and protecting against data theft, denial-of-service attacks, and privacy violation. Basically, the PFS system can be divided into four main parts, which are detecting running application that has online connection, blocking inappropriate website, viewing log file and displaying Windows process. The purpose of research, particularly literature review is to collect data and weakness of the current system. Through the literature review, project's scope and user requirements has been retrieved and identified how big the project is. Waterfall Model has been chosen as a methodology for this project and implemented along the system development process to ensure the objectives of the project can be fulfilled. PFS system is developed by using Microsoft Visual Basic 6.0 on the Windows XP Professional operating system. Text file is used as database to keep log file. Therefore, PFS system can only be implemented within the environment of Windows XP and Microsoft Visual Basic 6.0. With the latest and powerful technology, the system is not only expected to be workable, but also highly efficient in terms of execution speed and response time. Since PFS system provides the features of privacy, controllability, high security and ease to use system, home users can be more rest assured while PFS system is used to protect their computers.

ABSTRAK

Personal Firewall System (PFS) ialah satu perisian aplikasi yang khas untuk mengawal keselamatan komputer bagi pengguna peribadi. Terdapat perbagai jenis *firewall* peribadi yang boleh didapati dalam pasaran. Namun demikian, kebanyakan *firewall* peribadi dalam pasaran tidak dapat menjamin keselamatan maklumat pengguna dengan berkesan. Oleh itu, tujuan utama PFS ialah menyediakan system perlindungan yang lebih baik untuk mengelakkan daripada berlakunya kecurian data, serangan dari segi keselamatan komputer dan pelanggaran hak individu. Pada asasnya, PFS dibahagikan kepada empat bahagian utama, iaitu mengesan aplikasi internet yang sedang dijalankan, menghalang laman web yang tidak bersesuaian, melihat *log file* dan memaparkan proses windows. Tujuan penyelidikan, terutamanya kajian literatur ialah mengumpul data dan kelemahan sistem pada ketika ini. Melalui kajian literatur, skop projek dan kehendak pengguna dipertimbangkan dan menentukan saiz projek. Model *Waterfall* telah dipilih sebagai metodologi projek dan pelaksanaan proses pembangunan sistem untuk memastikan objektif projek dipenuhi. Sistem PFS dibangunkan dengan menggunakan *Microsoft Visual Basic 6.0* dalam sistem pengoperasian *Windows XP Professional*. Fail teks digunakan sebagai pangkalan data untuk menyimpan *log file*. Oleh itu, sistem PFS hanya boleh dilaksanakan dalam persekitaran *Windows XP* dan *Microsoft Visual Basic 6.0*. Dengan teknologi yang terbaru dan berkuasa, sistem ini bukan sahaja boleh digunakan tetapi juga amat berkesan dalam kelajuan pelaksanaan dan masa tindak balas. Oleh kerana sistem PFS mempunyai ciri-ciri seperti persendirian, mudah dikawal, taraf keselamatan yang tinggi dan kesenangan menggunakan sistem, pengguna peribadi akan lebih selesa sekiranya sistem PFS digunakan untuk mengawal keselamatan computer mereka.

TABLE OF CONTENTS

CONTENT	PAGE
TESIS^ APPROVAL STATUS FORM	
DESIGN AND DEVELOPMENT OF AN IMPROVED PERSONAL FIREWALL SYSTEM	i
ADMISSION	ii
DEDICATION	iii
ACKNOWLEDGEMENTS	iv
ABSTRACT	v
ABSTRAK	vi
TABLE OF CONTENTS	vii
LIST OF TABLES	xii
LIST OF FIGURES	xiv
LIST OF ACRONYMS	xv
LIST OF APPENDICES	xviii
CHAPTER I INTRODUCTION	1
1.1 Overview	1
1.1.1 Project Description	1
1.2 Problem Statement	2
1.2.1 Suggestion to Problem Solving	3
1.3 Objective	4
1.4 Scopes	6
1.5 Contributions	7
1.6 Expected Output	9

