

## BORANG PENGESAHAN STATUS TESIS

JUDUL: INVESTIGATING GOLDDREAM ANDROID MALWARE BEHAVIOR THROUGH DYNAMIC ANALYSIS

SESI PENGAJIAN: SESI 2012/2013

Saya LOW JUN KEAT mengaku membenarkan tesis Projek Sarjana Muda 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 : 924, Permatang Bendahari  
13110 Penaga S.P.U  
Pulau Pinang, Malaysia

DR. SITI RAHAYU SELAMAT  
Nama Penyelia

Tarikh : 30/8/2013

Tarikh: 30/8/2013

**INVESTIGATING GOLDDREAM ANDROID MALWARE BEHAVIOR THROUGH  
DYNAMIC ANALYSIS**

**LOW JUN KEAT**

**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**

**2013**

## DECLARATION

I hereby declare this project report entitled  
INVESTIGATING GOLDDREAM ANDROID MALWARE BEHAVIOR  
THROUGH DYNAMIC ANALYSIS

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

STUDENT :  \_\_\_\_\_ Date: 30/8/2013

(LOW JUN KEAT)

SUPERVISOR:  \_\_\_\_\_ Date: 30/8/2013

( DR. SITI RAHAYU SELAMAT )

## **DEDICATION**

This work is dedicated to my beloved family and siblings, who passed on a love of reading and respect for education.

To my supportive friends, my supervisor and all lecturers, thank you so much for assist and help.

## **ACKNOWLEDGEMENTS**

Thanks the god for giving me the opportunity to complete this Final Year Project which is titled Investigating GoldDream Android Malware Behavior Through Dynamic Analysis.

Firstly, I would like to thanks to, my supervisor, DR. SITI RAHAYU SELAMAT for her technical guidance and valuable time in assisting us in the accomplishing my project. I also want to thanks to all lecturers for their cooperation during completing my final year project by giving valuable information, suggestions and guidance in the compilation and preparation of this report.

Lastly, deepest thanks and appreciation to my parents, family and friends for their understanding, cooperation and full of support for the report completion, from the beginning till the end of this project. Also thanks to all of my friends and everyone, that has been contributed by supporting my work and helps myself during the final year project progress until it is fully completed.

## ABSTRACT

In recent year, the growing of Android user are become popular. Unfortunately, as Android is getting more popular, at the same time, it cause the growing of the mobile malware. As the malware are growth rapidly, the current problem is difficulty on detecting and identifying the behavior of android malware. Thus, the aim of this project is to investigate *GoldDream* Android malware behavior through dynamic analysis. This project used software and hardware tool such as *Wireshark* for capturing network traffic, emulator for running the android malware applications and Windows 7 operating system as a platform in order to complete the analysis. Hence, the emulator, *Wireshark* and other tools are installed in Windows 7 operating system which the experiment is executed and data is collected. The objective of this project is to investigate the parameter of android malware's behavior, generate the attack pattern of android malware and formulate the procedure of extracting the attack pattern. The project are start with literature review, analysis, design and implementation, finally is evaluate and testing. In the end of project, the general attack pattern of *GoldDream* malware is generated based on its basic attack model and its attributes. Then, the *GoldDream* attack pattern extraction script is developed base on the attack pattern.

## ABSTRAK

Kini, kegunaan Andorid menjadi semakin popular, tetapi dalam masa yang sama ia menyebabkan penyebaran *malware* semakin serius. Oleh sebab *malware* menyebar dan berevolusi dengan cepat telah menyebabkan kesukaran dalam mengesan dan mengenalpasti sifat-sifat *malware*. Dalam projek ini, sifat GoldDream android *malware* akan dikenalpasti melalui analisis dinamik. Projek ini menggunakan perisian dan perkakasan serta alatan seperti *Wireshark* bagi pengumpulan data trafik rangkaian, *emulator* untuk memasang aplikasi *malware* Android dan system pengoperasian Windows 7 untuk menjalankan analisis. *Emulator*, *Wireshark* dan alat-alat lain di pasang dalam sistem pengoperasian Windows7 untuk mengesan dan pengumpulan data aktiviti *malware* Android. Objektif projek ini adalah untuk mengenalpasti parameter tingkah laku, menjana corak serangan dan merangka prosedur mengeluarkan corak serangan. *malware* Android. Projek ini dimulakan dengan kajian literatur, analisis, reka bentuk dan pelaksanaan, serta akhirnya menilai dan menguji. Pada akhir projek, corak serangan umum GoldDream dihasilkan berdasarkan model serangan dan sifatnya. Seterusnya, satu *script* dibangunkan bagi mengenalpasti dan menghasilkan corak serangan GoldDream.

