FORMULATING GENERALIZE MALWARE ATTACK PATTERN USING FEATURES SELECTION

RUDY FADHLEE BIN MOHD DOLLAH

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

FORMULATING GENERALIZE MALWARE ATTACK PATTERN USING FEATURES SELECTION

RUDY FADHLEE BIN MOHD DOLLAH

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2014

BORANG PENGESAHAN STATUS TESIS

JUDUL:
FORMULATING GENERALIZE MALWARE ATTACK PATTERN USING FEATURES SELECTION

SESI PENGAJIAN: SESI 2013/2014

Saya RUDY FADHLEE BIN MOHD DOLLAH 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 14 Lot 19830
Kg Banggol Tok Jiring, 21060
Kuala Terengganu
Terengganu Darul Iman.

Nama Penyelia:
(Dr. Robiah Binti Yusof)

Tarikh : _____ Tarikh: _____

FORMULATING GENERALIZE MALWARE ATTACK PATTERN USING FEATURES SELECTION

RUDY FADHLEE BIN MOHD DOLLAH

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
2014

DECLARATION

I hereby declare that this project report entitled

FORMULATING GENERALIZE MALWARE ATTACK PATTERN USING FEATURES SELECTION

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

STUDENT : _____ Date: _____

(RUDY FADHLEE BIN MOHD DOLLAH)

SUPERVISOR :_____ Date: _____

(DR. ROBIAH BINTI YUSOF)

DEDICATION

Dear Allah
May my life is within your guidance.

Dear Beloved Parents
Thank you for your never ending love, support, patience and encouragement. May Allah bless always with you

Dear Lecturers and Supervisor
Thank you for all the knowledge and support.

Dear Friends
Thank you for all the knowledge, support and encouragement…

ACKNOWLEDGEMENTS

I would like to thank Dr.Robiah binti Yusof for her excellent support, guidance, motivation, constant patience, and continuous understanding throughout the semester of my Final Year Project in Universiti Teknikal Malaysia Melaka (UTeM).

I would also like to express my deepest appreciation to my beloved mother (Maimun), beloved father (Mohd Dollah) and my siblings (Murni Hayati and Murni Hayana) for their endless love, constant encouragement, support, motivation, patience and understanding throughout the year of my studies in UTeM.

To my friends, thank you for listening, offering me advice, and supporting me through this entire process. Special thanks to Amir Hamdi, Adibah Razali, Safarina, Hidayah Ibrahim, Al-Hafiz, Zhafri, Hafiz Gapar and all members of FTMK 3 BITC 2013/2014 which made my final years at UTeM a moment to remember.

ABSTRACT

Number of malware is growing dramatically. Malicious codes can be easily obtained and use as one of weapon to gain illegal objectives. Hence, in this project, network traffic are explored to identify the traces left on the victim and attacker to reveal the true victim and attacker. For the purpose of this project, it focused on malware intrusion and traditional worms namely Blaster and Sasser worm variants. This project is operated based on victim's and attacker's perspective. Thus, the objective of this project is to identify the features/attributes of malware in perspective of victim and attacker, to generate attack pattern of malware in perspective of victim and attacker, and to generalize the attack pattern in perspective of victim and attacker. Based on generating the attack pattern, the attack pattern for malware is generalized in algorithm script to verify it accuracy.

ABSTRAK

Bilangan *malware* semakin meningkat secara mendadak. Kod *malicious* mudah diperolehi dan digunakan sebagai salah satu senjata untuk mencapai objektif yang tidak baik. Oleh itu, dalam projek ini, rangkaian trafik diteroka untuk mengenalpasti kesan – kesan yang ditinggalkan oleh mangsa dan penyerang untuk menentukan corak surih *worm* untuk mendedahkan mangsa atau penyerang yang sebenar. Bagi tujuan itu, ia tertumpu kepada pencerobohan *malware* dan *traditional worm* iaitu variasi Blaster dan Sasser *worm*. Projek ini dikendalikan berdasarkan perspektif mangsa dan penyerang. Oleh itu, objektif projek ini adalah untuk mengenalpasti ciri – ciri atau sifat *malware*, untuk menjana corak serangan *malware*, dan untuk menjana corak menyerang secara umum dalam perspektif mangsa dan penyerang. Corak menyerang *malware* dijadikan umum dalam bentuk skrip algoritma untuk memastikan ketepatannya

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

1.1 Project Background

Malware, a word that stands for “malicious software” is a software or program that designed to penetrate or damaged a computer system which the victim not know their machine is being attacked. It can be grouped into two categories; independents and dependents. Independents malware does not need a host or program to spread the threats. Meanwhile, dependents need host or program to spread the attacks and require human intervention to launch the threat. The malware includes Trojan, virus and worm.

