BORANG PENGESAHAN STATUS TESIS^

JUDUL : THE COMPARISON BETWEEN SECURE SHELL (SSH) AND TELNET USING NETWORK ANALYZERS

SESI PENGAJIAN : 2006 / 2007

Saya NUNI NATASSA BINTI MOHD SANI
(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 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)

(TANDATANGAN PENYELIA)

Alamat tetap : KAMPUNG IPOH,
17500 TANAH MERAH, KELANTAN.

Tarikh : 21.11.2006

ENCIK OTHMAN BIN MOHD
Nama Penyelia

Tarikh 21.11.2006

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

THE COMPARISON BETWEEN SECURE SHELL (SSH) AND TELNET USING NETWORK ANALYZERS

NUNI NATASSA BINTI MOHD SANI

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

FACULTY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY
KOLEJ UNIVERSITI TEKNIKAL KEBANGSAAN MALAYSIA
2006

DECLARATION

I hereby declare that this project report entitled

THE COMPARISON BETWEEN SECURE SHELL (SSH) AND TELNET USING NETWORK ANALYZERS

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

STUDENT : _____ Date : 21.11.2006

(NUNI NATASSA BINTI MOHD SANI)

SUPERVISOR : _____ Date : 21.11.2006

(ENCIK OTHMAN BIN MOHD)

DEDICATION

Specially dedicated to
My beloved father, Mohd Sani bin Daud, and mother, Zainun binti Mahmood
and also to my dearest family, friends and colleagues
who have always being there to encourage and inspire me throughout my life.

ACKNOWLEDGEMENTS

In the name of Allah s.w.t the Almighty and most Merciful

In this opportunity, I would like to express my highest gratitude to my supervisor, Encik Othman bin Mohd for his guidance and considerate for all the time being that leads me to finally finish doing this Projek Sarjana Muda (PSM). I also like to express my deepest gratitude to Puan Wahidah binti Md. Shah, Encik Nazrul Azhar bin Bahaman and Encik Zulkiflee bin Muslim for their advices and also for the time as they had given me so much information and guidance during this semester. Not to forget, I also want to say thanks to all PSM committee member that have worked hard in order to enable us, the final year student of FTMK to get through this semester without having any problem. Last but not least, I would say thank you to my fellow friends who have been helping me and giving tips on how I can work through this semester task and for supporting me in all time.

ABSTRACT

The project "The Comparison Between Secure Shell (SSH) and Telnet Using Network Analyzers" is a research on differentiate two types of data transmission approaches over the computer network using three different network analyzers. In this project, the network analyzers that are being used are Wireshark, Colasoft Capsa and Commview. In order to give the guideline on differentiating the two approaches, basic knowledge about the meanings and concepts for Secure Shell (SSH) and Telnet is crucial. First, it is important to get know Telnet as SSH is an improvement of the existing Telnet. Telnet is a network protocol used on the Internet or local area network (LAN) connections. The Telnet typically used to provide user oriented command line login sessions between hosts on the Internet. Meanwhile SSH is an advanced protocol providing secure encrypted remote communications over an unsecured channel, such as the Internet. A hostile user has control over the network can only force SSH session to disconnect, but cannot decrypt or play back the traffic, or hijack the connection. SSH has takes the place of Telnet, which is insecure, and uses encryption to protect both the exchange of username and password as well as all data that is passed between the remote client and the network server. The SSH works in a similar manner to Telnet, and many of the interfaces that have been developed look just like the Telnet clients that users have become accustomed to.