CHAPTER II	LITERATURE REVIEW	10
2.1	Introduction	Error! Bookmark not d 10
2.2	Fact and Finding	11
2.2.1	The Reason to Choose PFS System as PSM Topic	12
2.2.2	Research on Concept and Technology	14
2.2.2.1	Theory of Personal Firewall	14
2.2.2.2	Architecture of Personal Firewall	16
2.2.2.3	Technology of Three Layer Architecture	17
2.2.2.4	Programming Language (Microsoft Visual Basic 6.0)	18
2.2.2.5	Database	18
2.2.3	Research to Similar System in Market	19
2.2.4	Research of Methodology	22
2.3	Conclusion	Error! Bookmark not d 23
CHAPTER III	PROJECT PLANNING AND METHODOLOGY	25
3.1	Introduction	Error! Bookmark not d 25
3.2	High-Level Project Requirements	26
3.2.1	Project Facilities Requirement	26
3.2.2	Software Requirement	27
3.2.3	Hardware Requirement	29
3.3	System Development Approach	30
3.3.1	Preliminary Planning Phase	32
3.3.2	Analysis and Requirements Phase	33
3.3.3	System Design Phase	34
3.3.4	Development and Implementation Phase	35
3.3.5	System Testing phase	36
3.3.6	Operation and Maintenance Phase	36
3.4	Project Schedule and Milestones	37
3.4.1	Work Breakdown Structure	37
3.4.2	Gantt Chart	40

3.5	Conclusion	42
CHAPTER IV ANALYSIS		43
4.1	Introduction	43
4.1.1	Information Gathering Approach	43
4.2	Analysis of Current System	44
4.2.1	Business Process	45
4.2.1.1	Sygate Secure Enterprise	45
4.2.1.2	Main Business	46
4.2.1.3	Company's Modules	46
4.2.2	Problem Analysis	49
4.2.3	Problem Statements	52
4.2.3.1	Identify Problems	52
4.3	Analysis of to be System	54
4.3.1	Functional Requirement	54
4.3.2	Technical Requirement	55
4.3.2.1	Software Requirement	55
4.3.2.2	Hardware Requirements	58
4.3.2.3	Implementation Requirements	58
CHAPTER V DESIGN		60
5.1	Introduction	60
5.2	Preliminary/High Level Design	61
5.2.1	Raw Data/Pilot Review	61
5.2.2	System Architecture	62
5.2.2.1	Detect Running Application Module	63
5.2.2.2	Block Inappropriate Websites Module	64
5.2.2.3	View Log File Module	64
5.2.2.4	Display Windows Process Module	64
5.2.3	User Interface Design	66
5.2.3.1	Navigation Design	66
5.2.3.2	Input Design	67
5.2.3.3	Output Design	67

5.2.4	Database Design	69
5.3	Detailed Design	69
5.3.1	Software Specification	69
5.3.1.1	Sequence Diagram	72
5.3.1.2	Collaboration Diagram	74
5.3.1.3	Activity Diagram	74
5.3.1.4	Class Diagram	75
5.3.1.5	Pseudocode	75
5.3.2	Physical Database Design	75
5.4	Summary	76
CHAPTER VI IMPLEMENTATION		78
6.1	Introduction	78
6.2	Software Development Environment Setup	79
6.2.1	Programming language	80
6.2.2	Development Environment	81
6.2.3	Operating System	81
6.2.4	Database	81
6.3	Software Configuration Management (Optional)	82
6.3.1	Configuration Environment Setup	82
6.3.1.1	Installation of Microsoft Visual Studio 6.0	82
6.3.1.2	Installation of Personal Firewall System	82
6.3.2	Version Control Procedure	83
6.4	Implementation Status	83
6.5	Summary	85
CHAPTER VII TESTING		87
7.1	Introduction	87
7.2	Test Plan	88
7.2.1	Test Environment	88
7.2.2	Test Schedule	89
7.3	Test Strategy	89
7.4	Test Design	91

7.4.1	Test Description	91
7.4.2	Test Data	96
7.5	Test Case Results	98
7.6	Summary	99
CHAPTER VIII PROJECT CONCLUSION		101
8.1	Observation on Weaknesses and Strengths	101
8.2	Propositions for Improvement	102
8.3	Conclusion	Error! Bookmark not d 103
BIBLIOGRAPHY		105
APPENDICES		107

LIST OF TABLES

TABLE NO	TITLE	PAGE
Table 2.1:	Comparison Personal Firewall	21
Table 2.2:	Comparison between Waterfall Model and Spiral Model	23
Table 3.1:	Project Facilities Requirement	26
Table 3.2:	Software Requirement	27
Table 3.3:	Hardware Requirement	29
Table 4.1:	Feature Analysis 1	50
Table 4.2:	Feature Analysis 2	51
Table 4.3:	Usability Analysis	52
Table 4.4:	Software Requirement	56
Table 4.5:	Hardware Requirement	58
Table 5.1:	Sample Raw Data	61
Table 5.2:	Input Design	67
Table 5.3:	Output Design	68
Table 5.4:	Actor Description	70
Table 5.5:	Use Case Description	71
Table 5.6:	Data Dictionary for password.txt, traffic.txt and security.txt	76
Table 6.1:	The Implementation Status of PFS System for Each Function	83
Table 6.2:	The Implementation Status of PFS System for Each Module	84
Table 7.1:	Test Schedule for PFS System	89
Table 7.2:	Test Description for User Login	91
Table 7.3:	Test Description for Change Password	92