This project purpose is to analyze the malware ability on the view of victim and attacker. It is also to give outcome of generalize attack pattern of three malwares (Sasser.B, Blaster.A and Blaster.T).The generalize attack pattern is important to computer security researcher to enhance the security measure of the computer system.

Figure 1.1 shows a graph of incident received by Malaysian Computer Emergency Response Team(MyCERT) and is stated in the third quarter 2013 report. The incidents are vulnerabilities, spam, malicious code, intrusion attempt, intrusion, fraud, denial of service, cyber harassment, and content related. According to the Figure 1.1 below, malicious code shows a high number of cases handled by MyCERT.

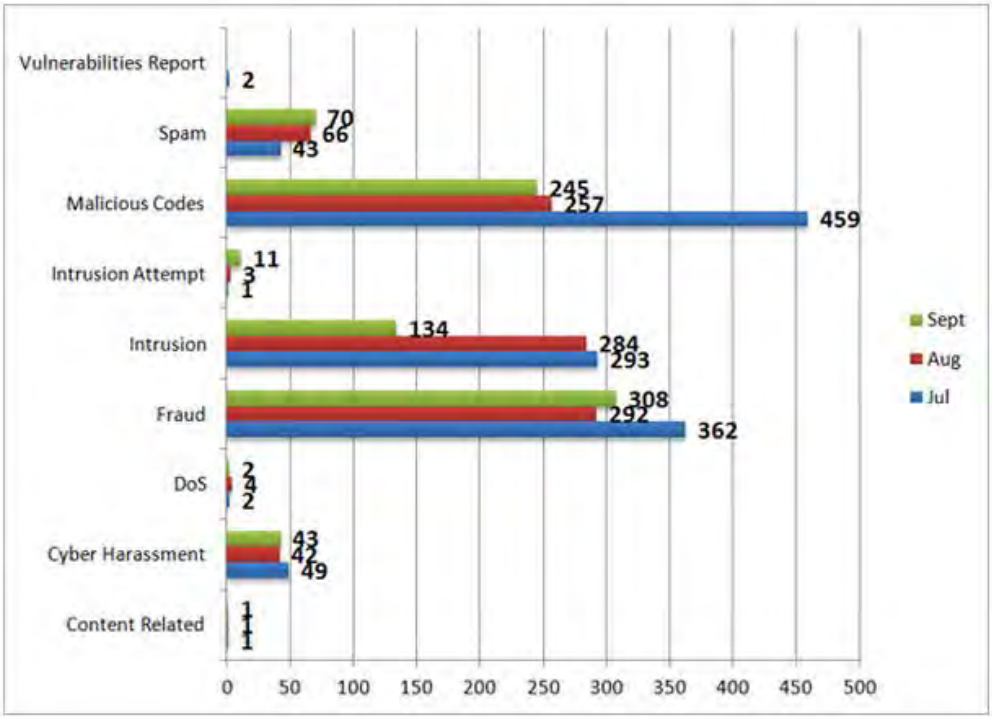

Figure 1.1 : Incidents received in Q3 2013 classified according to the type of incidents handled by MyCERT.

In addition, Figure 1.2 illustrates the incident handled by MyCERT of third quarter of 2013 compared to previous quarter. The data shows that Malicious Code have the highest increase compared to other categories of incident.

Categories of Incidents	Quarters		%
	Q2 2013	Q3 2013	
Content Related	26	3	88.46
Cyber Harassment	133	134	0.75
DoS	8	8	0.00
Fraud	1374	962	29.99
Intrusion	864	711	17.71
Intrusion Attempt	8	15	87.50
Malicious Codes	393	961	144.53
Spam	283	179	36.75
Vulnerabilities Report	4	2	50.00

Figure 1.2 : The incident handled by MyCERT in third quarter 2013 compared with previous quarter.

The summarized number of incidents about malicious code is created throughout the year 2013 is illustrated in Figure 1.3.