ABSTRAK

Tajuk projek "The Comparison Between Secure Shell (SSH) and Telnet Using Network Analyzers" adalah satu kajian kes mengenai perbezaan di antara dua jenis pendekatan penghantaran data dalam rangkaian komputer dengan menggunakan tiga jenis penganalisa rangkaian yang berlainan. Dalam projek ini, penganalisa rangkaian yang digunakan adalah Wireshark, Colasoft Capsa dan Commview. Bagi memberikan garis panduan dalam membezakan di antara kedua-dua pendekatan, pengetahuan asas mengenai maksud dan konsep bagi Secure Shell (SSH) dan Telnet amat penting. Pertama sekali, amat penting mengenali Telnet kerana SSH merupakan penambahbaikan daripada Telnet. Telnet adalah protocol rangkaian yang digunakan di rangkaian Internet dan rangkaian setempat (LAN). Telnet biasanya digunakan untuk menyediakan pengguna yang menggunakan baris-baris arahan dalam mencapai sesi kemasukan di antara hos-hos di rangakaiana Internet. Manakala SSH adalah protocol yang lebih maju dimana ia menyediakan komunikasi mudah-alih yang dienkripsikan dengan selama di dalam saluran yang tidak selamat seperti Internet. Seseorang pengguna yang mengawal sesebuah rangkaian hanya dapat sesi SSH ditamatkan tetapi tidak berupaya memecahkan enkripsi atau memainkan semula proses yang telah dilaksanakan atau merampas hubungan yang telah berlaku. SSH telah mengambil-alih tempat Telnet yang didapati tidak selamat kerana SSH menggunakan enkripsi untuk melindungi pertukaran kata nama serta kata laluan dan juga melindungi semua data yang yang melalui klien mudah-alih dan server rangkaian. SSH berfungsi sepertimana Telnet dengan antara muka yang telah dibangunkan menyerupai klien-klien Telnet yang biasa digunakan oleh para pengguna.

TABLE OF CONTENTS

CHAPTER	SUBJECT		PAGE
	DECLARATION		i
	DEDICATION		ii
	ACKNOWLEDGEMENTS		iii
	ABSTRACT		iv
	ABSTRAK		v
	TABLE OF CONTENTS		vi
	LIST OF TABLES		xii
	LIST OF FIGURES		xiv
	LIST OF ABBREVIATIONS		xv
	LIST OF ATTACHMENTS		xviii
CHAPTER I	INTRODUCTION		
	1.1	Project Background	1
	1.2	Problem Statements	2
	1.3	Objectives	3
	1.4	Scopes	4
	1.5	Project Significance	5
	1.6	Expected Output	5
	1.7	Conclusion	6
CHAPTER II	LITERATURE REVIEW AND PROJECT METHODOLOGY		

2.1	Introduction	7
2.2	Fact and Finding	8
	2.2.1 Protocol	8
	2.2.2 SSH	9
	2.2.3 The SSH Protocol	10
	2.2.4 History of SSH	11
	2.2.5 Components of SSH	12
	2.2.6 How Secure Shell Works	15
	2.2.7 Secure Shell in OSI Model	19
	2.2.8 SSH Protocol Version 1	20
	2.2.9 SSH Protocol Version 2	21
	2.2.10 The Differences Between SSH1 and SSH2	22
	2.2.11 Telnet	22
	2.2.12 History of Telnet	24
	2.2.13 Telnet History Methodology	26
	2.2.14 Fundamental Telnet Concepts	26
	2.2.15 The 7 Layers of the OSI Model for Telnet	28
	2.2.16 Telnet Applications	30
	2.2.17 Telnet's Legacy	31
	2.2.18 Host Key	32
	2.2.19 Private Key	32
	2.2.20 Public Key	32
	2.2.21 Public Key Infrastructure (PKI)	33
	2.2.22 How Public and Private Key Cryptography Works	34
	2.2.23 Public Key Algorithms	35
	2.2.24 Secret Key Algorithms	36
	2.2.25 Hash Functions	39

2.2.26 Compression Algorithms 40
2.2.27 Authentication 40
2.2.28 Encryption 42
2.2.29 Integrity 42
2.2.30 Tunneling (Forwarding) 43
2.2.31 Problems In Current Data Transmission 44
2.3 Project Methodology 46
2.3.1 Waterfall Model Methodology 46
2.3.2 Chosen Methodology Justification 49
2.4 Project Requirements 50
2.4.1 Software Requirements 50
2.4.2 Hardware Requirements 51
2.4.2.1 Server Computer Hardware Requirement 51
2.4.2.2 Client Computer Hardware Requirement 52
2.4.3 Other Requirements 52
2.5 Project Schedule and Milestones 53
2.6 Conclusion 54

