

BORANG PENGESAHAN STATUS TESIS*

JUDUL: ANALYSIS ON TELNET AND SSH

SESI PENGAJIAN: 2007

Saya TAMIL CHELVI A/P VADIVELU
(HURUF BESAR)

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

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
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 pengajiab 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

Tamilchelvi
(TANDATANGAN PENULIS)

Alamat tetap: LOT 3248 BATU 4,
JALAN KAPAR, 42100 KLANG,
SELANGOR DARUL EHSAN

Tarikh: 1/11/2007

M. Wahidah
(TANDATANGAN PENYELIA)

PN.WAHIDAH MD SHAH
Nama Penyelia

Tarikh: 1/11/2007

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

ANALYSIS ON TELNET AND SSH

TAMIL CHELVI A/P VADIVELU

**This report is submitted in partial fulfillment of the requirements for the
Bachelor of Computer Science (Computer Networking)**

**FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2007**

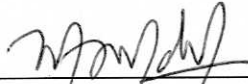
DECLARATION

I hereby declare that this project report entitled

ANALYSIS ON TELNET AND SSH

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

STUDENT :  Date: 1/11/2007
(TAMIL CHELVI A/P VADIVELU)

SUPERVISOR:  Date: 1/11/2007
(PN.WAHIDAH MD SHAH)

DEDICATION

A special dedication to my parents who have always inspired me in everything I do. They have taught me that determination and hard work is the key to success. Thank you so much....

ACKNOWLEDGEMENTS

I would like to express my gratitude to all those who gave me the possibility to complete my Final Year Project and prepare a final report of analysis. First of all, I would like to all the lecturers and friends for their valuable supports towards me and great helps during difficulty times.

I am deeply indebted to my supervisor Pn.Wahidah Md Shah whose help, stimulating suggestions and encouragement helped me in all the time of project and writing of this report. She showed me different ways to approach a problem and the need to be persistent to accomplish any goal. She also gave insightful and beneficial comments and reviewed my work. Her guidance gave me a high confidence in completing this report.

Thanks also to my evaluator, En.Zulkiflee for all his guidance and advice about my project and also for always being there to meet and talk about my ideas and confusion, to proofread and mark up my knowledge and to guide me with all the tasks.

Last but not least, one of the greatest pleasures is acknowledging the efforts of many people whose names may not appear on the cover, but whose sincerity, cooperation, friendship and understanding were crucial throughout the process of this project.

ABSTRACT

The "Analysis on Telnet and SSH" is a project to analyze the Telnet and SSH protocol. Every final year students are compulsory to do a project related to their field of studies. "Analysis on telnet and SSH" requires basic knowledge on both the protocols as in how they are used as remote login utilities. The configuration of hardware and software to setup both the services and the commands to perform activities are some of the basic knowledge to be known before carrying out any detailed analysis. The objective of this analysis is to compare and analyze the data transmission for both the protocols. Four parameters are chosen as benchmark to analyze and compare and they are packet sequence, packet content, round trip time and throughput. The idea of this analysis is based on the problem statement and problem analysis in Siemens Malaysia Sdn. Bhd. This is basically a case study analysis. The main aim is to determine a better command based protocol in Siemens environment. At the end of the analysis, a better protocol is determined and conclusion for the project is made. All these data and results obtained can be used for future references for all those who are interested in knowing more about the protocols.

ABSTRAK

Tajuk projek "Analysis on Telnet and SSH" ialah satu analisis mengenai dua protokol iaitu Telnet dan SSH. Setiap pelajar tahun akhir diwajibkan melaksanakan satu project berkaitan dengan pengkhususan matapelajaran masing-masing. Kajian ini memerlukan pengetahuan asas mengenai kedua-dua protokol dari segi konfigurasi perkakasan dan perisian, command untuk arahan aktiviti sebelum menjalankan kajian ini. Objektif utama projek ini ialah untuk membuat perbandingan antara kedua-dua protokol dari segi komunikasi data melalui sesuatu rangkaian. Empat parameter dijadikan kayu pengukur bagi mencapai objektif dan parameter tersebut ialah "round trip time", "throughput", ututan paket data dan kandungan paket. Idea untuk menjalankan analisa ini adalah setelah mengkaji masalah yang wujud di Siemens Malaysia Sdn. Bhd. Analisa ini sebenarnya adalah untuk mengetahui protokol yang lebih baik untuk diimplementasikan di rangkaian Siemens. Perbezaan di antara kedua-dua protokol juga dibincangkan. Setelah menjalankan analisa ini, protokol yang lebih baik dengan penerangan yang sewajarkan juga disertakan. Kesemua data dan keputusan yang diperolehi boleh digunakan oleh golongan yang ingin mengetahui lebih lanjut mengenai kedua-dua protokol Telnet dan SSH.

