INFORMATION HIDING WITH COVERT CHANNEL

ERNEES INSYIRAH BINTI MOHAMAD FUAAD

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS TESIS

JUDUL : INFORMATION HIDING WITH COVERT CHANNEL

SESI PENGAJIAN : 2016 / 2017

Saya, ERNEES INSYIRAH BINTI MOHAMAD FUAAD

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti 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 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 : No 20 Jalan BK5/6C
Bandar Kinrara 47180
Puchong Selangor

Prof Madya Dr Mohd Faizal Bin Abdollah

Tarikh: 24/8/17

Tarikh: 24/8/17

INFORMATION HIDING WITH COVERT CHANNEL

ERNEES INSYIRAH BINTI MOHAMAD FUAAD

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

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2017

DECLARATION

I hereby declare that this project report entitled

INFORMATION HIDING WITH COVERT CHANNEL

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

STUDENT : ______________________ Date: 24/8/17
(ERNEES INSYIRAH BT MOHAMAD FUAAD)

SUPERVISOR : ______________________ Date: 24/8/17
(PM DR. MOHD FAIZAL BIN ABDOLLAH)

DEDICATION

~ To my beloved parents and those who had always by my side during my upside down ☺ ~

ACKNOWLEDGEMENTS

Alhamdulillah, praises to Allah. With His Willing, I manage to finish my Final Year Project, Information Hiding With Covert Channel for PSM 2 Presentation. I would like to express my appreciation and gratituted to my supervisor, PM Dr Mohd Faizal Bin Abdollah for his vital encouragement and support. He had given me a valuable guidance for my project. Without him, I may face a problem to complete my project. Besides, I would like to thank my parents and family who always encouragement and suppport me. Last but not least, thanks to member of Faculty of Information Communication and Technology UTeM and my classmates for their commitment and cooperation during completing my project. Also, thanks to my partner, Nurul Fazreen Binti Noorashid for her never ending support during period of completing my Final Year Project.

ABSTRACT

A covert channel is described as a communication link between two parties that allows one party to transfer information to the other in a manner that violates the system's security policy. Covert channels are categorized into *covert storage channels* and *covert timing channels*. Communication in a covert storage channel entails the writing of hidden data into a storage location (not meant for communication) by the transmitting party, and the subsequent retrieval of that information by the receiving party. In difference, communication in a covert timing channel requires that the transmitting party signal information by modulating its own system resources such that the manipulation affects the response time observed by the receiving party. The problem statement for this project are data sent over the network could be attack by third party and the confidentialiy and integrity of data are not guaranteed while being transmitted in the network. This project embarks on the following objectives are; To study in-depth of covert channel and to identify parameter that will used in developing covert channel system, to develop a robust covert channel system to increase integrity and confidentiality of data, and to test and verify the system through network. While the methodology being used to develop the project by using iterative model. The development contribution of the project helps to determine what the project will produce beside its objective. Besides, it will help to determine the parameter that will be used to develop the covert channel. Also, it will helps to determine the procedure involve in developing the system and if the system will achieve the objective of the project which is to develop a robust covert channel system.

ABSTRAK

Saluran rahsia adalah penghubung komunikasi antara dua pihak membolehkan satu pihak untuk memindahkan maklumat kepada yang lain dengan cara yang melanggar dasar keselamatan sistem. Saluran rahsia ini dikategorikan kepada dua kategori iaitu saluran rahsia simpanan dan saluran masa rahsia. Saluran rahsia simpanan melibatkan penulisan data tersembunyi ke lokasi penyimpanan oleh pihak yang menghantar, dan mendapatkan semula yang berikutnya maklumat itu oleh pihak yang menerima. Manakala saluran rahsia masa memerlukan bahawa pihak yang menghantar isyarat maklumat dengan modulasi sumber sistem sendiri seperti bahawa manipulasi yang memberi kesan kepada masa tindak balas yang diperhatikan oleh pihak yang menerima. Kenyataan masalah bagi projek ini adalah data yang dihantar melalui rangkaian boleh menjadi serangan oleh pihak ketiga di mana kerahsiaan dan integriti data adalah tidak dijamin semasa ia dihantar dalam rangkaian. Projek ini memulakan objektif berikut adalah; Untuk mengkaji dengan lebih mendalam saluran rahsia dan untuk mengenal pasti parameter yang akan digunakan dalam membangunkan sistem saluran rahsia, untuk membangunkan satu sistem saluran rahsia yang mantap untuk meningkatkan integriti dan kerahsiaan data, dan untuk menguji dan mengesahkan sistem melalui rangkaian. Tambahan pula kaedah yang digunakan untuk membangunkan projek ini adalah dengan menggunakan model lelaran. Sumbangan pembangunan projek membantu untuk menentukan apa projek itu akan menghasilkan sebelah objektifnya. Selain itu, ia akan membantu untuk menentukan parameter yang akan digunakan untuk membangunkan saluran rahsia. Ia juga akan membantu untuk menentukan prosedur yang terlibat dalam membangunkan sistem dan jika sistem akan mencapai objektif projek iaitu untuk membangunkan sistem saluran rahsia teguh.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

