

## 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: 30/8/2012

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: \_\_\_\_\_

(LIM SOK MING)

SUPERVISOR: \_\_\_\_\_

(DR.ROBIAH BINTI YUSOF)

DATE: 29 / 8 / 2012

DATE: 25 / 8 / 2012

## **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 mencadangkan menghasilkan corak serangan *worm* dari dua perspektif yang berbeza iaitu penyerang dan mangsa dengan menggunakan *worm Blaster.A* sahaja. Seterusnya, hasil tersebut boleh digunakan dalam penyelidikan dan penyisatan forensik komputer

## TABLE OF CONTENTS

CHAPTER	SUBJECT	PAGE
	<b>DECLARATION</b>	<b>i</b>
	<b>DEDICATION</b>	<b>ii</b>
	<b>ACKNOWLEDGMENT</b>	<b>iii</b>
	<b>ABSTRACT</b>	<b>iv</b>
	<b>ABSTRAK</b>	<b>v</b>
	<b>TABLE OF CONTENTS</b>	<b>vi</b>
	<b>LIST OF TABLES</b>	<b>xi</b>
	<b>LIST OF FIGURES</b>	<b>xiii</b>
<b>1</b>	<b>INTRODUCTION</b>	
	1.1 Project Background	1
	1.2 Problem Statement	3
	1.3 Objectives	4
	1.4 Scopes	5
	1.5 Project Significance	5
	1.6 Conclusion	5
<b>2</b>	<b>LITERATURE REVIEW AND PROJECT METHODOLOGY</b>	
	2.1 Introduction	6



2.2	Fact and Finding	8
2.2.1	Malware Definition	8
2.2.1.1	Worm Definition	11
2.2.1.2	Worm classification	11
2.2.1.3	Blaster. A Worm	12
2.2.1.4	Blaster A Characteristic	13
2.2.2	Attack Pattern	15
2.2.2.1	Definition	15
2.2.2.2	Importance	15
2.2.2.3	Attack pattern of Blaster .A from attacker perspective	16
2.2.2.4	Attack pattern of Blaster .A from victim perspective	16
2.2.3	Network Traffic	17
2.2.3.1	Definition	17
2.2.3.2	IP Header	17
2.2.3.3	TCP Header	19
2.2.3.4	Wireshark	21
2.2.3.5	Summary of Literature Review	24
2.3	Project Methodology	25
2.3.1	Phase I: Literature Review	26
2.3.2	Phase II: Analysis	27
2.3.3	Phase III: Design and Development	27
2.3.4	Phase IV: Implementation	27
2.3.5	Phase V: Testing and Evaluation	28
2.4	Project Requirements	28
2.4.1	Software Requirement	28
2.4.2	Hardware Requirement	29
2.5	Project Schedule and Milestones	29
2.6	Conclusion	30

<b>3</b>	<b>ANALYSIS</b>	
3.1	Introduction	31
3.2	Problem Analysis	32
3.3	Requirement Analysis	36
	3.3.1 Data Requirements	37
	3.3.1.1 Dumpfile	37
	3.3.1.2 Reading Manually line by line in Wireshark	37
	3.3.1.3 Flow Graph Capturing	46
	3.3.1.4 Scenario Sketching of Each Data Set in Dumpfile	47
	3.3.1.5 Percentage of Features on Scenario	50
	3.3.1.6 Features Selection	58
	3.3.2 Software Requirements	58
	3.3.3 Hardware Requirements	59
3.4	Conclusion	59
<b>4</b>	<b>DESIGN</b>	
4.1	Introduction	60
4.2	Process Flow Blaster. A in Perspective of Attacker and Victim	61
4.3	Attack Pattern Design	63
	4.3.1 Basic Attack Model	63
	4.3.2 Attack Pattern of Blaster. A	64
	4.3.3 Attack Pattern of Worm (Blaster.A, Blaster.T and Sasser.B)	66
4.4	Scripting design	68
	4.4.1 Flowchart of the Script	69
	4.4.2 Data Flow Diagram of the Script	71
4.5	Conclusion	73

