UNIVERSITI TEKNOLOGI MALAYSIA

DECLARATION OF THESIS / UNDERGRADUATE PROJECT PAPER AND COPYRIGHT

Author's full name : AHMED A. SABEEH
Date of birth : 2nd October 1985
Title : AN APPROACH TO ENHANCE SECURITY AWARENESS ON THE USE OF MOBILE DEVICES

Academic Session : 2010 / 2011

I declare that this thesis is classified as:

☐ CONFIDENTIAL  (Contains confidential information under the Official Secret Act 1972)*
☐ RESTRICTED  (Contains restricted information as specified by the organization where research was done)*
☐ OPEN ACCESS  I agree that my thesis to be published as online open access (full text)

I acknowledged that Universiti Teknologi Malaysia reserves the right as follows:

1. The thesis is the property of Universiti Teknologi Malaysia.
2. The Library of Universiti Teknologi Malaysia has the right to make copies for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by :

(SIGNATURE)

ASSOC. PROF. DR. MASLIN MASROM
(NAME OF SUPERVISOR)

G1214390
(NEW IC NO. / PASSPORT NO.)

Date : 2 December 2010

NOTES :  * If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization with period and reasons for confidentiality or restriction.
SUPERVISOR’S DECLARATION

“I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in terms of scope and quality for the award of the degree of Master of Computer Science (Information Security)”

Signature: [Signature]
Name of Supervisor: ASSOC. PROF. DR. MASLIN MASROM
Date: DECEMBER 2010
AN APPROACH TO ENHANCE SECURITY AWARENESS ON THE USE OF MOBILE DEVICES

AHMED A. SABEEH

A project report submitted in partial fulfilment of the requirements for the award of the degree of Master of Computer Science (Information Security)

Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

DECEMBER 2010
I declare that this thesis entitled "An Approach to Enhance Security Awareness on the Use of Mobile Devices" is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : [Signature]
Name : AHMED A. SABEEH
Date : DECEMBER 2010
Dedicated to my dear parents, my beloved fiancée, and my brothers and sister with thanks for all the endless support and encouragement
ACKNOWLEDGEMENT

I sincerely give gratitude to my supervisor, Associate Professor Dr. Maslin Masrom, for her support throughout the project, her patience and for allowing me to work in my own way. Her wide knowledge and her logical way of thinking have been of great value to me. Her understanding, encouraging and personal guidance have provided a good basis for this thesis.

I would like to give my special thanks to the Dean of the Advanced Informatics School (UTM AIS), Prof. Dr. Shamsul Sahibuddin and coordinator of Master of Information Security, Dr. Rabiah Ahmad and all the lecturers in for their encouragement and insightful comments. I also appreciate all the contributions of the staff who responded promptly to all the urgent requests I made. I also would like to thank Assoc. Prof. Dr. Nathan Clarke for his help and support to achieve the goal of my study.

My deepest gratitude goes to my parents for their unflagging love and endless support throughout my life. I am indebted to my father, for his understanding, endless patience, support and encouragement when it was most required. I would like to appreciate the support that my fiancée had given me throughout my studies which was a major leap towards my success.

Finally, I would like to thank everybody who supported me in completion of the thesis, as well as expressing my apology for not being able mention each and everyone personally.
ABSTRACT

The rapid development of mobile devices technology has turned them into real contenders and serious replacements for personal computers. On the other hand, this development has raised the number of attacks and security risks associated with the use of mobile devices. Mobile devices lack adequate protection in addition to the misuse of end-users. This study proposes a mobile devices security users’ security awareness framework. The framework was built based on an intensive review to security issues related to mobile devices, as well as the security awareness level among users. The framework consists of four variables namely; security knowledge, internet and services, privacy and updates and users’ attitudes. The data was collected through a quantitative method. The study has involved textual data and a survey questionnaire. The survey questionnaire was conducted in (UTM International Campus) including both students and staff as respondents in a try to reach a various number of mobile users. The results of this questionnaire came in contact with what was found in previous studies and indicated a significant weakness in users’ security awareness regarding mobile devices. Furthermore, the current security countermeasure, if found are not widely deployed due to the inconvenience they cause. The study has concluded that developing countermeasures alone without training users might not produce the secure environment required. This highlight security awareness and training as important factors to increase mobile devices’ security. Further work is necessary to develop practical guidelines in contact with NIST SP800-124 user oriented measures.
ABSTRAK

## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DECLARATION</td>
<td></td>
<td>ii</td>
</tr>
<tr>
<td>DEDICATION</td>
<td></td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENT</td>
<td></td>
<td>iv</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td></td>
<td>v</td>
</tr>
<tr>
<td>ABSTRAK</td>
<td></td>
<td>vi</td>
</tr>
<tr>
<td>TABLE OF CONTENTS</td>
<td></td>
<td>vii</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td></td>
<td>xi</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td></td>
<td>xii</td>
</tr>
<tr>
<td>LIST OF APPENDICES</td>
<td></td>
<td>xiii</td>
</tr>
</tbody>
</table>

1 INTRODUCTION 1
1.1 Introduction 2
1.2 Problem Background 2
1.3 Problem Statement 4
1.4 Research Questions 6
1.5 Project Aim 6
1.6 Project Objectives 6
1.7 Project Scope 6
1.8 Significance of the Study 7
1.9 Summary 7

2 LITERATURE REVIEW 8
2.1 Introduction 8
2.2 Security Threats Associated With Mobile Phones 8
   2.2.1 Mobile Malware 10
   2.2.2 Mobile Backdoor Trojans, DOS and Other Attacks 16
2.2.3 Mobile Malware New Technologies
2.2.4 What Makes Mobile Malware A Threat?
2.2.5 Mobile Phone Security Threats
Countermeasures
2.3 Mobile Devices User’s Security Awareness
2.4 A Review for Mobile Security Related Studies
2.5 Summary

3 METHODOLOGY
3.1 Introduction
3.2 Research Methodology
3.3 Observation, Definitions of the Measured Parameters
3.4 Literature Review
3.5 Research Philosophy
3.5.1 Qualitative Research
3.5.2 Quantitative Research
3.6 Research Purpose Types
3.6.1 Explanatory
3.6.2 Experimental
3.6.3 Descriptive
3.7 Research Strategy
3.7.1 Data Gathering
3.7.1.1 Data Collection method
3.7.2 Questionnaire Method
3.7.3 Sampling method
3.8 Data Analysis
3.8.1 Descriptive Analysis
3.8.2 Inferential Analysis
3.9 Validation of Research Framework
3.10 Research Plan and Schedule
3.11 Summary

4 RESEARCH FRAMEWORK
4.1 Introduction
4.2 The Hypothetical Model
4.3 Proposed Research Framework
ANALYSIS AND RESULTS

5

5.1 Introduction

5.2 Questionnaire
- 5.2.1 Population and Sample
- 5.2.2 Objectives of the Questionnaire
- 5.2.3 Fact Finding Analysis
  - 5.2.3.1 Demographics
  - 5.2.3.2 Security Knowledge
  - 5.2.3.3 Internet and Services
  - 5.2.3.4 Privacy and Updates
  - 5.2.3.5 Awareness
  - 5.2.3.6 Attitudes
- 5.2.4 Inferential Analysis Regarding Gender, Education, and Age
- 5.3 Summary

DISCUSSION AND CONCLUSION

6

6.1 Introduction

6.2 Discussion of Research
- 6.2.1 Mobile Security Knowledge
- 6.2.2 Internet and Mobile Services
- 6.2.3 Privacy and Updates
- 6.2.4 Attitudes and Awareness

6.3 NIST SP800-124 User Oriented Measures
- 6.3.1 Maintain Physical Control
- 6.3.2 Enable User Authentication
- 6.3.3 Backup Data
- 6.3.4 Reduce Data Exposure
- 6.3.5 Shun Questionable Actions
- 6.3.6 Curb Wireless Interfaces
- 6.3.7 Minimize Functionality
- 6.3.8 Add Prevention and Detection Software

