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)

(SIGNATURE OF SUPERVISOR)

G1214390
(NEW IC NO. / PASSPORT NO.)

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

Date : 2 December 2010

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 : 

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 : 
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

Perkembangan teknologi peranti mudah-alih yang pesat telah mengubah mereka menjadi pesaing dan pengganti serius untuk komputer peribadi. Di sisi yang lain pula, perkembangan ini telah meningkatkan kadar serangan dan risiko keselamatan yang berkaitan dengan penggunaan peranti mudah-alih. Peranti mudah-alih kurang perlindungan yang mencukupi di samping penyalahgunaan oleh pengguna akhir. Kajian ini mencadangkan satu kerangka kesedaran keselamatan pengguna bagi keselamatan peranti mudah-alih. Kerangka ini dibina berdasarkan satu penelahan intensif terhadap isu keselamatan yang berkaitan dengan peranti mudah-alih, serta tahap kesedaran keselamatan antara pengguna. Kerangka ini terdiri daripada empat pembolehubah iaitu; pengetahuan dalam keselamatan, internet dan perkhidmatan, privasi dan pengemaskinian, dan sikap pengguna. Data-data telah dikumpulkan melalui kaedah kuantitatif. Kajian ini telah melibatkan data tekstual dan tinjauan kaji selidik. Tinjauan kaji selidik ini telah dijalankan di (UTM International Campus) termasuk pelajar-pelajar dan staf-staf sebagai responden dalam percubaan untuk mendapatkan sejumlah pengguna peranti mudah-alih. Keputusan kaji selidik ini sejajar dengan apa yang telah ditemui dalam kajian sebelumnya dan menunjukkan kelemahan yang ketara dalam kesedaran keselamatan pengguna terhadap peranti mudah-alih. Tambahan pula, pencegahan keselamatan yang sedia ada, jika ditemui adalah tidak banyak digunakan disebabkan ketidakselesaan yang ditimbulkan. Kajian ini telah merumuskan bahawa dengan membangunkan tindakan pencegahan sahaja tanpa melatih pengguna mungkin tidak akan menghasilkan persekitaran keselamatan yang diperlukan. Ini menunjukkan bahawa kesedaran keselamatan dan latihan merupakan faktor penting untuk meningkatkan keselamatan peranti mudah-alih. Kajian lebih lanjut adalah diperlukan untuk membangunkan garis panduan praktikal dengan NIST SP800-124 berorientasikan tahap pengguna.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

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

Ackoff, R. (1953). *The Design of Social Research*. Chicago: University of Chicago Press.

Ament, P. (2007). Telephone history – invention of the telephone. Ideafinder, retrieved on January 19, 2010, from http://www.ideafinder.com/history/inventions/telephone.htm.

Bazeley, P. (2003). Teaching mixed methods. *Research Journal*. Special Issue 2003. 117-126.

Blackwell, C. (2008). A multi-layered security architecture for modeling complex systems. *Proc ACM CSIIRW, 288*.

Breckler, S. J., & Wiggins, E. C. (1992). On defining attitude and attitude theory: Once more with feeling. In A. R. Pratkanis, S. J. Breckler, & A. C. Greenwald (Eds.), Attitude structure and function. Hillsdale, NJ: Erlbaum. pp. 407–427.

Brehob, K. (2001). Usability Glossary,. from http://www.usabilityfirst.com,

Burgess, T. F. (2001). *Information Systems Services Guide to the Design of Questionnaires: A general introduction to the design of questionnaires for survey research* (1.1 ed.): University Of Leeds Edition.

Clarke, N. and Furnell, S. (2005). "Authentication of users on mobile telephones – A survey of attitudes and practices". Computers & Security, vol. 24, no. 7, pp519-527.

Clarke, N.L., Furnell, S.M., Rodwell, P.M., and Reynolds, P.L. (2002). "Acceptance of subscriber authentication methods for mobile telephony devices". *Computers & Security*, vol. 21, no.3, pp220-228.