<b>5</b>	<b>IMPLEMENTATION</b>	
5.1	Introduction	74
5.2	Software Development Environment Setup	74
5.3	Software Configuration Management	75
5.4	Implementation Status	85
5.5	Conclusion	86
<b>6</b>	<b>TESTING</b>	
6.1	Introduction	87
6.2	Test Plan	88
	6.2.1 Test Organization	89
	6.2.2 Test Environment	89
	6.2.3 Test Schedule	91
6.3	Test Strategy	92
	6.3.1 Classes of Tests	93
6.4	Test Design	93
	6.4.1 Test Description	94
	6.4.2 Test Data	94
6.5	Test Results and Analysis	95
	6.5.1 Team A – Blaster.A	95
	6.5.2 Team T- Blaster.T	100
	6.5.3 Team B – Sasser.B	105
	6.5 Conclusion	108
<b>7</b>	<b>PROJECT CONCLUSION</b>	
7.1	Observation on Weaknesses and Strengths	109
7.2	Propositions for Improvement	110
7.3	Contribution	110
7.4	Conclusion	111

## **REFERENCES**

**APPEDICES A**  
**APPEDICES B**  
**APPEDICES C**  
**APPEDICES D**

## LIST OF TABLES

<b>TABLE</b>	<b>TITLE</b>	<b>PAGE</b>
1.1	Summary of problem statement	3
1.2	Summary of research question	3
1.3	Summary of research objectives	4
2.1	Definitions and details on each category of malware [8]	9
2.2	Blaster worm naming [17]	13
2.3	Description of each field in IP Header	18
2.4	Description of each field in TCP Header	20
2.5	Packet List Pane	22
2.6	Features that selected and with it description	25
2.7	Hardware Specification	29
3.1	Summary on Blaster.A's attacker pattern (attributes found=√, attributes not found=×, nil) [9]	33
3.2	Summary on Blaster.A's victim pattern (attributes found=√, attributes not found=×, nil) [9]	34
3.3	Summary of features for 3 scenarios	57
3.4	Summary of Features's Percentage for 3 Scenarios	57
3.5	Features that selected and with it description	58
5.1	Summary of progress of development	85
6.1	Testers in the Testing Phase	89
6.2	Hardware Requirements	90
6.3	Software Requirements	90

6.4	Testing Schedule using Blaster.A	91
6.5	Testing Schedule using Blaster.T	91
6.6	Testing Schedule using Sasser.B	92
6.7	Data to be tested	94
6.8	Comparison of Testing Output of Blaster. A - 8Mac2010_0100pm	96
6.9	Comparison of Testing Output of Blaster. A - 9Mac2010_1220am	97
6.10	Comparison of Testing Output of Blaster. A - 9Mac2010_1730pm	99
6.11	Comparison of Testing Output of BlasterT_5.00pm	101
6.12	Comparison of Testing Output of BlasterT_10.15am	103
6.13	Comparison of Testing Output of BlasterT_12.45pm	105
6.14	Comparison of Testing Output of SasserB-230410	106
6.15	Comparison of Testing Output of SasserB-260410	107
6.16	Comparison of Testing Output of SasserB-270410	108

## LIST OF FIGURES

<b>FIGURE</b>	<b>TITLE</b>	<b>PAGE</b>
1.1	Incident type that occurred from 1982 until 2010 year [1]	2
2.1	Operational framework: Literature review phase	7
2.2	Malware Category [8]	9
2.3	Worm Taxonomy as Described by [9]	12
2.4	IP Header version 4	18
2.5	TCP Header	20
2.6	Packet List Pane in Wireshark	22
2.7	Packet Detail Pane in Wireshark	23
2.8	Packet Byte Pane in Wireshark	24
2.9	Project Methodology	26
3.1	Framework of identify the attacker and victim [9]	32
3.2	IPv4 Header [21]	35
3.3	TCP Header [21]	35
3.4	Process flow to select feature	36
3.5	Connection on port 135, protocol TCP	37
3.6	Connection on port 135, protocol DCERPC	38
3.7	Connection on port 135, TCP protocol	39
3.8	Connection on port 4444 with TCP protocol (1)	39
3.9	Connection on port 4444 with TCP protocol (2)	40
3.10	Connection on port 4444 with TCP protocol (3)	40
3.11	Connection on port 4444 with TCP protocol (4)	41