6.4 Contribution of Research

6.5 Limitations and Future Work
6.6 Concluding Remarks

REFERENCES

Appendices A-B
# LIST OF TABLES

<table>
<thead>
<tr>
<th>TABLE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Summary for The Reviewed Mobile Security Related Studies</td>
<td>38</td>
</tr>
<tr>
<td>2.2</td>
<td>Research Approaches for Solving the Research Questions</td>
<td>41</td>
</tr>
<tr>
<td>3.1</td>
<td>Questionnaire Dimensions</td>
<td>54</td>
</tr>
<tr>
<td>5.1</td>
<td>Profile of Questionnaire Respondents</td>
<td>74</td>
</tr>
<tr>
<td>5.2</td>
<td>Respondents’ Attitude towards Current and Future Security</td>
<td>88</td>
</tr>
</tbody>
</table>
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>FIGURE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Cabir Requesting a User for Installation</td>
<td>10</td>
</tr>
<tr>
<td>2.2</td>
<td>Langganan Telefon Selular / Cellular Phones Subscription</td>
<td>12</td>
</tr>
<tr>
<td>2.3</td>
<td>Growth in Number of Known Modifications (2004–2009)</td>
<td>14</td>
</tr>
<tr>
<td>2.4</td>
<td>Number of New Modifications Per Month (2004–2009)</td>
<td>14</td>
</tr>
<tr>
<td>2.5</td>
<td>Distribution of Mobile Malware Across Platforms</td>
<td>15</td>
</tr>
<tr>
<td>2.6</td>
<td>Trojan-SMS.Python.Flocker Modification</td>
<td>20</td>
</tr>
<tr>
<td>3.1</td>
<td>Questionnaire Flowchart</td>
<td>57</td>
</tr>
<tr>
<td>3.2</td>
<td>Operational Framework</td>
<td>63</td>
</tr>
<tr>
<td>4.1</td>
<td>Hypothetical Model</td>
<td>67</td>
</tr>
<tr>
<td>4.2</td>
<td>Proposed Research Framework</td>
<td>70</td>
</tr>
<tr>
<td>5.1</td>
<td>Manufacturers of Respondents Devices</td>
<td>76</td>
</tr>
<tr>
<td>5.2</td>
<td>Service in Use by Mobile Devices Users</td>
<td>77</td>
</tr>
<tr>
<td>5.3</td>
<td>Respondents’ Opinions About if Their Devices Requires Security</td>
<td>79</td>
</tr>
<tr>
<td>5.4</td>
<td>Respondents’ Internet Services in Use</td>
<td>80</td>
</tr>
<tr>
<td>5.5</td>
<td>Bluetooth Usage Pattern for Respondents</td>
<td>81</td>
</tr>
<tr>
<td>5.6</td>
<td>Respondents Answers for Update Frequency</td>
<td>82</td>
</tr>
<tr>
<td>5.7</td>
<td>Users’ Response if They Save Credit Card Number with No Encryption</td>
<td>84</td>
</tr>
<tr>
<td>5.8</td>
<td>Respondents’ PIN use Pattern</td>
<td>85</td>
</tr>
<tr>
<td>5.9</td>
<td>Respondents’ Invalidation for PIN</td>
<td>86</td>
</tr>
<tr>
<td>5.10</td>
<td>Respondents’ Opinions if PIN Provides Adequate Security</td>
<td>87</td>
</tr>
</tbody>
</table>
# LIST OF APPENDICES

<table>
<thead>
<tr>
<th>APPENDIX</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Project Schedule</td>
<td>116</td>
</tr>
<tr>
<td>B</td>
<td>Questionnaire Sample</td>
<td>117</td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION

Today’s information and communication revolution is growing beyond everyone’s imagination. If we take a quick look back at ourselves in ten years old pictures, we will find a huge difference in the way the picture was taken. However, the way that the digital world is changing brings fears in return to the concept of information security (Confidentiality, Integrity, and Availability) which is emerging side by side with technology.

This information and communication revolution was raised up by a very important invention which is the mobile phone. Nowadays, mobile phone is accompanying us in every single task we do no matter where we are, it is simply connecting us to the world by calls, SMS, and internet services.