TABLE OF CONTENTS

CHAPTER	SUBJECT	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENTS	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	xii
	LIST OF FIGURES	xiv
	LIST OF ABBREVIATIONS	xvi
	LIST OF APPENDICES	xvii
 CHAPTER I	 INTRODUCTION	
	1.1 Project Background	1
	1.2 Problem Statements	2
	1.3 Objective	4
	1.4 Scopes	5
	1.5 Project Significance	7
	1.6 Expected Output	8
	1.7 Conclusion	9

CHAPTER II**LITERATURE REVIEW AND PROJECT
METHODOLOGY**

2.1	Introduction	10
2.2	Fact and Finding	10
2.2.1	Telnet and SSH	11
2.2.1.1	Remote Login	11
2.2.1.2	The longevity of Telnet	12
2.2.1.3	Telnet Protocol	12
2.2.1.4	Network Virtual Terminal	13
2.2.1.5	SSH Protocol	14
2.2.1.6	Authentication in SSH	15
2.2.1.7	Advantages and Disadvantages of SSH	16
2.2.1.8	Network Analysis and Sniffing	17
2.2.1.9	Ethereal	18
2.2.1.10	Round Trip Time	19
2.2.1.11	Throughput	20
2.2.2	Domain	20
2.2.3	Existing system	21
2.2.4	Technique	22
2.3	Project Methodology	23
2.3.1	Waterfall Development Methodology	24
2.3.2	Justification for Methodology	26
2.4	Project Requirement	27
2.4.1	Software Requirement	27
2.4.2	Hardware Requirement	28
2.4.3	Other Requirement	29
2.5	Project Schedule and Milestone	29
2.6	Conclusion	30

CHAPTER III	ANALYSIS	
3.1	Introduction	32
3.2	Problem Analysis	32
3.3	Quality and Types of Data	34
	3.3.1 Encryption and Data Compression	37
	3.3.2 Bits and Bytes	37
	3.3.3 Environment of Analysis	38
	3.3.4 Data representation in Telnet and SSH	38
	3.3.5 Packet transfer and quality of data in Telnet and SSH	40
3.4	Requirement Analysis	41
	3.4.1 Software Requirements	41
	3.4.2 Hardware Requirements	42
	3.4.3 Network Requirements	42
3.5	Conclusion	43
CHAPTER IV	DESIGN	
4.1	Introduction	45
4.2	Network Architecture	45
4.3	Logical Design	48
4.4	Physical Design	51
4.5	Security Requirement	53
4.6	Conclusion	54
CHAPTER V	IMPLEMENTATION	
5.1	Introduction	55
5.2	Network Configuration Management	56
	5.2.1 Configuration Environment Setup	56
	5.2.2 Version Control Procedure	59
5.3	Hardware Configuration Management	60
	5.3.1 Hardware Setup	66

5.4	Security	68
	5.4.1 Security policies and plan	68
5.5	Development Status	69
5.6	Conclusion	70

CHAPTER VI TESTING

6.1	Introduction	71
6.2	Test Plan	72
	6.2.1 Test Organization	72
	6.2.2 Test Environment	73
	6.2.3 Test Schedule	74
6.3	Test Strategy	74
6.4	Test Design	75
	6.4.1 Test Description	76
6.5	Test Results and Analysis	76
	6.5.1 Packet Content	77
	6.5.1.1 User Authentication and Packet Content	77
	6.5.1.2 Justification	81
	6.5.2 Packet Sequence	82
	6.5.2.1 Connection Establishment/ Termination and Packet sequence	82
	6.5.2.2 Comparison of connection establishment and termination	85
	6.5.2.3 Justification	86
	6.5.3 Round trip Time	88
	6.5.3.1 Round Trip Analysis	88
	6.5.3.2 Justification	91
	6.5.4 Throughput	92
	6.5.4.1 Throughput Analysis	92
	6.5.4.2 Justification	95