3.12	Connection on port 69 with TFTP protocol	42
3.13	Connection of port 4444 with TCP protocol (5)	42
3.14	Data packet of msblast.exe	43
3.15	Connection of port 4444 with TCP protocol (6)	44
3.16	Connection of port 4444 with TCP protocol (7)	45
3.17	Connection of port 4444 with TCP protocol (8)	46
3.18	Scenario 1 of Blaster. A - 8Mac2010_0100pm	47
3.19	Scenario 2 of Blaster. A - 9Mac2010_1220am	48
3.20	Scenario 3 of BlasterA - 9Mac2010_1730pm	49
3.21	Percentage of Features on Scenario 1 of Blaster. A - 8Mac2010_0100pm	51
3.22	Percentage of Features on Scenario 1 of Blaster. A - 8Mac2010_0100pm	52
3.23	Percentage of Features on Scenario 2 of Blaster. A - 9Mac2010_1220am)	53
3.24	Percentage of Features on Scenario 2 of Blaster. A - 9Mac2010_1220am	54
3.25	Percentage of Features on Scenario 3 of BlasterA - 9Mac2010_1730pm	55
3.26	Percentage of Features on Scenario 3 of BlasterA - 9Mac2010_1730pm	56
4.1	Process flow of scripting design	60
4.2	Blaster. A attacker process flow	61
4.3	Blaster. A victim process flow	62
4.4	Basic Attack Model	63
4.5	Blaster.A attack pattern design on attacker perspective	64
4.6	Blaster. A attack pattern design on victim perspective	65
4.7	Worm attack pattern design on attacker perspective	66
4.8	Worm attack pattern design on victim perspective	67
4.9	General script design	69
4.10	Script design	70



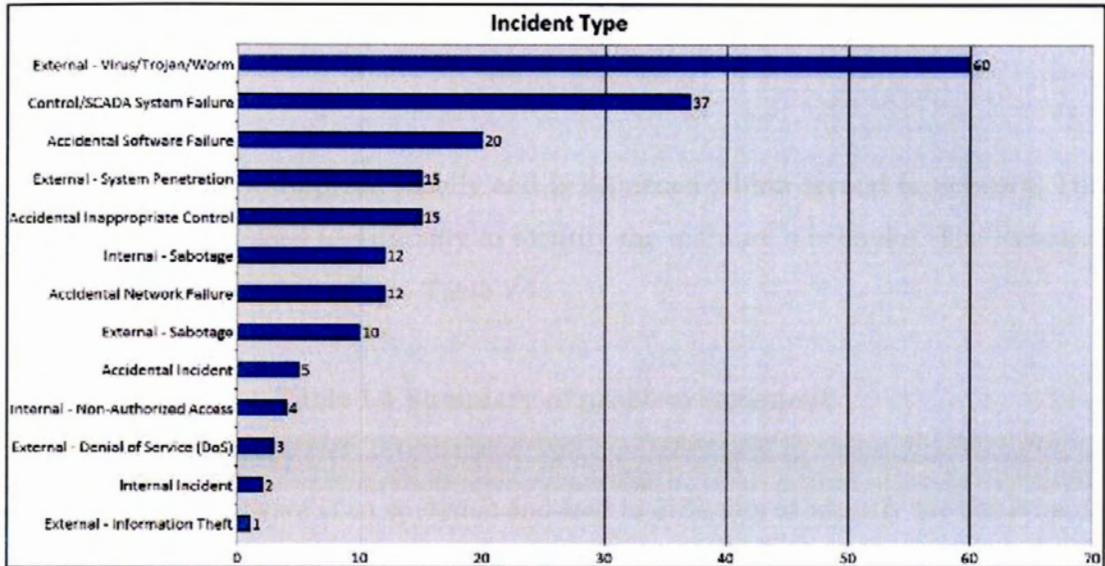
4.11	Context diagram of Data Flow Diagram (DFD)	71
4.12	Level 0 of Data Flow Diagram (DFD)	72
5.1	Code fragment for reading pcap file.	75
5.2	Code fragment for capturing packets	76
5.3	Window and its components	81
5.4	Code fragment of window	82
5.5	Code fragment of event listener	83
5.6	JFileChooser	83
5.7	Code fragment to show result	84
5.8	JOptionPane – Blaster	84
5.9	JOptionPane – Attacker and victim	84
5.10	Save file to MALWARE.txt	85
6.1	Testing Phase life cycle	88
6.2	Classes of Test	93
6.3	Testing output of Blaster. A - 8Mac2010_0100pm	95
6.4	Testing Output of Blaster. A - 9Mac2010_1220am	96
6.5	Testing Output of Blaster. A - 9Mac2010_1730pm (1)	97
6.6	Testing Output of Blaster. A - 9Mac2010_1730pm (2)	98
6.7	Testing Output of Blaster. A - 9Mac2010_1730pm (3)	98
6.8	Testing Output of Blaster. A - 9Mac2010_1730pm (4)	99
6.9	Testing Output of BlasterT_5.00pm (1)	100
6.10	Testing Output of BlasterT_5.00pm (2)	101
6.11	Testing Output of BlasterT_10.15am (1)	102
6.12	Testing Output of BlasterT_10.15am (2)	103
6.13	Testing Output of BlasterT_12.45pm (1)	104
6.14	Testing Output of BlasterT_12.45pm (2)	104
6.15	Testing Output of SasserB-230410	105
6.16	Testing Output of SasserB-260410	106
6.17	Testing Output of SasserB-270410	107