Creswell, J. W. (1994). Research Design: Qualitative and Quantitative Approaches *ScienceDirect*, 228.

Creswell, J. W. (2003). *Research Design: Qualitative, Quantitative, and Mixed Method Approaches*. (2nd ed.). Thousand Oaks, CA: Sage Publications.

Croom, S. (2002). Methodology Editorial, Special issue on research methodology in operations management. *International Journal of Operations and Production Management.* Volume 22 (2): 148-151.

Dodge, Y. (2003) The Oxford Dictionary of Statistical Terms, OUP. ISBN 0-19-850994-4.

Dwan, B. (2004). The mobile phone virus. Network Security, Volume 2004, Issue 7, July 2004, Pages 14-15.

Emm, D. (2006). Mobile malware – new avenues. Network Security, Volume 2006, Issue 11, November 2006, Pages 4-6.

ENISA. (2006). A Users' Guide: How to raise information security awareness (EN). European Network and information Security Agency, Jun 01, 2006, from http://www.enisa.europa.eu/act/ar/deliverables/2006/ar-guide/en

Farley, T. (2005). Mobile telephone history. Telektronikk, 3/4.2005 – 22.

Flick, U. (2006). *An Introduction to Qualitative Research*. (3rd ed). London: Sage Publications Inc.

Fogie, S. [2005]. Security Reference Guide. InformIT, Apr 1, 2005, from http://www.informit.com/guides/content.aspx?g=security&seqNum=92

Furnell, S. (2006). Securing mobile devices: technology and attitude. Network Security,Volume 2006, Issue 8, August 2006, Pages 9-13.

Gostev, A. (2009). Mobile Malware Evolution: An Overview. Viruslist, Sep 29 2009, from http://www.viruslist.com/en/analysis?pubid=204792080

Halpert, B. (2004). Mobile Device Security. InfoSecCD Conference'04, October 8, 2004, Kennesaw, GA, USA, 1-3.

Hancock, B. (2000). Hacker Target: Mobile Phones. Computers & Security, Volume 19, Issue 6, 1 October 2000, Pages 494-495.

Hopkins, W. G. (2000). Quantitative Research Design. SPORTSCIENCE, May 4, 2000, from http://www.sportsci.org/jour/0001/wghdesign.html

Ismail, S., and Hj Yunos, Z. (2005, March 24). Worms and Trojans Go Mobile. *The Star.* Retrieved May 27, 2010, from http://www.cybersecurity.my/data/content_files/13/91.pdf?.diff=1176416843

Jansen, W., and Scarfone, K. (2008). Guidelines on Cell Phone and PDA Security, NIST, Special Publication 800-124, October 2008, from http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

Jargowskya, Paul A., and Yang, R. (2005). Descriptive and Inferential *Statistics. Encyclopedia of Social Measurement*. Pages 659-668.

Kabay, M. E. (2009). Cell phone security, NIST document provides guidelines on cell phone and PDA security. Network world, February 24, 2009, from http://www.networkworld.com/newsletters/sec/2009/022309sec1.html

Karatzouni, S., Furnell, S.M., Clarke, N.L., Botha, R.A. Perceptions of User Authentication on Mobile Devices. *Proceedings of the ISOneWorld Conference*. April 11-13. Las Vegas, USA: CD Proceedings, 2007. (0-9772107-6-6).

Khalil, A., and Connelly, K. (2005). Context-Aware Configuration: A Study on Improving Cell Phone Awareness. Modeling and Using Context. (pp. 197-209). Heidelberg: Springer Berlin.

Kowalski, S., and Goldstein, M. Consumers ' Awareness of, Attitudes Towards and Adoption of Mobile Phone Security. *20th International Symposium on Human Factors in Telecommunication.* 20-23 March, 2006. Sophia-Antipolis, France: HFT.

Lawton, G. (2008). Is It Finally Time to Worry about Mobile Malware?. Computer, Volume 41, Issue 5, May 2008 Pages: 12-14.