	6.5.5 Conclusion of Analysis and Result	96
	6.6 Conclusion	98
CHAPTER VII	PROJECT CONCLUSION	
	7.1 Observation on Weakness and Strengths	99
	7.2 Propositions for Improvement	100
	7.3 Contribution	101
	7.4 Conclusion	102
	REFERENCES	103
	BIBLIOGRAPHY	105
	APPENDICES	106

LIST OF TABLES

TABLE	TITLE	PAGE
6.1	Test Schedule	74
6.2	Number of Packets for Telnet and SSH	81
6.3	Time Taken for Session Establishment	86
6.4	Time Taken for Session Termination	86

LIST OF FIGURES

DIAGRAM	TITLE	PAGE
2.1	Waterfall Development Methodology	24
3.1	Flow Chart on Packet Analysis	35
3.2	Process of analysis	36
3.3	TCP Segment Format (Behrouz A.Forouzan, 2004)	39
3.4	Three-step connection establishment	40
4.1	OSI Model	46
4.2	Network Architecture	47
4.3	Logical Design (Siemens Damansara)	48
4.4	Logical Design (Siemens Meditel)	49
4.5	Physical Design	51
4.6	Security Layout	53
5.1	IP and Domain for environment	56
5.2	Capturing data using Ethereal	57
5.3	TCP filtering option	58
5.4	Ethereal Round TCP Stream Graph	59
5.5	Telnet Server Setup	61
5.6	SSH Hostkey definition	62
5.7	SSH cipher options	63
5.8	Password and Public Key authentication Option	63
5.9	SSH User Properties	64
5.10	SSH Tunneling	64

5.11	Putty Configuration	65
5.12	SSH version selection	66
6.1	User Authentication in SSH	78
6.2	Ethereal Capture for User Authentication and Key Exchange	79
6.3	Capture of Password Transmitted	80
6.4	Packet Sequence for Session Establishment	83
6.5	Packet Sequence for Session Termination	84
6.6	Round Trip Time Graph for Telnet Within LAN	88
6.7	Round Trip Time Graph for SSH Within LAN	89
6.8	Round Trip Time Graph for Telnet Across LAN	90
6.9	Round Trip Time Graph for SSH Across LAN	90
6.10	Throughput Graph for Telnet Within LAN	93
6.11	Throughput Graph for SSH Within LAN	93
6.12	Throughput Graph for Telnet Across LAN	94
6.13	Throughput Graph for SSH Across LAN	94

LIST OF ABBREVIATIONS

CPU	-	Central Processing Unit
DES	-	Data Encryption Standard
DMZ	-	Demilitarized Zone
DNS	-	Domain Name System
FTP	-	File Transfer Protocol
GPL	-	General Public License
GUI	-	Graphical User Interface
IDS	-	Intrusion Detection System
IETF	-	Internet Engineering Task Force
ISP	-	Internet Service Provider
LAN	-	Local area Network
NIC	-	Network Interface card
NVT	-	Network Virtual Terminal
OSI	-	Open System Interconnection
RAM	-	Random Access Memory
RDP	-	Remote Desktop Protocol
RTT	-	Round-Trip Time
SDLC	-	System Development Life Cycle
SSH	-	Secure Shell
STP	-	Shielded Twisted Pair
TCP	-	Transmission Control Protocol
TCP/IP	-	Transmission Control Protocol/Internet Protocol
UDP	-	User Datagram Protocol
UTP	-	Unshielded Twisted Pair
WBS	-	Work Breakdown Structure

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
APPENDIX A	Log book	106
APPENDIX B	Proposal Form	113
APPENDIX C	Gantt Chart	118
APPENDIX D	Letter from Siemens Malaysia Sdn.Bhd	121
APPENDIX E	Samples of capture	123
APPENDIX F	Installation of Ethereal	126
APPENDIX G	Installation of FreeSSHd	130

CHAPTER I

INTRODUCTION

1.1 Project Background

Networks are for sharing resources remotely, so almost anything done on a network could fall within the definition of remote access. By tradition, a few TCP/IP utilities are classified as remote access utilities. These utilities are ported to many operating systems. The main purpose of these utilities is to give a remote user some of the capabilities a local user might have.