# 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 led 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**

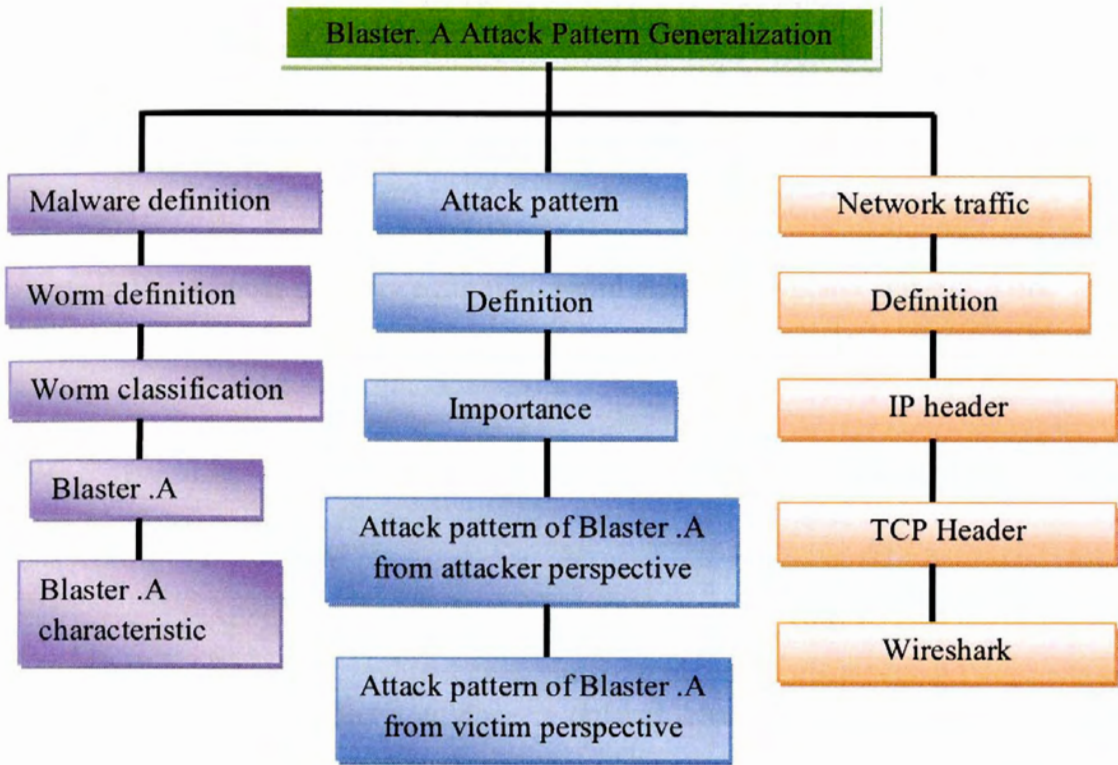
In conclusion, this project will identify features and behaviors of worm (Blaster.A), then construct the worm attack pattern from perspective of attacker and victim. In the next chapter, I will do more research about Blaster.A and network traffic. At the same time, literature review and project methodology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