CHAPTER III ANALYSIS
3.1 Introduction 55
3.2 Business View 56
3.2.1 Business Review From Cisco Authentication, Authorization and Accounting (Cisco AAA) Mechanisms 56
3.2.1.1 Cisco AAA Overview 56

3.2.1.2 Remote Administration:
Telnet versus Secure Shell 58
3.2.2 Business Review On SSH And
Telnet Algorithms 59
3.2.2.1 Secure Shell (SSH) and
Telnet Encryption
Algorithms 60
3.2.2.2 Secure Shell (SSH) and
Telnet Authentication
Algorithms 60
3.3 Problem Analysis 61
3.4 Requirement Analysis 62
3.4.1 Software Requirements 62
3.4.2 Hardware Requirements 64
3.4.3 Network Requirements 65
3.5 Conclusion 66

DESIGN
4.1 Introduction 67
4.2 Raw Input/ Data 68
4.3 Network Architecture 69
4.4 Flow Model 70
4.5 Logical Design 72
4.6 Physical Design 73
4.7 Security Requirements 74
4.8 Conclusion 75

IMPLEMENTATION
5.1 Introduction 76
5.2 Software Development Environment

		Setup	77
	5.3	Software Configuration Management	79
		5.3.1 Configuration Environment Setup	79
		5.3.2 Version Control Procedure	81
	5.4	Hardware Configuration Management	82
		5.4.1 Hardware Setup	82
	5.5	Security	83
		5.5.1 Security Policies and Plan	83
	5.6	Implementation For Server-side and Client-side Software	84
		5.6.1 Software Implementation For Server-side	84
		5.6.2 Software Implementation For Client-side	84
	5.7	Development Status	85
	5.8	Conclusion	85
CHAPTER VI	TESTING		
	6.1	Introduction	87
	6.2	Test Plan	88
		6.2.1 Test Organization	88
		6.2.2 Test Environment	89
		6.2.3 Test Schedule	91
	6.3	Test Strategy	95
		6.3.1 Classes of Tests	95
	6.4	Test Design	96
		6.4.1 Test Description	96
		6.4.2 Test Data	104

	6.5	Test Results and Analysis	105
		6.5.1 Test Summary	105
		6.5.1.1 Test Summary Report For System Testing	105
		6.5.1.2 Test Summary Report For Network Analyzers Test Result	107
	6.6	Conclusion	112
CHAPTER VII	PROJECT CONCLUSION		
	7.1	Observation On Weaknesses and Strengths	114
		7.1.1 Strengths	114
		7.1.2 Weaknesses	115
	7.2	Proposition For Improvement	116
	7.3	Conclusion	117
	REFERENCES		119
	BIBLIOGRAPHY		120
	ATTACHMENTS		121

LIST OF TABLES

TABLE	TITLE	PAGE
2.1	Table Shows 7 Layers of the OSI Model for Telnet	29
2.2	Table of Public and Private Key Cryptography Works	35
2.3	Software Requirement	50
2.4	Hardware Requirement (Server)	51
2.5	Hardware Requirement (Client)	52
2.6	Other Requirements	53
3.1	Table of Encryption Ciphers For SSH (SSH1 and SSH2) and Telnet	60
3.2	Table of Authentication Cipher For SSH (SSH1 and SSH2) and Telnet	61
3.3	Software Requirements	63
3.4	Server Application Computer	64
3.5	Client Application Computer	64
3.6	Other Hardware Device	65
5.1	Server-side Configuration Environment Setup	80
5.2	Client-side Configuration Environment Setup	80
5.3	Server Application Version 1.0	81
5.4	Client Application Version 1.0	81
5.5	Hardware Setup Minimum Requirement	82
5.6	Network Setup Function	83
5.7	Development Status of Module	85

6.1	Server-side Testing Environment Setup	90
6.2	Client-side Testing Environment Setup	90
6.3	Test Schedule for Functional Process	91
6.4	System Testing Schedule (Server and Client)	91
6.5	System Testing Schedule (Network Analyzer In LAN)	93
6.6	Description For All Module/ Functional Process	96
6.7	Test Description for Server and Client Applications	97
6.8	Test Description for Network Analyzers	99
6.9	Server and Client Applications System Testing	101
6.10	Network Analyzers System Testing	102
6.11	User Input (Correct Input Data)	103
6.12	User Input (Wrong Input Data)	103
6.13	Test Input Data	104
6.14	Test Summary Report For System Testing	105
6.15	The Comparison Between Secure Shell (SSH) and Telnet Using Network Analyzers	111