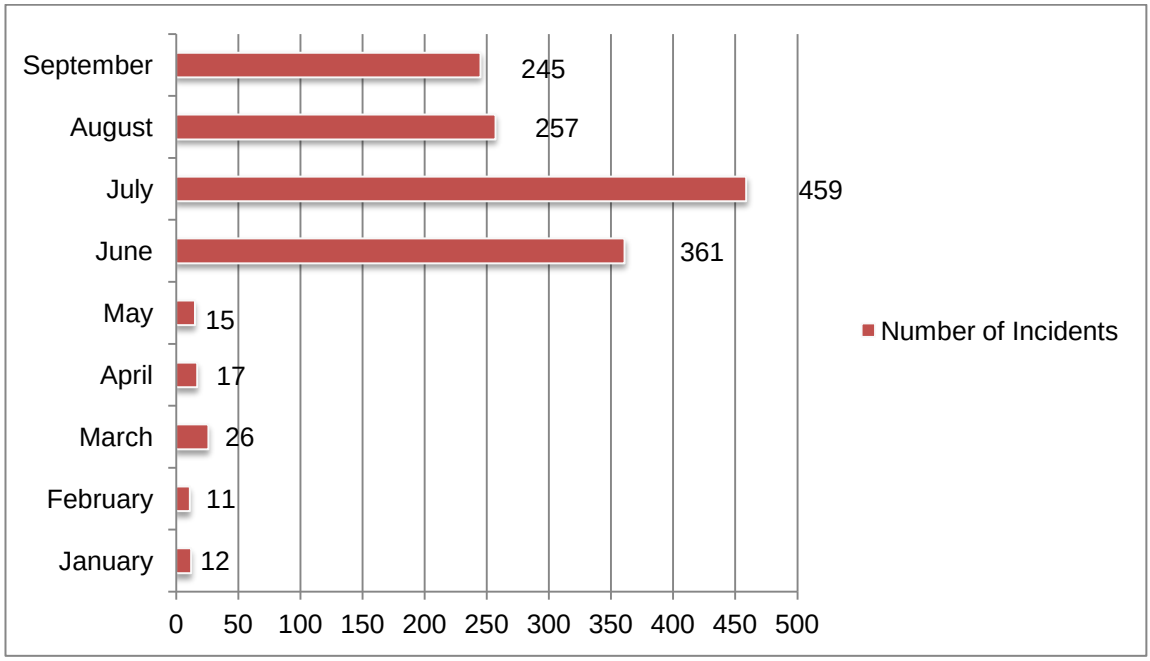

Figure 1.3 : Malicious code incidents received in 2013 handled by MyCERT.

Based on the both Figures 1.1, Figure 1.2 and Figure 1.3, we cannot take lightly of malicious code as it is a weapon that can be use by cybercriminal to do crime. Hence, it is very important to study and analyze the trace of the malware attack. The attack pattern provides information of their attack goals and we can use it to defend against the attack.

1.2 Problem Statement

Table 1.1 : Summary of problem statement

No	Problem Statement
RP1	With thousands of different malware on the Net, it is difficult to handling this malicious code based on it pattern individually.

1.2 Research Question

Only one Research Question (RQ) is generated to identify the research problem. From Research Problem 1 (RP1), Research Question 1 (RQ1) is produced. Table 1.2 is the summary of research question.

Table 1.2 : Summary of research question

RP	RQ	Research Question
RP1	RQ1	How can we generalize malware attack pattern of Sasser.B, Blaster.T and Blaster.A?

1.4 Objectives

Based on the research question in previous section, suitable Research Objective (RO) is produced to achieve aim of the research. There are three research objectives identified for this research.

RO1: To identify the general feature or attribute of malwares (Sasser.B, Blaster.T and Blaster.A).
Investigate the features or attributes of Sasser.B, Blaster.T and Blaster.A by analysing the network traffic of existing data.

RO2: To generate attack pattern in perspective of victim and attacker.
Based on identifying the features of malware, attack pattern of malware (Sasser.B, Blaster.T and Blaster.A) is generated for victim and attacker.

RO3: To verify the accuracy of the algorithm script.
Based on generating the attack pattern, the attack pattern for malware is generalized in algorithm script to verify it accuracy.

Table 1.3 : Summary of research objectives

RP	RQ	RO	Research Objective
RP1	RQ1	RO1	To identify the general feature or attribute of malwares (Sasser.B, Blaster.T and Blaster.A).
RP1	RQ1	RO2	To generate attack pattern in perspective of victim and attacker.
RP1	RQ1	RO3	To verify the accuracy of the algorithm script.

1.5 Scopes

The scope of this research will focus on certain matters as specified below:

1. This research is using only three specific type of traditional worm - Sasser.B, Blaster.T and Blaster.A.
2. Focusing on attack pattern of victim and attacker perspective.
3. Using network traffic data (tcpdump).

1.6 Project significance

Based on the research objectives, this research will contribute in identify the appropriate attributes / features in respective network traffic of malwares (Sasser.B, Blaster.T and Blaster.A) in perspective of victim and attacker. Besides, this research will propose the malware's (Sasser.B, Blaster.T and Blaster.A) attack pattern in perspective of victim and attacker. Furthermore, this research will propose the general malware's attack pattern in perspective of victim and attacker.

1.7 Conclusion

In conclusion, the generalize attack pattern help researcher to identify the objective of the attack and can expand it to strategize the defend mechanism of the computer network system. The next chapter will discuss on literature review, project methodology, software requirement, hardware requirement, and other requirement.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

In this chapter, there are two main topics that will be discussed, the literature review and project methodology. The literature review will based on reading phase framework design to ensure the literature are related to research title and will help to answer research question(RQ1) and achieve research objectives (RO1), (RO2) and (RO3). The project methodology will also discuss later in this chapter.