The internet has become the most economical means for communication between two remote sites. Telnet which stands for Terminal NETwork is the standard protocol that simply provides a facility for remote logins to computer via the Internet. The basic purpose of Telnet is to provide a means by which keyboard commands typed by a remote user can cross the network and become input for a different computer. The effect is that the remote user can interact with the server as if user were logged in locally.

Though internet plays an important role for remote communication, it does not provide any protection for the transmitted information and can become an information security nightmare. Firewalls and access controls such as one-time passwords do not fully solve the problem, as it is easy to record and analyze any transmitted data. The Telnet does not provide enough security to transmit data over the network.

Therefore, the Secure Shell or SSH is used for remotely logging in over public networks, where security is crucial. Both the Telnet and SSH plays similar functions but in SSH, all communications are encrypted to prevent the disclosure of security-critical information during transit over the network.

An 'Analysis on Telnet and SSH' is carried out to analyze the data communication in both of the protocols. The analysis will show the different form of traffic in both the protocols. The analysis is also to understand the security implementation in remote utilities and how encryption is used in the SSH protocol to solve one of the most acute security problems on the Internet, that is securely logging from one machine to another and to perform any activity such as securely transferring files between machines. The analysis is based on the case study in Siemens Malaysia Sdn. Bhd.

It is best to understand that SSH and Telnet works in a similar way but all communications in SSH are encrypted to prevent the exposure of confidential information during transit over the network. Telnet is inherently insecure as all the data transmitted is visible for anyone located between the user's computer and the server destination. In the SSH protocol, cryptographic algorithms are used to authenticate both ends of the connection, to automatically encrypt all transmitted data, and to protect the integrity of data.

1.2 Problem Statements

Siemens has many branch offices and the main branch resides in Damansara. Only administrators in the headquarters are allowed to remotely login to the servers and routers to check necessary settings. The username and password for administrators is very confidential. The process of remotely logging in to servers and routers using the Remote Desktop protocol often causes a high bandwidth. For an

example, to Remote Desktop a server in Gebeng, Kuantan it requires more time and the command are sent very slowly. The main reason for the slow connection is because the bandwidth in that office is low and the remote protocol takes most of the bandwidth to support the GUI based screen. This is not preferable as there are many site offices of Siemens that has very low bandwidth capacity. It takes longer time and bandwidth to remotely control the computers through remote desktop.

Therefore, the administrators have come with an idea to use a command based remote procedure to log in to servers and routers. The two possible protocols were either Telnet or SSH. Even though Telnet is obsolete, but the usage can be important if transfers of data are secured. Therefore, this analysis is carried out based on certain parameters that would help to give a better solution and determination of protocol to be used.

Security is a crucial issue when it comes to data transmission over the network. Insecure networking application such as Telnet simply passes all the confidential information, such as users' password in a clear text over the network. This situation aggravated through broadcast based network that allowed malicious user to eavesdrop on the network and collect all communicated information. Thus, the counter measure for this problem is to the SSH.

Remote desktop is basically used either to login to user's machine to check on some settings or on a router to see its interface. When remote desktop is done from the main Siemens branch to other site offices, it often takes plenty of time and the communication is very slow for some areas. For an example, it takes approximately five minutes to remote desktop to a server in the Gebeng, Kuantan office to check on the server. Some administrators in Siemens need to log in to the server periodically to check the status and performance of the server. Log files are also viewed to monitor the activity of servers like Mail Server.

Therefore, there was a need to analyze these two different protocols in terms of data communication and security to understand the effect on data security in Siemens Malaysia. The knowledge on SSH was also not sufficient enough to compare and determine the implementation of Telnet or SSH in Siemens. It is important for any companies to have a high sufficient level of security without making normal use any more difficult than necessary.

