A MEASUREMENT OF RISK SEVERITY LEVEL OF ANDROID MALWARE BASED ON DANGEROUS PERMISSIONS (PROBABILITY) AND DATA THEFT (IMPACT)

By

Rio Asepta
2-2015-102

MASTER'S DEGREE
in

INFORMATION TECHNOLOGY
ENGINEERING & INFORMATION TECHNOLOGY

SWISS GERMAN UNIVERSITY
EduTown BSD City
Tangerang 15339
Indonesia

August 2016

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.

Rio Asepta

Student   Date

Approved by:

Dr. Mulya R. Mashudi, S.T., M.E.M

Thesis Advisor   Date

Charles Lim, M.Sc

Thesis Co-Advisor   Date

Dr. Ir. Gembong Baskoro, M.Sc.

Dean   Date

ABSTRACT

A MEASUREMENT OF RISK SEVERITY LEVEL OF ANDROID MALWARE BASED ON DANGEROUS PERMISSIONS (PROBABILITY) AND DATA THEFT (IMPACT)

By

Rio Asepta

Dr. Mulya R. Mashudi, S.T., M.E.M, Advisor

Charles Lim, M.Sc, Co-Advisor

SWISS GERMAN UNIVERSITY

The usage of smartphone has grown rapidly, exceeded the computer market share. Undeniable, this phenomenon has attracted the malware developers. More than 2.5 million of new malware found in Q4 of 2015 and most of them were designed to infect Android smartphone. By design, Android smartphone is secured by using permission scenario. When a malware tries to steal and modify the data in the smartphone but there is no granted permission accepted by the Android user at the first-time of APK installation, the activity will be denied. Unfortunately, based on a survey of 308 Android users, only 3% were aware of installing an APK with dangerous Android permission could lead to the data theft. This research defines the risk severity level of a malware based on the dangerous permission (probability) and the data theft (impact). As the result, in 300 of 10 malware families from DREBIN malware collection, 34 malware were defined as High risk, 114 as Medium risk and 152 as Low risk severity level.

Keywords: Smartphone, Android Permission, Malware, Data Theft, Risk Severity.

DEDICATION

I dedicate this thesis work to all of the Android users. By understanding the risk of Android malware, hopefully it would increase the security awareness of potentially data theft as the impact of installing an APK with dangerous permissions.

ACKNOWLEDGEMENTS

In the Name of Allah, the Most Gracious, the Most Merciful, and peace be upon Muhammad His servant and messenger.

I am grateful to many people, who worked hard with me from the beginning until the completion of this present thesis research.

I would like to deliver my sincere gratitude to my advisor, Pak Mulya R. Mashudi, and my co-advisor,Pak Charles Lim, for the limitless support and limitless time during my thesis research, for their patience, motivation, and immense knowledge. Their wisely and superb guidance help me in all the time of research and writing of this thesis and related researches.

I would like to thank the thesis committee and also my upstanding lecturers, Pak Amin, for the optimistic support, Pak Lukas, for the way of thinking, and Pak Benfano, for the constructive support and challenge me in completing this thesis on-time.

I would like to thank the Thomas Patzke, for the WASE contribution and fastest respond during my lab experiment.

I would like to express my wholehearted thanks to my family for their generous support throughout my entire life. Because of their unconditional love and prayers, I have the chance to complete my master degree.

I owe profound gratitude to my wife, Nurmayulis, whose constant encouragement, limitless giving and great sacrifice through the process of pursuing this master degree.

I am very appreciative to my colleagues of batch 16th, you all are fabulous and excellent.

Last but not least, deepest thanks go to all people who took part in making this thesis real.

