BORANG PENGESAHAN STATUS TESIS

JUDUL: BLASTER.A ATTACK PATTERN GENERALIZATION

SESI PENGAJIAN: SESI 2011/2012

Saya LIM SOK MING 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 :33, Lorong Sejahtera 11,
Taman Sejahtera, 14000 Bukit Mertajam,
Pulau Pinang, Malaysia
Tarikh : 29/8/2012

Dr. Robiah Yusof
Nama Penyelia
Tarikh: 29/8/2012

BLASTER.A ATTACK PATTERN GENERALIZATION

LIM SOK MING

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

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2012

DECLARATION

I hereby declare that this project entitled

BLASTER.A ATTACK PATTERN GENERALIZATION

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

STUDENT: _____ DATE: 29/8/2012

(LIM SOK MING)

SUPERVISOR: _____ DATE: 30/8/2012

(DR.ROBIAH BINTI YUSOF)

DEDICATION

Dear Parent

Thank you for your sacrifice and love.

Dear Teachers and Supervisors

Thank you for all the knowledge and guidance.

Dear Friends

Thank you for all the knowledge, guide, encouragement and love.

ACKNOWLEDGEMENTS

I would like to show my gratitude and appreciation to my supervisor, Dr.Robiah bt Yusof for all ideas and advices in guiding me throughout the project.

I would also like to thank my family members especially my parents. They have been giving me moral supports and all sorts of material supports throughout my years studying in this university.

Last but not least, I would like to say thank you to all my friends and course mates for their kindness in sharing knowledge and resources.

Thanks a lot.

ABTRACT

The number of crime committed based on the malware intrusion is never ending as the number of malware infection is growing tremendously. The significant threats of traditional worms such as Blaster, Sasser, Code Red and Slammer are still continuing due to hasty spreading nature in the Internet. In this project, network traffic is extracted to identify worm attack pattern. These worm attack pattern are further analyzed to form the general worm's attack pattern which describes the process of worm's infection. This project proposes a general attack pattern for worm in two different perspectives which is attacker and victim using only Blaster.A variant. Thus, the general attack pattern can be extended into research areas in computer forensic investigation.

ABSTRAK

Bilangan jenayah yang berdasarkan pencerobohan *malware* tidak pernah berhenti hal ini disebabkan bilangan jangkitan *malware* semakin meningkat.*Worm* tradisional seperti *Blaster*, *Sasser*, *Code Red* dan *Slammer* masih menjadi ancaman besar kepada *Internet.* Dalam projek ini, rangkaian trafik diekstrak untuk mengenal pasti corak serangan *worm*. Kemudian corak serangan tersebut dianalisa untuk menghasilkan corak serangan umum worm yang justeru menerangkan proses jangkitan *worm*.Projek ini mencadang menghasilkan corak serangan worm dari dua perspektif yang berbeze iaitu penyerang dan mangsa dengan mengunakan *worm Blaster.A* sahaja. Seterusnya, hasil tersebut boleh digunakan dalam penyelidikan dan penyisatan forensik komputer

.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

1.1 Project Background

Nowadays, the Internet is growing rapidly, same goes to malware attacks as is showed in Figure 1.1 and becomes a serious threat to the user in the Internet. As the end of 2010, the RISI database reported 60 confirmed malware incidents that occurred between 1982 and 2010[1]. Malware or malicious software is software that is residing in a system and cause harm to the system, such as Trojan, virus and worm. The most well known traditional worm such as Blaster, Sasser, Code Red and Slammer, are the major threats to the security of the internet [2]. Therefore, we need to study and analyze the traces of these malware attacks from perspective of attacker and victim in order to ensure the security on the Internet. Besides that, the attack pattern can also be used in investigation for collecting and tracing the evidence in forensic field.