Leavitt, N. (2005a). Mobile phones: the next frontier for hackers?. Computer, Volume 38, Issue 4, April 2005 Page(s):20 – 23.

Leavitt, N. (2005b). Will proposed standard make mobile phones more secure?. Computer, Volume 38, Issue 12, Dec. 2005 Page(s):20 – 22.

Malaysian Communications and Multimedia Commission (2005). *Hand Phone Users Survey*. [Statistical Brief]. 63000 Cyberjaya, Selangor Darul Ehsan, Malaysia: the Malaysian Communications and Multimedia Commission.

Mann, P.S. (1995) Introductory Statistics, 2nd Edition, Wiley. ISBN 0-471-31009-3.

Marshall, C. G. B. R. (2006). Designing Qualitative Research, *SAGE Publication*

Marshall, G., and Jonker, L. (2010). An introduction to inferential statistics: A review and practical guide. *Radiography, In Press, Corrected Proof,* Available online 29 January 2010.

Miles, M. B., and Huberman, M. A. (1994). *Qualitative Data Analysis: An Expanded Sourcebook* (2nd ed.). Beverley Hills: Sage.

Mills, E. (2009). Researchers attack my iPhone via SMS. Cnet news, July 29, 2009, from http://news.cnet.com/8301-27080_3-10299378-245.html.

Namayandeh, M. (2009). *Development of Computer Ethical Framework for Information Security (Educational Context).* Master of Computer Science, Universiti Teknologi Malaysia, Kuala Lumpur.

Permatasari, S. (2010). Digi to Sell IPhone in Malaysia, Taking on Maxis. Bloomberg businessweek, February 28, 2010, from http://www.businessweek.com/news/2010-02-28/digi-to-sell-iphone-in-malaysia-taking-on-maxis-update1-.html

Rache, P. (2008). Convenience Samples and Research How Are The Findings? *Gerontologist.* United States. Volume 48: (6). 3-12.

Raywood, D. (2009). New 'SMiShing' spam targets WAP and smartphone users. SC magazine, October 07, 2009, from http://www.scmagazineuk.com/new-smishing-spam-targets-wap-and-smartphone-users/article/151637/.

Richardson, R. (2007). "2007 CSI computer crime and security survey,". In The 12th annual computer crime and security survey: *Computer Security Institute, 2007.*

Sapronov, K. (2006). Bluetooth, Bluetooth Security and New Year War-nibbling. Viruslist, Mar 03 2006, from http://www.viruslist.com/en/analysis?pubid=181198286

SC Staff. (2009a). Confidence in awareness for mobile phone security still at a low ebb. SC magazine, October 21, 2009, from http://www.scmagazineuk.com/confidence-in-awareness-for-mobile-phone-security-still-at-a-low-ebb/article/155835/.

SC Staff. (2009b). Smartphone users fail to secure devices and do not consider the security implications of using them for online shopping, SC magazine, October 05, 2009, from http://www.scmagazineuk.com/smartphone-users-fail-to-secure-devices-and-do-not-consider-the-security-implications-of-using-them-for-online-shopping/article/151472/.

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/

Seaman, C. B. (1999). Qualitative methods in empirical studies of software engineering. *Proc IEEE Transactions on Software Engineering, 25*(4).

Siponen, M. T. (2001). Five dimensions of information security awareness. ACM SIGCAS Computers and Society, Volume 31 , Issue 2 (June 2001) Pages: 24 – 29.

Talib, S., Clarke, N. L., and Furnell, S. M. "An Analysis of Information Security Awareness within Home and Work Environments,". *2010 International Conference on Availability, Reliability and Security*. February 15-18, 2010. Krakow, Poland: IEEE. 2010. ares, pp.196-203.

Yin, R., K. (2003). *Applications of Case Study Research*. Newbury Park: SAGE Publications.

Zikmund, W., G. (2000). *Business research methods-2000*, Australia; Canada: South Western/Thomson Learning.