Table 7.4: Test Description for Detect Running Application	93
Table 7.5: Test Description for Block Inappropriate Website	94
Table 7.6: Test Description for View Log File	94
Table 7.7: Test Description for Display Windows Process	95
Table 7.8: Test Description for System Integration Testing	96
Table 7.9: User Login Test Data	97
Table 7.10: Change Password Test Data	97
Table 7.11: Block Inappropriate Website Test Data	98
Table 7.12: Test Case Results for PFS System	99

LIST OF FIGURES

FIGURE NO	TITLE	PAGE
Figure 2.1:	Increasing of Home User in using Personal Firewall	13
Figure 2.2:	Cyber Attacks by Hacker on Home User	14
Figure 2.3:	Architecture of Two Way Filter	17
Figure 2.4:	Sygate Personal Firewall Pro 5.5	19
Figure 2.5:	ZoneAlarm Pro	20
Figure 3.1:	Waterfall Model	31
Figure 3.2:	Architecture Two Way Filter of PFS	35
Figure 3.3:	Work Breakdown Structure	38
Figure 3.4:	Gantt Chart	41
Figure 5.1:	Three Layer Architecture	62
Figure 5.2:	PFS System Architecture	65
Figure 5.3:	Navigation Design for PFS System	66
Figure 5.4:	Actor and Use Cases Notation	70
Figure 5.5:	System Distributed Diagram for PFS System	72
Figure 6.1:	The Software Development Environment Setup Architecture	79

LIST OF ACROYMNS

ACROYMN	DESCRIPTION
[A]	
AUT	Application Under Testing
[B]	
BASIC	Beginners' All-purpose Symbolic Instruction Code
[D]	
DOS	Denial Of Service
DSL	Digital Subscriber Line
DSN	Data Source Name
[E]	
EGA	Enhanced Graphic Adapter
ERD	Entity Relationship Diagram
EXE	Execute
[F]	
FTMK	Fakulti Teknologi Maklumat dan Komunikasi
FTP	File Transfer Protocol

	[G]	
GUI		Graphic User Interface
	[I]	
IDE		Integrated Development Environment
IP		Internet Protocol
	[K]	
KUTKM		Kolej Universiti Teknikal Kebangsaan Malaysia
	[L]	
LAN		Local Area Network
	[M]	
ME		Millenniums
	[N]	
NIC		Network Interface Card
NT		New Technology
	[P]	
PC		Personal Computer
PFS		Personal Firewall System
PSM I		Projek Sarjana Muda Satu
PSM II		Projek Sarjana Muda Dua

[R]

RAD	Rapid Application Development Model
RAM	Random Access Memory
RAS	Random Access Storage
ROBO	Branch-Office

[S]

SDLC	System Development Life Cycle
SMTP	Simple Message Transfer Protocol
SOHO	Home-Office
SQL	Structured Query Language

[U]

UML	Unified Modeling Language
URL	Uniform Resource Locator
UTP	Unshielded Twisted-Pair

[V]

VGA	Video Graphic Adapter
VPN	Virtual Private Network

[W]

WBS	Work Breakdown Structure
-----	--------------------------

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
APPENDIX 1:	Three Layer Architecture	108
APPENDIX 2:	Waterfall Model	109
APPENDIX 3:	Spiral Model	110
APPENDIX 4:	Gantt Chart	111
APPENDIX 5:	Personal Firewall System Questionnaires	112
APPENDIX 6:	User Interface Design	114
APPENDIX 7:	Use Case Diagram	119
APPENDIX 8:	Sequence Diagram For Detect Running Application Module	120
APPENDIX 9:	Alternate Flow Sequence Diagram for Detect Running Application Module	121
APPENDIX 10:	Sequence Diagram for Block Inappropriate Website Module	122
APPENDIX 11:	Alternate Flow Sequence Diagram for Block Inappropriate Website Module	123
APPENDIX 12:	Sequence Diagram for View Log File Module	124
APPENDIX 13:	Alternate Flow Sequence Diagram for View Log File Module	125
APPENDIX 14:	Sequence Diagram for Display Windows Process Module	126
APPENDIX 15:	Alternate Flow Sequence Diagram for Display Windows Process Module – Exit	127
APPENDIX 16:	Collaboration Diagram For Detect Running Application Module	128
APPENDIX 17:	Collaboration Diagram for Block Inappropriate Website Module	129