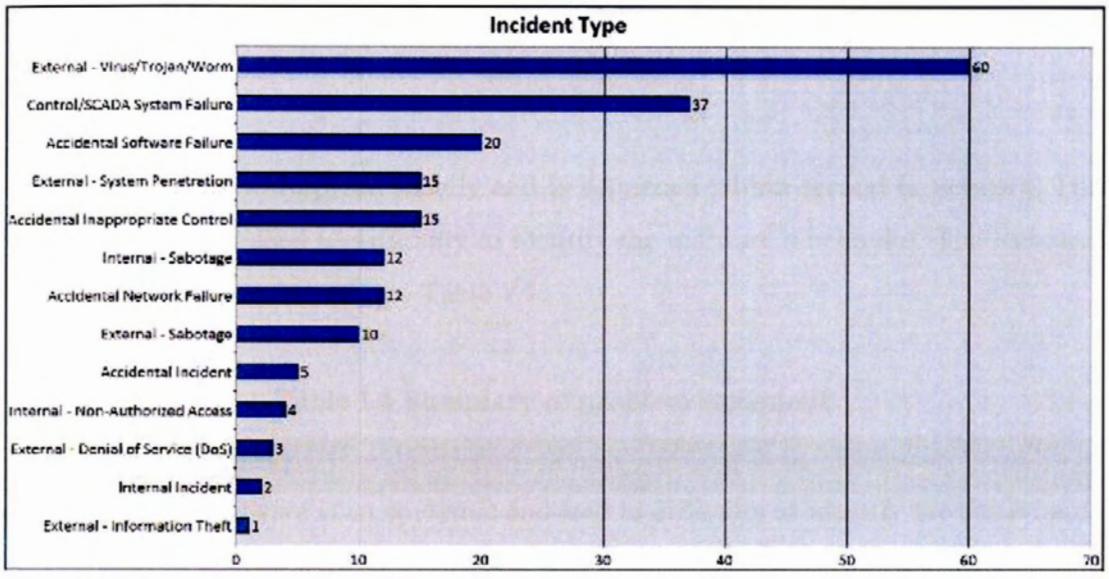

Figure 1.1 Incident types that occurred from 1982 until 2010 year [1]

As a result, a network environment of this project is conducted in Windows and Linux operating system workstations and IDS. The network is purposely infected by worm (Blaster.A) then, collect and analyze the network traffic data in order to generate specific worm attack pattern of Blaster.A of attacker and victim perspective. The network traffic is captured by using tcpdump tool. Tcpdump is a powerful command line interface packet sniffer and has ability to analyze network behavior by reading the detail of packets [1]. The worm attack pattern is important in order to provide a clear view on how the attack has performed [4] and from the result of it ,the attacker and victim also can be identified which will help how the crime is being committed.

1.2 Problem Statements

Malware is widespread rapidly and is happened within second in network. This characteristic had leaded to difficulty to identify the malware's behavior. The Research Problem (PR) is summarized into Table 1.1.

Table 1.1 Summary of problem statement

No	Research Problem
RP1	Malware is an epidemic and lead to difficulty to identify the behavior of the malware.

Thus, one Research Questions (RQ) is constructed to identify the research problem as discussed in previous section is depicted in Table 1.2.

Table 1.2 Summary of research question

RP	RQ	Research Question
RP1	RQ1	How can we identify the behavior of the malware?

RQ 1: How can we identify the behavior of the malware?

This research question is formulated by considering the malware's behavior issue which is epidemic as highlighted in RP1 in Table 1.1. This RQ is the primary guides to formulate the research objectives (RO) of this project.

1.3 Objective

Based on the research questions formulated in previous section, appropriate research objectives (RO) are developed as follows:

RO 1: To identify the feature of the malware in perspective of victim and attacker. In order to identify the behavior of malware, first need to find out the feature of the malware. Features of malware when malware is victim, and also when malware act as attacker.

RO 2: To generate attack pattern of malware in perspective of victim and attacker. After that, based on the features that had been identified can used to generate the attack of the malware in attacker and victim's perspective.

RO3: To generalize attack pattern malware in perspective of victim and attacker. Next, generalize attack pattern from the attack pattern of malware that had been defined before. From the attack pattern can point out the attacker and victim identity.

Table 1.3 Summary of research objectives

RP	RQ	RO	Research Objective
RP1	RQ1	RO1	To identify the feature of the malware in perspective of victim and attacker
		RO2	To generate attack pattern of the malware in perspective of victim and attacker
		RO3	To generalize attack pattern malware in perspective of victim and attacker

1.4 Scopes

Scope of project that is going to be conducted as follows:

1. Using only one specific type of traditional worm—Blaster.A
2. Focusing on attack pattern of victim and attacker perspective.
3. Using network traffic data (tcpdump).

