LOCATION AWARE SECURITY SYSTEM FOR MOBILE DEVICES

Dinusha Nivanthaka Amerasinghe

(118201P)

Thesis submitted in partial fulfillment of the requirements for the degree Master of Science

Department of Computer Science & Engineering

University of Moratuwa

Sri Lanka

May 2015

LOCATION AWARE SECURITY SYSTEM FOR MOBILE DEVICES

Dinusha Nivanthaka Amerasinghe

(118201P)

Thesis submitted in partial fulfillment of the requirements for the degree Master of Science

Department of Computer Science & Engineering

University of Moratuwa

Sri Lanka

May 2015

DECLARATION

I declare that this is my own work and this thesis does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my thesis/dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

Signature: …… Date: ……..

Name: D.N. Amerasinghe

Index No: 118201p

I certify that the declaration above by the candidate is true to the best of my knowledge and that this report is acceptable for evaluation for the CS6998 M.Sc. Research Project.

Signature of the supervisor: ……. Date: ……..

Name: Dr. Malaka Walpola

ABSTRACT

Smart phones and related mobile computing device usage is increasing exponentially. Prices of these devices are going down, making them attractive to a larger audience. People tend to prefer mobile computing devices since due to their inherent facilitation of mobility, advanced features, connectivity etc. These devices make the possibility of ubiquitous computing a reality. As discussed in this report there are evidence that mobile computing devices are actually a convergence of various discrete devices such as GPS Receivers, Personal Digital assistants (PDA's) etc. These devices have their own pros and cons compared with traditional computing devices. One of the main shortcomings of technology for these devices is security, due to the inherent mobile nature of these devices, the security controls that apply to PC's aren't suitable for these types of devices. Malware targeting mobile devices are very complex, they tend to exploit a number of shortcomings of these devices. The currently available technology has shortcomings on addressing these security requirements. Furthermore current malware detection technology is new and evolving. Traditional approaches such as a virus scanners doesn't work in these environments due to power, processing and other constraints.

This report analyses the approaches available to implement a location context aware security solution. An analysis of current research in this area is conducted. Several implementations of different malware detection systems, security policy management systems and location context aware systems are discussed in order to evaluate their feasibility of approach and effectiveness of the solutions. Furthermore our analysis includes the discussion of current malware behavior in the Smartphone base. Android is chosen as the platform for the implementation since it is widely deployed on many Smartphone and other mobile computing devices. Other platforms such as Apple iOS, Symbian and Blackberry features similar architectures and hence the concept discussed in this report applies to those platforms as well.

In this report we analyze the feasibility of implementing a middleware based approach to provide a location context aware security solution. In order to select the appropriate approach several malware detection methods were analyzed.

ACKNOWLEDGMENTS

I take this opportunity to express my sincere gratitude to my supervisor, Dr. Malaka Walpola, for his invaluable thoughts, encouragement, supervision and guidance throughout this research work. He offered his generous guidance every time I reached him even during his busy time schedules.

Further, I use this opportunity to thank my MSc lecturers who guided me throughout my MSc (Computer Science) course and shared their valuable knowledge with dedication.

Finally, I express my gratitude to my parents and my friends for the support and encouragement throughout my life to bring me up to this level.

TABLE OF CONTENTS

Abstract i

List of Figures vi

List of Tables vii

Chapter 1 - Introduction 1

1.1 Background 1

1.2 Problem Domain 2

1.3 Objectives 2

1.4 Proposed Solution 4

1.5 Overview of the Dissertation 4

Chapter 2 - Literature Review 6

2.1 Introduction 6

2.2 Context Aware Systems 6

2.3 Context Aware Security Systems for Mobile Devices 8

2.3 Security Models of Smartphone Platforms 11

2.4 Security Mechanisms for Android Mobile Devices 18

2.4.1 Security Refinements of Android SDK 25

2.5 Threat Models and Malware for Mobile Devices 27

2.6 Malware Detection Techniques for Mobile Devices 31

2.6.1 Detection in Mobile Device Only 31

2.6.2 Detection at a Separate Server 35

Chapter 3 - Design and Implementation 37

3.1 The Proposed Software Architecture 37

3.1.1 The Server 39

3.1.2 The Client 39

3.2 The Implemented Solution 40

3.3 The Client Software 41

3.3.1 Main Activities 41

3.3.2 Class Structure 45

3.3.3 Data Storage 46

3.3.4 The Background Service 47

3.3.5 Location based Security Policy Management 47

3.3.6 Application Security Audit 48
3.3.7 Communication Method 48
3.3.8 The Strace Utility 48
3.3.9 The Client Software User Interfaces 49
3.3.10 Background Services 49
3.3.11 App Tracing 50
3.3.12 Location Services 50
3.3.13 App Security 50
3.4 The Server Software 51
3.4.1 Data Storage 53
3.4.2 Behavior Rule format 53
CHAPTER 4 - Testing and Results 54
4.1 Malware Behavior Rules 54
4.2 Location Rules 56
4.3 Results 58
4.3.1 Malware Detection System 58
4.3.2 Location Aware Security System 59
CHAPTER 5 - Conclusions and Future Work 62
References 64

LIST OF FIGURES

Figure 2.1: Location based Architecture (Source: Ardagna et al. [12]) 8
Figure 2.2 - L4Android Architecture. (Source: M Lange [19]) 16
Figure 2.3 - Hosted hypervisor and baremetal hypervisor. (Source: Gudeth et al. [20]) 17
Figure 2.4: Android usage control framework (Source: Bai et al. [21]) 19
Figure 2.5 : Overhead of running ConUCON. (Source: Bai et al. [21]) 20
Figure 2.6: Multi-level approach for performance efficient taint tracking within a common smartphone architecture. (Source: Enck et. al. [25]) 25
Figure 2.7 - "Andromaly" framework overview. (Source: Shabtai et al. [28]) 32
Figure 2.8 - "Crowdid" Framework Overview. (Source: I Burguera and S Nadjm-Tehrani [29]) 36
Figure 3.1 - The proposed architecture of the "AndroSec" system 38
Figure 3.2 - Activity diagram for location context detection in the client 42
Figure 3.3 - Activity diagram for application log/trace collection in the client 43
Figure 3.4 - Activity diagram for application log upload to a remote server from the client 44
Figure 3.5 - Class diagrams of main classes 46
Figure 3.6 - Entity Relationship(ER) diagram of client database 47
Figure 3.7 - Pseudo code for location based security policy management 47
Figure 3.8 - Pseudo code for application security audit 48
Figure 3.9 - Application home screen 49
Figure 3.10 - Application system call trace collection 50
Figure 3.11 - Application interfaces 51
Figure 3.12 - Pseudo code for application security audit 52
Figure 3.13 - Server application trace processing 52
Figure 3.14 - Entity Relationship(ER) Diagram of Server Database 53

LIST OF TABLES

Table 2.1 : Examples of access control rules regulating access to a mobile network console. (Source: Ardagna et al. [12]) 9
Table 2.2: Smart phone permission modes. (Source: Kathy Au et al. [9]) 14
Table 2.3: Applications with duplicate permissions by market category. (Source: Vidas et al. [23]) 22
Table 2.4: Top ten duplicate permissions requested. (Source: Vidas et al. [23]) 23
Table 2.5: Malwares and their methods of infection. (Source: La Polla et al. [32]).. 28
Table 3.1: Behavior rule format 53
Table 4.1: Malware detection rules list 55
Table 4.2: Location Rules List 56
Table 4.3: Cumulative score for malware behaviors 58
Table 4.4: Results for real applications 60