## TABLE OF CONTENTS

CHAPTER	SUBJECT	PAGES
	<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>x</b>
	<b>LIST OF FIGURES</b>	<b>xii</b>
<b>1</b>	<b>INTRODUCTION</b>	
	1.1 Project Background	1
	1.2 Problem Statements	2
	1.3 Project Questions	2
	1.4 Project Objectives	3
	1.5 Project Contribution	4
	1.6 Scope	4
	1.7 Project Significant	5
	1.8 Report Organization	5
	1.9 Summary	6
<b>2</b>	<b>LITERATURE REVIEW</b>	
	2.1 Introduction	7
	2.2 Android	8
	2.2.1 Definition	8



2.2.2	Architecture	8
2.3	Malware	9
2.3.1	Malware Definition	9
2.3.2	Malware Distribution	10
2.3.3	Malware Classification	10
2.3.4	Basic Malware Attack Model	12
2.3.5	Trojan Horse Definition	13
2.3.6	Trojan Horse Classification	13
2.3.7	Android Malware	14
2.4	Analysis Technique	17
2.4.1	Static Analysis	17
2.4.2	Dynamic Analysis	18
2.5	Parameter	18
2.5.1	Network Traffic	18
2.5.2	System Call	22
2.6	Attack Pattern	23
2.7	Summary	24
<b>3</b>	<b>METHODOLOGY</b>	
3.1	Introduction	25
3.2	Project Methodology	25
3.2.1	Phase I: Literature Review	26
3.2.2	Phase II: Analysis	26
3.2.3	Phase III: Design & Implementation	26
3.2.4	Phase V: Testing & Evaluation	27
3.3	Project Schedule & Milestones	28
3.3.1	Gantt Chart	28
3.3.2	Milestones	29
3.4	Summary	29
<b>4</b>	<b>DESIGN AND IMPLEMENTATION</b>	
4.1	Introduction	30

4.2	GoldDream Analysis Approach	30
4.2.1	Setup Network	31
4.2.2	Setup Environment	33
4.2.3	Malware Activation & Data Collection	34
4.2.4	Data Analysis	37
4.3	GoldDream attack pattern extraction	
	Scripting Design	55
4.3.1	General Design for GoldDream attack pattern extraction Script	55
4.3.2	GoldDream attack pattern extraction Process Script	56
4.4	Summary	60

## **5 TESTING AND RESULT ANALYSIS**

5.1	Introduction	61
5.2	Test Planning	61
5.2.1	Test Organization	61
5.2.2	Test Environment	62
5.2.3	Test Schedule	65
5.3	Test Strategy	65
5.3.1	Unit Testing	66
5.3.2	Integrate Testing	66
5.4	Test Design	66
5.4.1	Test Data Set	66
5.5	Test Result	67
5.5.1	Test Result for System Call	67
5.5.2	Test Result for Network Traffic	71
5.6	Result Analysis	73
5.6.1	System Call Result Analysis	73
5.6.2	Network traffic Result Analysis	78
5.7	Discussion of Result Analysis	82

5.7.1	Capturing Phone Call Log and Sms Malware Activity	82
5.7.2	Sending Information to Server	85
5.7.3	General GoldDream Attack Pattern	86
5.8	Summary	87
<b>6</b>	<b>CONCLUSION</b>	
6.1	Introduction	88
6.2	Project Summarization	88
6.3	Project Contribution	88
6.4	Project Limitation	89
6.5	Further Project	89
	<b>REFERENCES</b>	90
	<b>APPENDIX</b>	93

5.5	Datasets summarization	67
5.6	Comparison of system call result between script output and manual analysis for DS1	74
5.7	Comparison of system call result between script output and manual analysis for DS2	75
5.8	Comparison of system call result between script output and manual analysis for DS3	76
5.9	Comparison of system call result between different Dataset	77
5.10	Comparison of network traffic result between script output and manual analysis for DS1	78
5.11	Comparison of network traffic result between script output and manual analysis for DS2	79
5.12	Comparison of network traffic result between script output and manual analysis for DS3	80
5.13	Comparison of network traffic result between different Dataset	81

