

# **COVERT CHANNEL: NETWORK STEGANOGRAPHY DEPLOYMENT**

By

**NURUL MAJDI BINTI MD ALI**

(2004633671)

Supervised by

**PROF. MADYA DR. SAADIAH YAHYA**

A project research paper submitted to

**FACULTY OF INFORMATION TECHNOLOGY AND QUANTITATIVE  
SCIENCES**

**UNIVERSITI TEKNOLOGI MARA**

In partial fulfillment of requirement for the

**BACHELOR OF SCIENCE (Hons.) IN DATA COMMUNICATION AND  
NETWORKING**

**UNIVERSITI TEKNOLOGI MARA**

**SHAH ALAM, SELANGOR**

**NOV 2005**

## ACKNOWLEDGMENT

All praises to Allah s.w.t for all His bless that help me on completing this research project. On this opportunity, I would like to show gratitude for those who had involved in contributing the idea and support either directly or indirectly along making this research project until it is complete. Special thanks to my supervisor, Dr Saadiah Yahya for her encouragement, guidance, comment and ideas that led me in producing a better quality research project. To En Adzhar who give me a great guidance, encouragement and tolerance. Your clarification is very pleasure.

Last but not least, to all Computer Technology and Networking lecturers and my colleagues and other in the faculty, who are simply too numerous to indicate, thanks to all encouragement and support given. To my parents and closest friends, it is all thank you so much that I could say. All the assist and support is much appreciated. Finally to all mentioned here, may Allah will reciprocate all of them for all those support. Thank you for everything.

To all the aforementioned, may Allah bless all of you.

Nurul Majdi binti Md Ali.

2004633671

BSc. Data Communication and Networking

## ABSTRACT

Steganography is one of the major techniques used to hide the existence of communication that lies between two overt parties. Steganography also denoted by art of hiding communication. This work relates the areas of steganography, network protocols and security for practical data hiding in communication networks employing TCP/IP. This project major focus is to deploy steganography on network protocol using *covert\_TCP* tool. This tool uses 3 methods in order to employ steganography at TCP/IP header; IP identification encoding, TCP sequence number encoding and ACK “bouncing” server method. We also employ network steganography in two different network environment which is on transmission on single host (loopback interface) and inter local area network. After that phase, we analyze packet income and out the network. We used network sniffer tool, tcpdump to dump all the packet and analyze the accuracy of the data transmit using covert channel as employ by *covert\_TCP*.

## TABLE OF CONTENTS

	Page
ACKNOWLEDGEMENTS	ii
LIST OF TABLES	vi
LIST OF FIGURES	vii
ABSTRACT	viii
CHAPTERS	
<b>1 INTRODUCTION</b>	
1.1 INTRODUCTION	1
1.2 BACKGROUND OF THE PROBLEM	1
1.3 STATEMENT OF THE PROBLEM	2
1.4 OBJECTIVES OF THE RESEARCH	3
1.5 SCOPE AND LIMITATION OF RESEARCH	3
1.6 SIGNIFICANCE OF RESEARCH	4
1.7 CONCLUSION	4
<b>2 LITERATURE REVIEW</b>	
2.1 INTRODUCTION	5
2.2 BRIEF HISTORY	6
2.3 STEGANOGRAPHY IN DETAILS	7
2.3.1 TYPES OF STEGANOGRAPHY	7
2.4 DEFINITION OF TECHNICAL TERMINOLOGIES	8
2.4.1 Steganography	8
2.4.2 Steganographer	8
2.4.3 Covert Channel	8

2.4.4	Overt Communication	9
2.4.5	Steganalysis	9
2.4.6	Encoding	9
2.4.7	Decoding	9
2.5	COVERT CHANNEL: DEFINITION AND BACKGROUND	9
2.6	CONCLUSION	12
<b>3</b>	<b>METHODOLOGY</b>	
3.1	INTRODUCTION	13
3.2	PRELIMINARY STUDY	13
3.3	DETAILED STUDY	14
3.3.1	Information Gathering	14
3.3.2	Software Requirements	14
3.3.3	Hardware Requirements	15
3.3.4	Network Design and Consideration	16
3.4	DATA ANALYSIS	16
3.4.1	Platform Preparation Workflow	17
3.4.2	TCP/IP Steganography Establishment Workflow	18
3.4.3	Experimental Testing Workflow	19
3.4.4	Analysis of Packet	19
3.5	CONCLUSION	19
<b>4</b>	<b>COVERT CHANNELS: A DISCUSSION ON TCP/IP PROTOCOL SUITE</b>	
4.1	INTRODUCTION	20
4.2	TCP/IP PROTOCOL SUITE COVERT CHANNEL	20
4.2.1	Application Layer	23
4.2.2	Transport Layer	23
4.2.3	Network Layer	23
4.2.4	Data Link Layer	23
4.3	TCP/IP HEADER: PIGGYBACKING	23
4.4	CONCLUSION	28