Applied Human Factors and Ergonomics International

The Heuristic Evaluation Methodology of the Smartphone Operating System on the User preferences and Satisfaction of the Security System

Ryang-Hee Kim and Young-Guk Kwon

Department of Safety Engineering
Seoul National University of Science and Technology
138 KongNung gil, NoWon-Ku, Seoul , ZIP: 139-743, South Korea

ABSTRACT

The aim of this study is to study the smartphone operating system on the user preferences and satisfactions using selected heuristic usability method. In the security operating systems, the first layer of security within a smartphone is at the level of the operating system. Beyond the usual roles of the security operating system on a smartphone, it must also establish the protocols for introducing external applications and data without introducing risk. The security operating system contains important incidents which have greatly influenced development of smartphone security and of their importance today. There has been a leaking of personal information from a major portal site by the hackers. The selected usability principles are classified systematically using paired t-test (two aged groups) selected by Duncan's Multiple Range Test and Principle Components Analysis (PCA) using Factor Analysis. The results are as follows: 25 usability principles for the operating system on the user preferences and satisfaction of the security system are categorized into four groups. According to their correlations and we named them respectively, users' preference and awareness of smartphone security operating system were significantly statistical different between Adolescence group and Senior-age group (***p< .001).

Keywords: Heuristic Evaluation, Smartphone Security, Human-Smartphone Interaction, Security Awareness, Aging Ergonomics

INTRODUCTION

Recently, computer itself or anything that is related to computer, in other words, hardware, software, handling data, computer communication, computer facilities, and its management. Students of Massachusetts Institute of Technology (MIT) started a group called Tech Model Railroad Club (TMRC) to explore and program the college's PDP-1 main frame computer system. The group used the name 'hacker' which is commonly known today.

The information was leaked easily by the hackers, although this website is a huge company with 35 million users. This incident shows the lack of security awareness of South Korea. Along with the increase of people who are trying to find personal, financial, and other information through public network, level of information security has increased. In all sectors of industry started to reconsider the way of transfer and announce its information. Also, the effort to augment data security increased along with the popularity of the use of internet.

https://openaccess.cms-conferences.org/#/publications/book/978-1-4951-2105-0

All smartphones, as mobile computers, are preferred targets of attacks. These attacks exploit weaknesses related to smartphones that can come from means of communication like Short Message Service (SMS, aka text messaging), Multimedia Messaging Service (MMS), Wi-Fi networks, Bluetooth and GSM for mobile communications. There are also attacks that exploit software vulnerabilities from both the web browser and operating system. Finally, there are forms of malicious software that rely on the weak knowledge of average users (Bishop, M., 2004).

Also, mobile security and mobile phone security has become increasingly important in mobile computing. It is of particular concern as it relates to the security of personal and business information now stored on smartphones. There is possibility of leaking one's personal information in the middle of smartphones if keep pursuing convenience. When viewed from this aspect, the convenience of high-quality IT product has inverse relationship with its security. So, it is necessary to enhance security conscious of smartphones users who put high priority on IT products' convenience.

More and more users and businesses use smartphones as communication tools but also as a means of planning and organizing their work and private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks. Indeed, smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company.

Different security counter-measures are being developed and applied to smartphones, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps. Hence, in this research, we statistically investigated the level of user preference and awareness of smartphone security operating system, and were to evaluate severity of security consciousness of smartphones users.

THEORETICAL BACKGROUND

Definition of Smartphone Security

U.S. Department of Defense invented interworked computer network through ARPA (the Advanced Research Project Agency) project which was originally created to support sharing of information among the agencies such as research institutions, defense-related business, or etc. This invention comprises underlying network of today's internet and left as important aspect of internet. In the 1970's, computer researching and inventing companies under the U.S. Department of Defense, Bolt, Beranet, and Newman invented commercial version of Arpanet, the 'Telnet' protocol. Therefore, data network that were available only to the government research institutes and defense-related companies has been made available to the public. However, according to some security researchers, 'Telnet' protocol is known as the weakest protocol in public network. Steve Jobs and Steve Wozniak established Apple Computer Company and started sales of personal computers. However, personal computer became a springboard for some malicious users who uses regular PC communication hardware such as analog modems and war dialer in hacking into remote system (Becher, M., 2009).

Now, new millennium came, where about 400 million people use internet globally (Computer Industry Almanac, 2004). Also, nearly 225 incidents of security breaches are reported to CERT Coordination Center in Carnegie Mellon university every day, and the number of reports is increasing (2001 – 52,658: 2002 – 82,094: 2003 – 137,529). Economical loss by 3 most perilous internet viruses is reported to be about 1.32 billion dollars for last 2 years.