## LIST OF TABLES

<b>TABLE</b>	<b>TITLE</b>	<b>PAGE</b>
1.1	Summary of problem statement	2
1.2	Summary of project questions	2
1.3	Summary of project objectives	3
1.4	Summary of project contributions	4
2.1	Malware classification and Definition	11
2.2	Trojan Horse classification and Definition	13
2.3	Android malware type and Definition	15
2.4	Description of each field in IP Header	20
2.5	Description of each field in TCP Header	21
3.1	PSM 1 Milestones	29
4.1	Collected user and devices information	48
4.2	Network traffic attributes	50
4.3	System call attributes	51
5.1	Test organization	62
5.2	Hardware Requirements	63
5.3	Software Requirements	63
5.4	Test Schedule	65

## LIST OF FIGURES

<b>FIGURE</b>	<b>TITLE</b>	<b>PAGE</b>
2.1	Operational framework: Literature review phase	8
2.2	Android Architecture	9
2.3	Malware distribution in 2013	10
2.4	Malware classification	10
2.5	General Malware attack pattern	12
2.6	Basic Malware attack model	12
2.7	Trojan Horse classification	13
2.8	Percentage of mobile operating system infected by malware	14
2.9	Analysis technique	17
2.10	IP header	19
2.11	TCP header	19
3.1	Project Methodology	25
3.2	Project Gantt Chart	28
4.1	Analysis Approach	30
4.2	Physical design of malware analysis environment	31
4.3	Logical design of malware analysis environment	32
4.4	Process of collect network traffic	34

4.5	Process of collect system call	36
4.6	Data analysis Approach	37
4.7	Collected network traffic	38
4.8	Content of network traffic	39
4.9	Capture of phone call log	40
4.10	Capture of received message content	41
4.11	Location of zjphonecall.txt and zjsms.txt	42
4.12	Content of zjphonecall.txt	45
4.13	Content of zjsms.txt	45
4.14	Process of sending user and devices information	47
4.15	Collect user and devices information	48
4.16	Resolve domain name to IP address	48
4.17	Establish connection to server	49
4.18	Process flow of capture the phone log and sms	52
4.19	Basic Attack Model	53
4.20	GoldDream attack Pattern	54
4.21	General design for goldDream attack pattern extraction script	55
4.22	Overall process of GoldDream attack pattern extraction script	56
4.23	Phone call and sms identification	57
4.24	Information stealing identification	58
4.25	Extraction of malicious network traffic payload	59
5.1	Test environment design	64

5.2	Result of capture phone call log and sms from DS 1	68
5.3	Result of capture phone call log and sms from DS 2	68
5.4	Result of capture phone call log and sms from DS 3	69
5.5	Result of send user and devices information to server from DS 1	70
5.6	Result of send user and devices information to server from DS 2	70
5.7	Result of send user and devices information to server from DS 3	71
5.8	Result of network traffic from DS 1	72
5.9	Result of network traffic from DS 2	73
5.10	Result of network traffic from DS 3	73
5.11	Example captured data	83
5.12	General format of captured data	83
5.13	Example location of store text file	84
5.14	General pattern of file location	84
5.15	Method to save captured data	84
5.16	Request url	86
5.17	General url pattern	86
5.18	Proposed General goldDream Attack Pattern	87



# CHAPTER 1

## INTRODUCTION

### 1.1 Project Background

In recent year, the growing of smart phone is become popular. There are various of operating system in smart phone such as *IOS*, *Window*, *Android* as well as *Symbian*. Android is the most popular (40.9%) compare to Apple ios(40.5%), Blackberry (8.9%) (Arlotta, 2013). Unfortunately, as android are getting more popular, at the same time, it cause the growing of the mobile malware.

Malware also known as malicious software used or created by attackers to damage or destroy computer operation, stole sensitive information and break into private computer systems. It can be emerge as a collection of code, script, active content and embedded in other application (McMahon, 2013).

The malware are grows rapidly, it is a need to take effectively defend against the malware. In order to create a method to against the malware, we need to study, analysis and investigate the malware. Malware analysis is an activity in which carry out by reverse engineering the malware and investigate on code structure, operation and functionality ( Varghese, 2011).

The goal of this project is to understand the behavior of an android malware. In addition, Android OS is a popular environment for mobile malware. It needs to take an action to overcome it before it getting serious. However, we need to understand how it works before we can defend it.