LIST OF FIGURES

FIGURE	TITLE	PAGE
2.1	SSH Architecture	10
2.2	Unencrypted Telnet Session	23
2.3	Encrypted SSH Session	24
2.4	The 7 Layers of the OSI Model	28
2.5	Man-in-the-Middle Attack	45
2.6	Waterfall Model	47
3.1	An AAA ISP Implementation Example	57
3.2	Network Environment	66
4.1	Basic Network Architecture	69
4.2	SSH Connection Flow Model	71
4.3	Telnet Connection Flow Model	72
4.4	Logical Design	73
4.5	Physical Design	74
5.1	Software Development Environment Setup (1)	77
5.2	Software Development Environment Setup (2)	78
5.3	Software Development Environment Setup (3)	78
5.4	Configuration Environment Setup	79

LIST OF ABBREVIATIONS

ABBREVIATIONS		FULL TERMS
3DES	-	Tripal DES
A1	-	Authetication
A2	-	Authorization
AAA	-	Authentication, Authorization, Accounting
ACK	-	Acknowledge flag
AES	-	Advanced Encryption Standard
AIX	-	Advanced Interactive Executive (BM's version of Unix)
ARP	-	Address Resolution Protocol
ATM	-	Asynchronous Transfer Mode
BSD	-	Berkeley Software Distribution
CA	-	Certification Authority
CRC-32	-	Cyclic Redundancy Check
DES	-	Data Encryption Standard
DSA	-	Digital Signature Algorithm
FTP	-	File Transfer Protocol
GB	-	Gigabyte
HTTP	-	Hypertext Transfer Protocol
ICMP	-	Internet Control Message Protocol
ID	-	Identification Data
IDEA	-	International Data Encryption Algorithm
IETF	-	International Engineering Task Force
IP	-	Internet Protocol

ISDN	-	**Integrated Service Digital Network**
ISO/ OSI	-	**Interconnection System Operation/ Open System Interconnection**
ISP	-	**Internet Service Provider**
KUTKM	-	**Kolej Universiti Teknikal Kebangsaan Malaysia**
LAN	-	**Local Area Network**
Len	-	**Length**
LLC	-	**Logical Link Control**
MAC	-	**Media Access Control**
MB	-	**Megabyte**
MD5	-	**Message Digest Algorithm Number 5**
NVT	-	**Network Virtual Terminal**
PC	-	**Personal Computer**
PKI	-	**Private Key Infrastructure**
POP3	-	**Post Office Protocol 3**
PSH	-	**Push flag**
RA	-	**Registration Authority**
RACE	-	**Research and Development in Advanced Communication Technology in Europe**
RAM	-	**Random Access Memory**
RIPE	-	**RACE Integrity Primitive Evaluation**
RIPEMD-160	-	**The RIPE Message Digest (160 bits)**
RSA	-	**Rivest, Shamir and Adleman Algorithm**
SCS	-	**SSH Communication Security**
SHA-1	-	**Secure Hash Algorithm**
SMTP	-	**Simple Mail Transfer Protocol**
SSH	-	**Secure Shell**
SSH-1	-	**Secure Shell Version 1**
SSH-2	-	**Secure Shell Version 2**
TCP	-	**Transmission Control Protocol**

TCP/ IP	-	**Transmission Control Protocol/ Internet Protocol**
UTP	-	**Unshielded Twisted Pair**
WBS	-	**Work Breakdown Structure**

LIST OF ATTACHMENTS

ATTACHMENT	TITLE	PAGE
A	Project Activities Schedule Of PSM	121
B	Gantt Chart	124
C	Steps For Implementing Project Software and Protocol Analysis	127
D	Results and Analysis From Network Analyzers	141

CHAPTER I

INTRODUCTION

1.1 Project Background

Nowadays, many people have multiple computer accounts. There are many ways a user can obtain multiple accounts. For a reasonable savvy user, the user might have a personal account with Internet service provider (ISP), a work account on the employer's local network and a few computers at home. The user might also have permission to use other accounts owned by family members or friends.