Mobile devices can perform many tasks that were performed only by the PC before; they now have internet browsers, games, interactive applications, Wi-Fi and Bluetooth connections, digital cameras, and much more. All these superior capabilities are ruined by security breaches being exploited by malicious attackers which transfer that beneficial device to a big loss once stolen or fall under data theft and information confidentiality to be compromised by viruses which means losing important data.

Nevertheless, by considering the importance of mobile devices and the importance of user actions in protecting all information resources around, the
security awareness is a very big step in achieving a secure environment, having said that, this study is to develop a guideline for mobile phone users to enhance the security awareness based on investigating the security awareness level of mobile phones usage between users. The study will concentrate on users’ security awareness regarding the common security threats associated with using mobile phones. This research is directed towards mobile phones users’ and service providers.

Introduction

This chapter describes the entrance to the study by highlighting the major plans to be taken to complete the research. The chapter will address the problem background of this project, followed by the problem statements, research questions, objectives, scopes, aim and the significance of the study.

Problem Background

Mobile phones particularly have a rapid influence on users; users got so many facilities through the mobile phones. Mobile phones currently are not for adults only but for children as well due to the ease of use and the reasonable price. These devices are not dedicated only for making and receiving calls but to send text messages, listen to music, surf the internet, play videos and even play mobile games.

Moreover, mobile phones are engaged more in e-banking, e-commerce, online shopping and many other applications which pose the threat of social issues like information security, privacy violation, hacking and many others.

However, probably no means of communication has revolutionized the daily lives of ordinary people more than the telephone. The actual history of the telephone is a subject of complex dispute. The controversy began with the success of the
invention and continues today. Some of the inventors credited with inventing the telephone include Antonio Meucci, Philip Reis, Elisha Gray and Alexander Graham Bell. Bell's experiments with his assistant Thomas Watson finally proved successful on March 10, 1876, when the first complete sentence was transmitted: "Watson, come here; I want you." (Ament, 2007).

Later on, public mobile telephone history begins in the 1940s after World War II. Although primitive mobile telephones existed before the War, these were specially converted two way radios used by government or industry, with calls patched manually into the landline telephone network, but only since 1995 have mobiles become low cost, rich in features, and used worldwide (Farley, 2005).

Mobile devices and phones security has grown as a major concern for organizations. Because of their small size, memory capability, and the ease with which information can be downloaded and removed from a facility, Wi-Fi and Bluetooth connections, mobile devices pose a risk to organizations when used and transported outside physical boundaries (Halpert, 2004).

According to the Russian antivirus firm Kaspersky Lab, Mobile phones have become the focus of attacks by virus writers and hackers (Hancock, 2000). Since mobile phones offer users the same capabilities as PCs, they also offer the same ‘rewards’ for the criminal underground. The relative lull in numbers of new malicious programs for mobile phones during the last few years is unlikely to mean a decline in mobile malware. On the contrary, the increasing complexity of smart phones, coupled with the widening market for these devices will certainly bring in its wake further mobile malware, particularly ‘crimeware’ programs written by professional malware writers and used by the criminal underground to make money (Emm, 2006).

Furthermore, security experts are finding a growing number of viruses, worms, and Trojan horses that target mobile phones describing the common approaches as SMS and MMS services as well as E-mail services, while vendors of
phones and mobile operating systems are still looking for ways to improve security (Leavitt, 2005a).

If we narrow it down, the main target recently are the smart phones, they are becoming increasingly popular. Offering Internet connectivity, they function like minicomputers and can download a growing variety of applications and files, store personal information such as credit card numbers, and even conduct financial transactions. Moreover, studies show that about 90 different types of viruses, worms, and Trojan horses were targeting smart phones in 2005 (Leavitt, 2005b), in addition to recent news that New instances of ‘SMiShing’ have been detected in Europe that target smart phone users, which is an attack using a SMS faking a YouTube link (Raywood, 2009).