Therefore, this project will use dynamic analysis to analyse the malware. It will focus on the behavior of attack, determine how and what it gets installed, how it runs, what background processes have been created, which ports are used to communicate, who they are communicating to, etc. (Distler, 2007). In this project, the parameters such as system calls and network traffic will be investigated.

**1.2 Problem Statement**

Malware will spread widely, rapidly, will embed in other software and some may encrypt the network traffic. This characteristic causes the difficulty to detect and identify the malware (Yen, 2011). The Project Problem (PP) is summarized into Table 1.1.

Table 1.1 Summary of problem statement

No	Research Problem
PP1	Difficulty on detecting and identifying the behavior of Android malware

**1.3 Project Questions**

Three Project Questions (PQ) is constructed to identify the problem statement as discussed in previous section is depicted in Table 1.2.

Table 1.2 Summary of project questions

RP	RQ	Research Question
PP1	PQ1	What is the parameter used to study the behaviour of Android malware?
	PQ2	What is the behavior of android malware?
	PQ3	What is the procedure of extract the behavior?

**PQ1: What is the parameter use to study the behaviour of Android malware?**

This project question is to analyses which parameter is suitable to use to study on the behavior of Android malware. Because of different type of malware may infect to different parameter, thus it is important to analyses which parameter should be use.

**PQ2: What is the behavior of Android malware?**

This project question is to study and identify which technique is suitable to use to collect the data that use to identify the behavior.

**PQ3: What is the procedure of extract the behavior?**

This project question is to find out how to extract the behavior and generate the attack pattern automatically.

**1.4 Project Objectives**

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

Table 1.3 Summary of research objectives

RP	RQ	RO	Research Objective
PP1	PQ1	PO1	To investigate the parameter of Android malware's behavior
	PQ2	PO2	To generate the attack pattern of Android malware
	PQ3	PO3	To formulate the procedure of extracting the attack pattern

**PO 1: To investigate the parameter of Android malware's behavior**

In order to analyse the Android malware, first we must identify what parameter will be use to analyse the malware. Different type of malware may have different type of parameter to inspect.

**PO 2: To generate the attack pattern of Android malware**

After determine the parameter use to analyses the malware, the next step is to collect data and analyses the data to identify the behavior in order to generate attack pattern.

**PO3: To formulate the procedure of extracting the attack pattern**

After generate the attack pattern of malware, then will formulate the procedure and develop a script to extract the attack pattern automatically from raw data.

**1.5 Project Contributions**

The contribution of this project are summarized in Table 1.4

Table 1.4 Summary of project contributions

RP	RQ	RO	RC	Project Contributions
PP1	PQ1	PO1	PC1	The parameter use to analyses android malware's behavior
	PQ2	PO2	PC2	The attack pattern of android malware
	PQ3	PO3	PC3	The script to extract android attack pattern

**1.6 Project Scope**

The project will be focused on:

- a. *GoldDream* malware
- b. System call and network traffic parameter
- c. Using dynamic analysis
- d. Develop script to extract the attack pattern

## **1.7 Project Significant**

The attack pattern of *GoldDream* will help developer in develop a method or software to protect the system from *GoldDream* malware.

## **1.8 Report organization**

This report consist of six chapter namely Chapter 1: Introduction, Chapter 2: Literature Review, Chapter 3: Methodology, Chapter 4: Design and Implementation, Chapter 5: Testing and Result Analysis and Chapter 6: Conclusion.

### **Chapter 1: Introduction**

This chapter will discuss about introduction, project background, research problem, research question, research objective, scope, project significant and report organization.

### **Chapter 2: Literature Review**

This chapter will explain related work of this project, such as Android, malware, analysis technique and parameter.

### **Chapter 3: Methodology**

This chapter will explain the method use to analyse the malware and organise the sequence of project work in phase by phase.

### **Chapter 4: Design and Implementation**

This chapter will introduce the software and hardware use in this project, environment setup, implementation of malware as well as the data collected.

### **Chapter 5: Testing and Result Analysis**

This chapter will analyse the collected data and carry out the scripting proposed to support the evidence.

## **Chapter 6: Conclusion**

This chapter will concludes and discussed the finding, limitations, contribution and the future work of the project.

### **1.9 Summary**

In this chapter, problem statement, questions and objective of the projects are clearly identified. The next chapter, Chapter 2 will discuss the related work of this project.