TABLE OF CONTENTS

Pages

STATEMENT BY THE AUTHOR 2

ABSTRACT 3

DEDICATION 5

ACKNOWLEDGEMENTS 6

TABLE OF CONTENTS 7

LIST OF FIGURES 12

LIST OF TABLES 15

CHAPTER 1– INTRODUCTION 18

1.1. Background 18

1.2. Research Problems 20

1.3. Research Objectives 21

1.4. Research Questions 21

1.5. Significance of Study 22

1.6. Scope of Study 22

1.6.1 Protocol Analysis 22

1.6.2 Malware dataset 22

1.6.3 Execution Time 22

1.7 Hypothesis 22

1.8 Thesis Structure 23

CHAPTER 2 – LITERATURE REVIEW 24

2.1 Android Architecture 24

2.1.1 Overview of an Android Architecture 24

2.1.2 Overview of an APK Anatomy 26

2.2 Android Permission Model 26

2.2.1 Introduction 26

2.2.2 Android Dangerous Permissions 27

2.3 Smartphone Malware 30

2.3.1 Introduction 30

2.3.2 Types of Smartphone Malware and Malware Families 31

2.4 Theory of Data Theft 35

2.4.1 Types of Data Stored in Smartphone 35

2.4.2 Confidential, Sensitive and Private Data in Smartphone 39

2.4.3 Data Theft in Smartphone 43

2.5 Attribute Extraction: Theory of Android Reverse Engineering 45

2.5.1 Reversing an APK 45

2.5.2 Android Application Activity Lifecycles 46

2.6 Log Collection: Theory of Traffic Data Analysis for Smartphone 47

2.6.1 Introduction 47

2.6.2 Traffic Data Interception in Smartphone 48

2.7 Theory of Risk Scoring and Risk Categorization 50

2.7.1 Risk Formula 50

2.8 Risk Severity Categorization 54

2.9 Relevant Previous Research 56

2.10 State of the Art 57

2.11 Theoretical Framework 58

CHAPTER 3 – RESEARCH METHODOLOGY 59

3.1 Overview 59

3.2 Framework of the Methodology 59
3.3 Framework Combinations 60
3.4 Feature Extraction 61
3.4.1 Android Reverse Engineering 61
3.4.2 Traffic Interception, SSL Certificate Authority and Log Parsing 62
3.5 Risk, Severity Level and Risk Matrix 63
3.5.1 Risk 63
3.5.2 Risk Matrix and Risk Severity Level 65
3.5.3 Proposed Risk Formula 66
3.5.3.3 Risk Severity Level 67
3.5.4 Case Study 67
CHAPTER 4 – RESULT AND ANALYSIS 70
4.1 Virtualized Environment Preparation 70
4.1.1 Lab Setup 70
4.1.2 Dummy Data Preparation 72
4.1.3 Lab Testing Result 73
4.1.4 Malware Dataset 74
4.1.5 Permission Extraction and Traffic Data Log Collection Timeframe 75
4.2 Attributes Extraction 76
4.2.1 Reverse Engineering: Extracting Permissions of Android Malware 76
4.2.2 Traffic Log Collection: Data Theft 83
4.3 Risk Severity Level 86
4.3.1 Probability Score 86
4.3.2 Asset Impact 94
4.3.2.1 BaseBride Malware Asset Impact 94

4.3.2.2 DroidKungFu Malware Asset Impact 94

4.3.2.3 FakeDoc Malware Asset Impact 94

4.3.2.4 FakeInstaller Malware Asset Impact 95

4.3.2.5 Geinimi Malware Asset Impact 95

4.3.2.6 GingerMaster Malware Asset Impact 95

4.3.2.7 Iconosys Malware Asset Impact 95

4.3.2.8 Kmin Malware Asset Impact 95

4.3.2.9 OpFake Malware Asset Impact 96

4.3.2.10 Plankton Malware Asset Impact 96

4.3.3 Risk Severity Level Comparison 96

4.4 Analysis of Highest Score Malware from the Asset Impact 97

4.5 Discussion 99

CHAPTER 5 CONCLUSIONS & RECOMMENDATION 101

5.1 Accomplishment 101

5.2 Conclusion 101

5.3 Recommendation to the Development of Android Security 102

5.3.1 People 102

5.3.2 Process 102

5.3.3 Technology 102

5.4 Limitation 103

5.4.2 Protocol Limitation 103

5.5 Future Works 103

5.5.1 Source Code Analysis and Obfuscation 103

5.5.2 Encryption 103

5.5.3 Certificate Pinning 106

5.5.4 Updated Malware Dataset 106

GLOSSARY 107

REFERENCES 108

APPENDIX 116

Appendix A 116

Dummy Data - Phonebook 116

Dummy Data – Emails 117

Lab Initial Experiment: 120

Appendix B 121

Analyzed Malware Lists 121

Appendix C 130

Complete Probability Score Result 130

Appendix D 141

Risk Severity Result 141