It is obvious from what have been stated above that the efforts of the mobile phone vendors as well as the antivirus companies are not a sufficient cure for the mobile security, but users’ awareness plays a massive role in protecting private data that might cause users a financial or social loss. According to the 2009 Mobile Security Survey by Goode Intelligence and Acumin Consulting, 89 per cent of security professionals have doubts about mobile phone security and only 11 per cent of security professionals feel that the current level of awareness for mobile phone security is adequate, while 46 per cent of surveyed organizations do not have a specific security policy for mobile phones (SC, 2009a). Therefore, this research will focus on identifying the current security awareness among mobile phones users’ in Kuala Lumpur and the required measurements to be taken to reach a secure level and an optimum operation of mobile phones.

**Problem Statement**

Mobile phones users’ are facing several security threats that mainly attack the privacy of those users, one public example was shown in the recent Black Hat security conference in Las Vegas which demonstrate how researches can easily hack
an iPhone using a SMS that gives a complete control for the phone’s content like pictures, music, credit card numbers and more as well as handing a full control to send text messages and even making a call (Mills, 2009).

Such news will pose a real danger against mobile banking and internet e-banking transactions; a real life pattern would be a hacker controlling your mobile phone during any transaction made using (Cimbclicks) internet banking website for instance, and while you are prepared to receive the Transaction Authorization Code (TAC) to confirm the transaction, the hacker can read it and may have a control over all your banking activities and account details.

As the survey by Goode Intelligence and Acumin Consulting stated above (SC, 2009a) and a further look at another survey for mobile users in the UK tells that Nine out of ten smart phone users in the UK do not secure their devices against online crime and data theft. However, the problem does not stop there but the same study confirms that over half of the respondents (54 per cent) admitted to submitting their credit card details via their smart phones to purchase or download items online on the move over the last three months of the study (SC, 2009b). That is showing clearly that users are not aware enough to the danger of misusing their devices.

Considering all the above facts, users’ awareness is undoubtedly a major factor of mobile phones security. Therefore, this research aims to question if the users have enough security awareness regarding the usage of mobile phones and its services, the vendors are equipping their devices with sufficient security measures for secure usage, the service providers are warning users about current threats or advising them for an optimum usage, and if the e-banking facilities have good defense measurements to protect their clients against possible breaches like the above mentioned.
Research Questions

What are the potential risks associated with mobile phone usage?
Can security awareness enhance mobile device usage security?
What is the security awareness level among mobile device users?

Project Aim

The aim of this study is to develop a framework for mobile phones awareness that focus on the security factor of using mobile phones.

Project Objectives

The objectives of this study will be as follows:

1. To investigate the security awareness framework components through mobile security threats assessment.
2. To propose and develop a framework for enhancing mobile phone security awareness for mobile phones users’ and service providers.
3. To evaluate and validate the developed framework.

Project Scope

For the purpose of completing this project, a quantitative method will be used. Unit of analysis for this study are mobile phones users. Variant mobile phones users’ as population sample which are located at Kuala Lumpur (UTM International Campus) are selected for this study.
Significance of the Study

Mobile phone malwares were first identified in the year of 2000. And since then there was not adequate researches to observe and follow their development and consequences in both technical and non technical aspects (Leavitt, 2005a).

Moreover, the mobile phone security awareness is an emerging need, since mobile phones are growing technically to replace computers which affect the social part regarding protecting users’ data and privacy (Leavitt, 2005b). In addition, the person who does not own and mobile phone nowadays can be considered as ‘unique’ (Fogie, 2005). Therefore, enhancing users’ security awareness to use their mobile phones has a major role in today’s information security study.

1.9 Summary

In this chapter, we discussed a brief view of the research, starting from presenting the fundamental concepts of the mobile phones usage moving towards the problem that we would like this research to address then, highlighting the objectives to be carried out later on in this research. Mobile phones awareness issues are promising to researchers in the field of information security in Malaysia’s environment. And since there is a lack of study about it, this study will provide a good opportunity to enhance mobile phones users’ awareness in Malaysia.
REFERENCES


SC Staff. (2010). Deployment of mobile security software is on the agenda for more than half of companies this year, SC magazine, January 07, 2010, from http://www.scmagazineuk.com/deployment-of-mobile-security-software-is-on-the-agenda-for-more-than-half-of-companies-this-year/article/160792/.