If a user has multiple accounts, it is natural to want to make connections between the accounts. For example, the user might want to copy files between computers over the network, log into one account remotely from another or transmit commands to a remote computer for execution. Various programs exist for these purposes such as ftp for file transfer, rsh for remote execution of commands and telnet for remote login.

However, many of the network-related programs have a fundamental problem as the lack the security. If a sensitive file is transmitted via the Internet or the

network, an intruder can potentially intercept and read the data.

Therefore, the "The Comparison Between Secure Shell (SSH) and Telnet Using Network Analyzers" is a research to understand the concept of two types of data transmission that have been used over the network using three different network analyzers. The two approaches that will be studied in this project are Secure Shell (SSH) and Telnet. The project will cover in what way both of the SSH and Telnet have the similarity and the differences.

SSH is a protocol that is a specification of how to conduct secure communications over a network. Meanwhile, Telnet refers to a basic network utility and related protocol that allows a user to interact with a remote host using a text-based virtual terminal. First of all, it is best to acknowledge that SSH works in a similar way to Telnet and many the interfaces that have been developed look just like the Telnet clients that user have become accustomed to. However, Telnet is inherently insecure as when a Telnet connection being initiated, the user's username, password and other bits of important information is visible for anyone located between the user's computer and the intended server destination are broadcast in cleartext. SSH in other hand, covers the authentication, encryption, and the integrity of data transmitted over the network.

1.2 Problem Statements

Security is a most important issue when it comes to web servers and workstations. Therefore, it is an important issue when the user wants to keep up on the latest patches to cure the systems of viruses, "security holes" and software exploits.

One of the most popular ways of working on the network is Telnet. Telnet allows a user to open session on a remote server and work in the file system as the user is sitting in front of a machine. The concept brings security to mind instantly. What if someone were able to get the user's password? The intruder could easily gain access to the actual machine from anywhere! There is a more secure solution available. It requires little more configurations to set up, but it provides a far more secure environment and connection to the remote server.

Secure Shell (SSH) is what the network needed. SSH will allow the user the same benefits of Telnet without the plain text, "open" connection across the Internet. What's more, the user can configure SSH to use an encrypted pass-phrase instead of a plain text password to authenticate the users. This means the likelihood of someone gaining access to the machine is minimal. As a further security measure the user should restrict the SSH connections to specific IP addresses as this will cause anyone outside the set of permitted IPs to be denied access via SSH even if they have the user's pass-phrase.

1.3 Objective

This is a case study to explain about the concepts of SSH and Telnet and to further the knowledge about how that the two approaches the user thought identical actually are different in their own ways. The objectives of "The Comparison Between Secure Shell (SSH) and Telnet Using Network Analyzers" are as below:

a) To learn the meanings and concepts of SSH and Telnet and how the two approaches are different in the way they functions.

b) To recognize the similarity between SSH and Telnet and the differences that both of the approaches have.

c) To evaluate and compare SSH and Telnet and summarize which one is better than another.

d) Using three different network analyzers to identify the capabilities of SSH and Telnet.

1.4 Scopes

The main tasks for this project are to compare the meaning, concept, function and feature for both of SSH and Telnet. Thus, a basic and small setting is needed in order to accomplish the tasks.

In the project of "The Comparison Between Secure Shell (SSH) and Telnet Using Network Analyzers", the scope is for educational purpose only where the user can know how SSH and Telnet works, the similarity and differences between both of SSH and Telnet and finally figure out which one is better than another.

It is a common knowledge that SSH and Telnet can be implemented on platforms such as UNIX, Microsoft Windows and Macintosh. Therefore, the flexibility usage of SSH and Telnet is widely spread out in the data transmission over the network.

In defining and explaining the concept of SSH and Telnet as the data transmission approach, it definitely not a statement to say that either one or both of SSH and Telnet is a complete security solution as SSH and Telnet have their own advantage and disadvantages.