APPENDIX 18: Collaboration Diagram for View Log File Module	130
APPENDIX 19: Collaboration Diagram for Display Windows Process Module	131
APPENDIX 20: Activity Diagram for Detect Running Application Module	132
APPENDIX 21: Activity Diagram for Block Inappropriate Website Module	133
APPENDIX 22: Activity Diagram for View Log File Module	134
APPENDIX 23: Activity Diagram for Display Windows Process Module	135
APPENDIX 24: Class Diagram For Detect Running Application Module	136
APPENDIX 25: Class Activity Diagram for Block Inappropriate Website Module	137
APPENDIX 26: Class Diagram for View Log File Module	138
APPENDIX 27: Class Diagram for Display Windows Process Module -	139
APPENDIX 28: Pseudocode	140
APPENDIX 29: Installation of Personal Firewall System	141
APPENDIX 30: User Manual	145

CHAPTER I

INTRODUCTION

1.1 Overview

The PSM II is provided for KUTKM students to apply their knowledge and skills in order to develop an individual project. The objective of the PSM II is to train the student adapts to face and overcome internal and external challenges and problems in the constantly changing environment as well as striving to positively compete in carrying out the assigned project within the specified time frame and use time wisely.

1.1.1 Project Description

“A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks” (Johnsor, 1987). Personal firewall also called desktop firewalls, are used to protect individual personal computers from malicious hackers and programs. They are able to stop network scanning and attack programs from accessing resources on the individual PC. Since they are monitoring all of the traffic passing to and from the computers network interface they are able to stop local programs from accessing external resources.

The final project that has been suggested to undergo is entitled Personal Firewall System (PFS). This system is an application that developed by using Microsoft Visual Basic 6.0 programming language to provides a superior arsenal of defences against PC infiltration by denying unauthorized access by remote hackers and protecting against data theft, denial-of-service attacks, and privacy violation. A personal firewall is the most important first line of defences for computer security. It creates a protective barrier between individual computer and potentially harmful content on the Internet. The PFS system is developed especially for the home user to protect their computer security. It is designed for the home user with Windows XP Professional Edition platform. The user can change the PFS system status according to their needs and requirement from time to time.

The system that will be developed has four specific functions/modules which are:

- a) Detect running application that connects to the Internet.
- b) Block inappropriate website to avoid the children from exploring to the illegal website.
- c) Display the security and traffic log file
- d) Display all the Windows process.

1.2 Problem Statements

Analyst the identified problems is collection of information about all the current personal firewall in the market. After analysis the current system, the main problem statement for the current personal firewall in the market is identified such as below:

1. Not User Friendly

Some of the current system does not clearly elaborate the function of the firewall. Home users are not able to control and use the function efficiently. Some open source firewall like Iptables in Linux does not provide GUI for the users while installation and configuration. Users will face difficulties while command and rule sets are needed for installation and configuration.

2. Low Security

Some of the personal firewalls are not able to detect and block the intrusions by hackers. Some of them do not provide the Packet Filtering function. They only provide the simple security level like "low", "medium" and "high". These functions are not able protecting the PC effectively.

3. Lack of Controllability

Most of the current system cannot protect children from exploring illegal or inappropriate websites. Some of personal firewall cannot block the unnecessary application in the PC effectively.

4. Lack of the Basic Feature

Some of the personal firewall like ZoneAlarm does not provide basic features such as log file and website blocking function. A complete system should include the features of security, privacy, controllability and ease to use features.

1.2.1 Suggestion to Problem Solving

Due to a lot of the weakness of current personal firewall system in the market, the PFS system will be built up to protect users' individual PC. The well-defined requirements of the personal firewall will be strongly focused to meet the user's satisfactions. The skills of defining system requirements, effective methods

for gathering information and good programming language in Microsoft Visual Basic 6.0 in developing the PFS system is needed.

Due to a lot of the skills are needed while developing the PFS system, the Fact-Finding method will be used. Fact-Finding is a classical set of techniques used to collect information about the system problems, opportunities, solution requirements, and priorities. Therefore, the techniques of the fact-finding in observation of the current system, research to of relevant literature, research/site visits and sampling of existing documentation or related source code is utilized.

The research and site visits technique is to thoroughly research the problem domain. Computer trade journals and reference books are a good source of information. It can provide a lot of information on how to solve the similar problem. Immeasurable amounts of information can be obtained by exploring the Internet.

Methodology that will be used to develop this project is Waterfall Model. There are many phases and steps that are suitable as a guideline and adapted to establish the PSM II.

Besides that, the advice and opinion from the supervisor, Professor Shahrin is valuable and important in completing this project.

1.3 Objective

The objectives of the PFS system are as below:

- To provide privacy to the home users