Figure 2.1 and Figure 2.2 are reading framework for literature review phase. This framework will be use as the guide in this chapter. The project title is breakdown into several items consist of malware definition, worm attack pattern and feature selection. The malware definition focused on literature of worm definition and the scopes are about three worms which are Blaster.A, Blaster.T and Sasser.B. The worm attack pattern framework part is about defining the attack pattern term and identifying the role perspective of attacker, victim and victim/attacker scenario. In addition, the feature selection part focused on network tools, network traffic and programming language for scripting at later phase of the project.

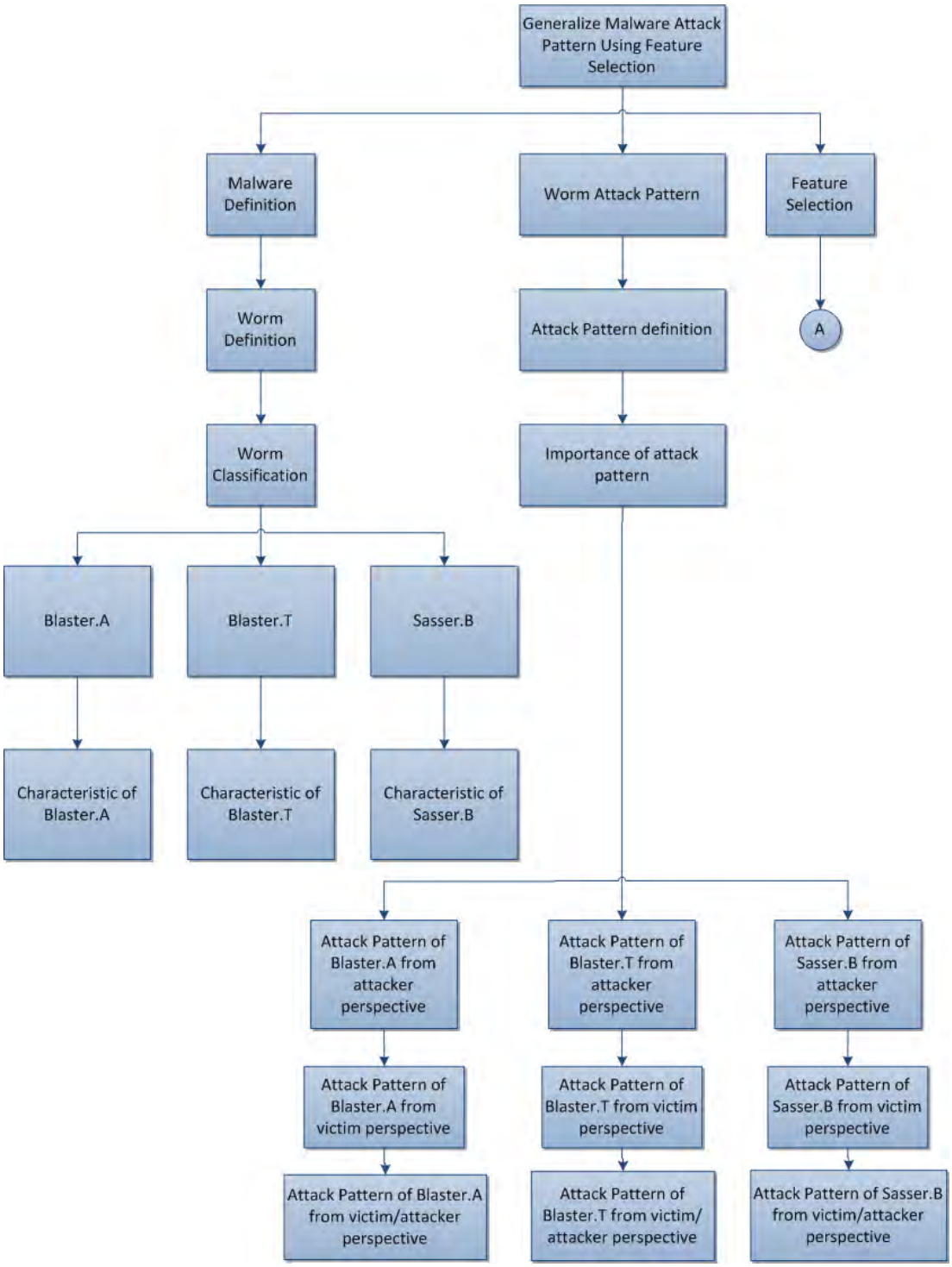

Figure 2.1 : Literature review phase part 1