HTTP	Hypertext Transfer Protocol
SSL-MITM	Session Layer Protocol- Man-in-the-middle
CA	Certificate Authority
SSL	Session Layer Protocol
RWWWShell	Reverse WWW Shell
DNS	Domain Name Server
HTML	Hypertext Markup Language
LAN	Local Area Network
WISIWIR	what-is-sent-is-what-is-received

CHAPTER I

INTRODUCTION

1.1 Introduction

In this chapter, I will first identify the problem has been issued with current situation which about confidentiality and integrity of transmitted data or information. Next, the objective will be defined to answer the project question which arises during planning for the project development. Also, the scope will define which field is involved for the project development and the contribution will identify what the project is contributing. Last but not least, this chapter will conclude summarization for all chapters on what will be done on each chapter.

1.2 Problem Statement

According to (Cole, 2003), covert channels are similar to stego where both parties know they are communicating and what they are communicating. The only big difference is that no overt channel is used. Normal data is transmitted and the covert message is not hidden in traditional stego. The hidden message is the used of covert channel itself.

Steganography in (J.Cox, L.Miller, A.Bloom, Fridrich, & Kalker, 2008) stated that, steganography is the act of covert communication, which means that only the sender and receiver are aware of the secret message. However, from (Cole, 2003) there is a flaw by using traditional steganography which is there is no security technology is. A person can read the message if he or she knows there are hidden message there or knows the algorithm that was used and if the message is not encrypted. Another problem is, if someone thinks that that you are using stego, he or she could easily destroy any hidden message without destroying the host file. For example, in most cases, the data will be hidden in an image of least significant bits. The easiest way to destroy the file by convert into a format that can be read or leave it the way they are.. If the bit composition changes even slightly, the message will be destroyed.

Here comes the variation of steganography. A covert channel is a subclass of steganography. According to (Cole, 2003), covert channels used when two parties communicate covertly over normal communication channels they are, in essence, using covert channels over communication. The goal is to use normal data objects but modify them slightly so that they can be used to communicate secretly. However, the modification should not make the object being sent over the channels look unusual.

According to (J.Cox et al., 2008), (Channels et al., 2012) and (Cole, 2003) covert channels are divided into two categories which are Timing Channel and Storage Channel. Covert storage channels are methods of communication that “include all vehicles that would allow the direct or indirect writing of a storage location by one process and the direct or indirect reading of it by another”. In other words, one process writes to a shared resource, while another process reads from it. While covert timing channels is method of communication that requires the transmitting party signal information by controlling its own system resources such that the manipulation affects the response time observed by the receiving party. It is essential to use a clock or measurement of time to signal the value being sent over channel.

The Prisoners’ Problem

From (J.Cox et al., 2008), the definition of covert channels first formulated by Simmons as The Prisoners Problem. Alice and Bob are under surveillance of a warden, Jack. The warden permitted Alice and Bob to communicate but with Jack’s monitoring the messages passes. If the warden thinks Alice’s message to Bob is innocuous, she may simply forward it to Bob. Alternatively, she may intentionally distort the content in the hope that such a distortion will remove any secret message that might present. So, Alice and Bob must exchange innocuous messages containing hidden information that hopefully Jack will not notice.