1.5 Project Significant

The worm attack pattern of Blaster.A will help in network security to identify the identity of attacker and victim in network forensic.

1.6 Conclusion

In conclusion, this project will identify features and behaviors of worm (Blaster.A), then construct the worm attack pattern from perspective of attacker and victim. In the next chapter, I will do more research about Blaster.A and network traffic. At the same time, literature review and project methodology will also be done.

CHAPTER II

LITERATURE LEVIEW

2.1 Introduction

In this chapter, the two main topics are literature review and project methodology will be discussed. First of all, findings from the literature review about malware issues will discover the one research objective (RQ1) which to identify the behaviour of the malware that had been formulated in Chapter I, while, the first, second and third research objective (RO1, RO2, RO3) which are to identify the feature of the malware attack, then from the information gathered to construct a malware attack pattern from perspective of attacker and victim.

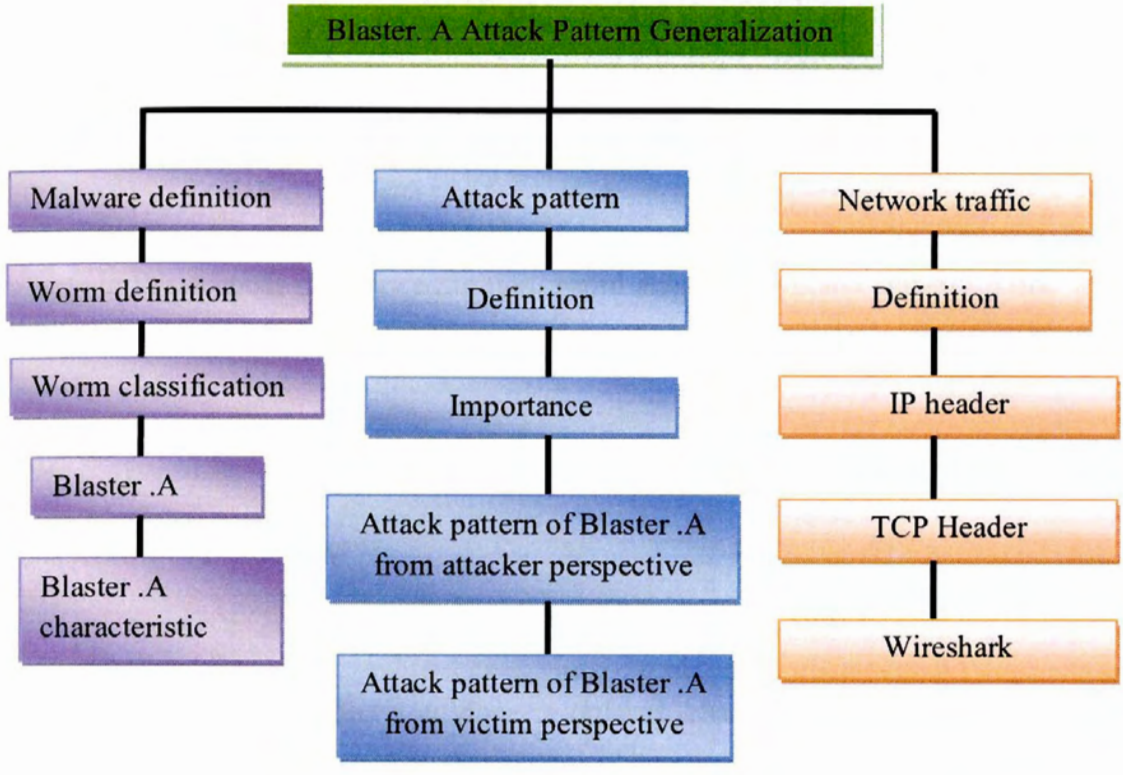

Figure 2.1 Operational framework: Literature review phase

In the Literature Review phase, as depicted in Figure 2.1, further information on malware, attack pattern and network traffic issues are gathered. During the Literature Review phase, the relevant literature in journals, articles, thesis, technical reports, books, websites and other academic sources are reviewed.