# CHAPTER 2

## LITERATURE REVIEW

### 2.1 Introduction

In chapter 1, the problem statement, questions and objective of the projects are clearly identified. For this chapter, the main topics are literature review will be discussed. The aim of this chapter is to review several issues related with this project, such as Android, malware, analysis technique and parameter as depicted in Figure 2.1.

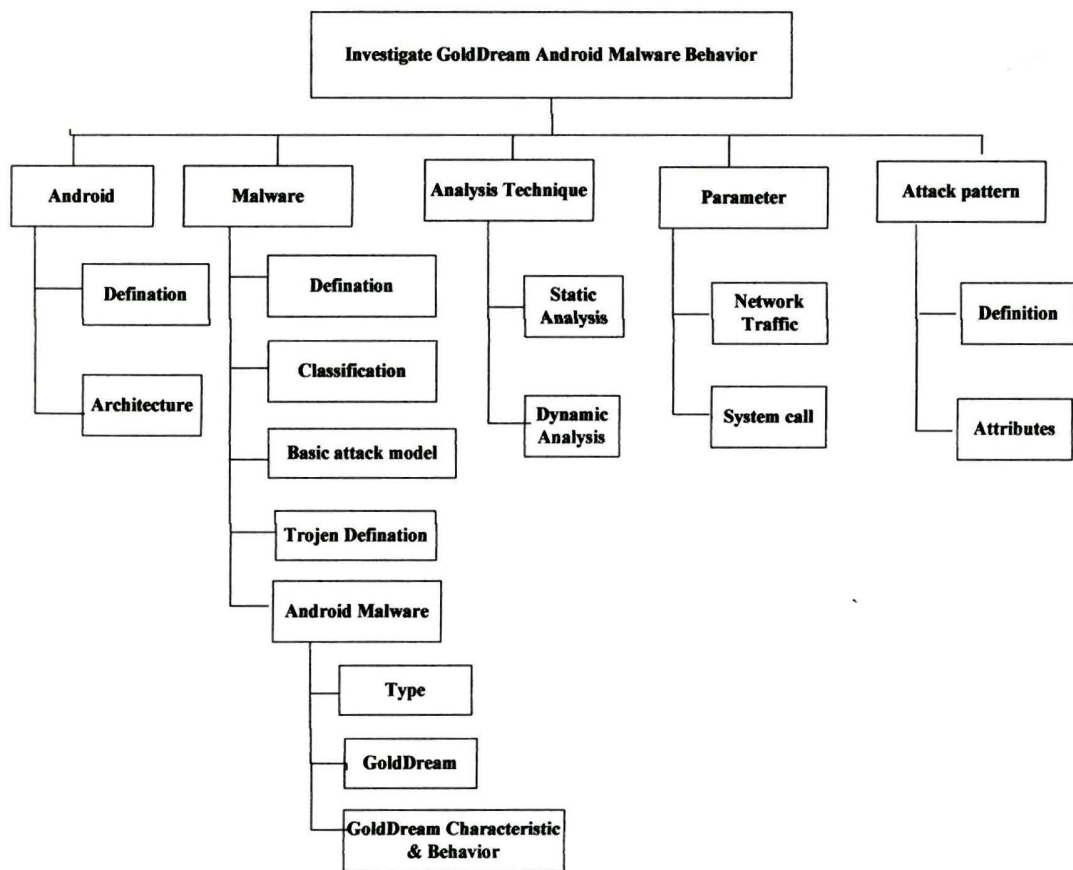


Figure 2.1 Operational framework: Literature review phase

Figure 2.1 shows the topic will be discussed in the following sections. Further information on Android, malware, analysis technique and system parameter 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. The 5 main issues to discuss in literature review is Android, malware, analyses technique, system parameter and attack pattern.

## **2.2 Android**

In this section, the definition and the architecture of android is discussed.

### **2.2.1 Definition**

Android is a Linux-based operating system (Katsarakis, 2012) that mainly designed for touch screen mobile device such as tablet and smart phone. Android, Inc. was the first who start to develop Android and it is financially backed by Google, but in 2005 it is bough by Google (Elgin and Ben, 2005). Android is open source and Google release the code under the Apache License in september 2008 (Katsarakis, 2012).

### **2.2.2 Architecture**

The Android architecture structural diagram is shown in Figure 2.2. The Android architecture are consist of 5 layer, which is the lowest layer Linux kernel layer, native libraries, the Android Runtime, the application framework layer and application layer is on the top layer (Brahler, 2010).