1.3 Objective

This analysis is to provide information on Telnet and SSH protocol and to further understand the transmission of data in both the protocols. The objectives of “Analysis on Telnet and SSH” are as below:

- a) To collect and gather all the data related to packet transmission in Telnet and SSH using protocol analyzer called Ethereal. Data collected are in terms of four parameters that are packet sequence, content of the packet, round trip time and throughput.

The ethereal analyzer will be run to capture all the data needed to analyze the traffic. All the data is analyzed using the same protocol analyzer. A few settings are done at the analyzer to capture only related data.

- b) To analyze and compare the data relayed across the network in Telnet and SSH.

Results obtained are analyzed and compared among the two protocols. The comparison is of the four parameters stated in earlier objective. The results of analysis and comparison will be shown in graphical representation.

- c) To determine the better protocol in terms of packet sequence, security of the data transmitted, round trip time, throughput and the better protocol to be used in Siemens environment.

The results are analyzed and conclusion is made to verify a better protocol for Siemens environment. Proper justification on why such conclusion is made is also provided.

1.4 Scopes

The analysis of Telnet and SSH are based on a few scopes. The analysis is mainly on the data and the transmission of packets over the network. Packets will be analyzed in terms of packet sequence, content of the packet, round trip time and throughput. These elements are analyzed to give a better comparison in terms of data communication between both the protocols.

To analyze the packet sequence, data for session establishment and termination is examined to give a clearer explanation about the sequence of packets in both protocols. Content of the packet can learn by looking at the session where user is authenticated for password. In this session, a detailed analysis on the exposure of the data transmitted can be known. This may provide a better justification on the security of the protocols. Number of packets transmitted for the same amount of data is also examined for both protocols to determine the higher probability for data lost, retransmission and traffic congestion.

Network analyzers are used to capture the packets and analyze the protocols. The selection of the protocol analyzer is based on the functions available in the analyzer and its importance in providing appropriate results for this analysis. In this analysis, the Ethereal is used as the protocol analyzer.

In Siemens, the Telnet and SSH server is set on the File server. This server resides in the Siemens Meditel Office. Analysis in Siemens is done on two categories. The first one is a session just within the LAN in Siemens Meditel. The second one is across the LAN which means session is from a client in Meditel to server in Damansara office. In Damansara office, the server software is installed on the Orlig Server that handles ticketing system for the Helpdesk Team.

The Telnet and SSH can be implemented on many platforms. But for this analysis, only Microsoft Windows is used because that is the platform used in all servers and clients in Siemens Malaysia. There is no UNIX or Macintosh based stations in that company. Therefore, the results of this analysis will be upon implementation on a Windows platform.

The screen capture on the servers in Siemens is not allowed to be saved. All the confidential data of the server is not transparent to outsider. Therefore, when installation was done on the server and sessions were established, the interfaces and the content of the servers were not allowed to be recorded. Only clients in Siemens were allowed to be screen captured for its content and settings.

The results of this analysis can be used for educational purpose and is based on case study in Siemens. The results may vary from one place of case study and another depending on the bandwidth and transfer rate of the network at the place of case study. It is also to understand that when it comes to security issues, there is no statement to say that either Telnet or SSH can provide a complete security solution as they have many advantages and disadvantages.

1.5 Project Significance

The analysis is basically to give information to everyone on the data transmission on both the Telnet and SSH protocols and to provide understanding on the encrypted transmission in SSH. It is also to give awareness to users on the possible security vulnerabilities that can be faced due to visible data transmission over the network.

The administrators in the Helpdesk Team of Corporate Information Office in Siemens can view this analysis to see how important it is to have secured remote sessions with users or to check on the servers because all the transmissions involves username, password and other confidential data. Administrators are also able to learn more on the implementation of the protocols and to understand the difference between both the protocols.

Besides Siemens Malaysia, the report of this analysis can also be used as reference to carry out any other analysis based on Telnet and SSH. Anyone interested to know more on the protocols can view the report and gain some knowledge. As for students in university, this analysis can be stepping stone or a good reference to further their project or enhance the analysis on the remote login protocols.

The explanation and results of this analysis will also determine the better protocol to be used in a network and the advantages of using a more secured remote login. In short, it will give a clearer picture of remote sessions and secure channels between machines.