Based on (Channels et al., 2012), the scenario was extended towards computer networks where Alice and bob use two networked computers for communication. Alice and Bob share a secret, used for determining covert channel encoding parameters and encrypting/authenticating the hidden messages.

For practical purposes, Alice and Bob may also be the same person. Jack manages the network and monitors the passing traffic for covert channels or alters the passing traffic to eliminate or disrupt covert channel.

Basically, computer network were used for communication, connectedness and collaboration. The notion of openness behind this revolution however, does not address the security aspect in such environments. Security issues thus finally arisen out with the pace more than the rate at which Internet has gotten in to our lives. This work attempts to integrate network security with another emerging technology, data hiding; primarily associated with oblivious communication or more recently protecting copyright in digital media appearing on the Internet.

Nowadays, the safety of the transmitted data on the network becomes an issue when there are a lot of case such as data breaching issues and data being stolen or lost through network, the confidentiality and integrity of data cannot being guaranteed. Hence, the idea to develop a covert channel is an alternative ways to secure the data on the network.

Table 1.1 Summary of problem statement

PS	Problem Statement
PS1	The confidentiality and integrity of data cannot be guaranteed as it can be attack by third party while being transmitted through network

1.3 Project Question

When the system has been successful being implemented, the confidentiality and integrity still not guaranteed. Hence, the system should figure out how it will run and sending the data safely. In fact, how to verify if the program successfully embed the data into the IP identification?

Table 2 Summary of project question

PQ	Project Question
PQ1	Can the confidentiality and integrity of data preserved with covert channel system?
PQ2	Will the program embed successfully in IP ID?

1.4 Objective

Based on the project question, this project will conduct three main objectives. In ensuring the covert channel can successfully implemented. The architecture of network protocol should be reviewed and studied. After study and collect information about covert channel, network architecture structure, the protocols being used and parameter suitable to used, the implementation need to be done as well. When the implementation has been successful, testing and validation will be conducted to verify the system running through network. The project objective summarization as Table 1.3 below:

Table 3 Summary of project objectives

PQ	PO	Project Objective
PQ1	PO1	To identify parameter that will used in developing covert channel system
	PO2	To develop a covert channel system based on IP identification
	PO3	To test and verify the system through network

1.5 Scope

The scope of this project will focus on network security. This project will be based on Linux host, Fedora 25 where it will be installed on desktop both of the receiver and sender to setting up the channel on network.

Mainly this project focused on developing a covert channel to hide data through network using parameter from IP header structure, IP identification.

1.6 Contribution

The development contribution of the project helps to determine what the project will produce beside its objective. This project will help to determine the parameter that will be used to develop the covert channel. Also, it will helps to determine the procedure involve in developing the system and if the system will achieve the objective of the project which is to develop a covert channel system using IP identification. The project contribution are summarize as in Table 1.4 below.

Table 4 Summary of project contribution

PS	PQ	PO	PC	Project Contribution
PS1	PQ1	PO1	PC1	To introduce the parameter that will be used to developed the covert channel
		PO2	PC2	Determine the procedure involve in developing the system
		PO3	PC3	Determine whether the system has achieved the objective.

1.7 Thesis Organization

The report organization is constructed chapter by chapter in order to make sure that this project can be developed suits with the objective. The summarization and description of each chapter are stated as below:

Chapter 1: Introduction

This chapter discuss about introduction of covert channel which explained their concept and definition, scope of project and their contribution. Also briefly summarize the problem statement and objective of conducting this project.

Chapter 2: Literature Review

This chapter discuss about previous work, preview of current problem and justification and proposed solution.

Chapter 3: Project Methodology

This chapter discuss about the method will be use to develop the project and project milestone which show each stage of project development.

Chapter 4: Analysis and Design

This chapter discuss about the design and all of the software and hardware will be used to develop the project.

Chapter 5: Implementation

This chapter will discuss about how the system will works and step by step to configure and manage the system. Also it will state the status of the project implementation.

Chapter 6: Testing

This chapter will discuss about analysis and testing of this project. It will show the result of testing and test plan which include the organization, environment, schedule and strategy.

Chapter 7: Project Conclusion

This is the last chapter which will make the conclusion of this project. It will explain about the project limitation and contribution of the project. And also a brief of project summarization and suggestion for future work.