Types of Smartphone Security

As security standard, all industry follows laws and regulations enacted by institutions such as AMA, or IEEE. It is the same with information security field. Many security consultants and retailers agree with Confidentiality,

Integrity, and Availability, known as CIA standard model. This 3-tier model is generally used for measuring security risk level of confidential information and establishing appropriate security policies (Dunham, K., Abu, N., Becher, M., 2008).

First, Network Security is security used for disclosure of inside information and protection from external intrusion. Second. System Security is preventing unlawful usage of computer system by using loopholes of computer system's operating systems, applications, or server. Third, Data Security is for protecting system data, preventing interception or modification of the data in transferring, and safely transferring the data (Figure 1).

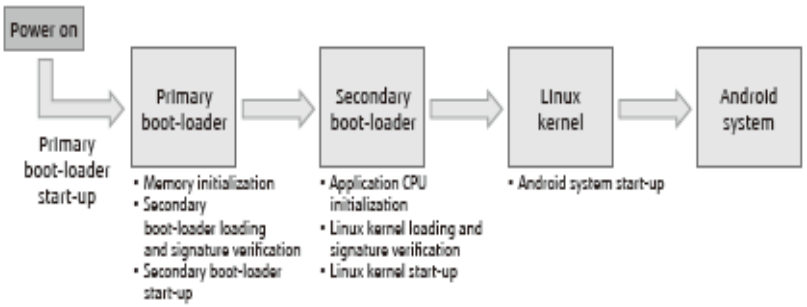


Figure 1. Sequential execution of multiple boot-loaders (Source: Y., Abe, and et al, Security technology for Smartphones)

Previous Studies of Smartphone Security

Nearly half of Smartphone users responded that they use Smartphone to get in touch with their acquaintances. Trendmonitor made public that 45.9% of total respondents use text messages and SNS to form and maintain relationships, on survey of utilization of Smartphone. In other words, Smartphone has important role in expanding everyday social encounters into online webs. This survey, planned by Trendmonitor and progressed by easy-survey, was based on 1000 adults who use Smartphone. Purposes other than interpersonal relations, Smartphone were mostly used for their technical functions. 18.9% of respondents used Smartphone for daily life and time management, and 15.3% used Smartphone for their high tech functions. Users who use Smartphone for high tech, showed interests when having conversations with others about latest technology and trends (source: http://www.zdnet.co.kr/news/news_view.asp?artice_id=20111026133819&type).

A smartphone user is exposed to various threats when they use their phone. Just in the last two quarters closing 2012 the number of unique mobile threats grew by 261%, according to ABI Research. These threats can disrupt the operation of the smartphone, and transmit or modify the user data. For these reasons, the applications deployed there must guarantee privacy and integrity of the information they handle. In addition, since some apps could themselves be malware, their functionality and activities should be limited (for example, restricting the apps from accessing location information via GPS, blocking access to the user's address book, preventing the transmission of data on the network, sending SMS messages that are billed to the user, etc.).

There are three prime targets for attackers: 1) Data: smartphones are devices for data management, therefore they may contain sensitive data like credit card numbers, authentication information, private information, activity logs (calendar, call logs), 2) Identity: smartphones are highly customizable, so the device or its contents are associated with a specific person. For example, every mobile device can transmit information related to the owner of the

mobile phone contract, and an attacker may want to steal the identity of the owner of a smartphone to commit other offenses, 3) Availability: by attacking a smartphone one can limit access to it and deprive the owner of the service.

Security on Operating System

Sometimes it is possible to overcome the security safeguards by modifying the operating system itself. As real-world examples, this section covers the manipulation of firmware and malicious signature certificates. These attacks are difficult.

In 2004, vulnerabilities in virtual machines running on certain devices were revealed. It was possible to bypass the bytecode verifier and methods to access the native underlying operating system. The results of this research were not published in detail. The firmware security of Nokia's Symbian Platform Security Architecture (PSA) is based on a central configuration file called SWI Policy. In 2008 it was possible to manipulate the Nokia firmware before it is installed, and in fact in some downloadable versions of it, this file was human readable, so it was possible to modify and change the image of the firmware. This vulnerability has been solved by an update from Nokia (Hollerer, T., Feiner, S., Terauchi, T., Rashid, G. and Halaway, D. , 1999, Schmidt, A. D., Schmidt, H. G., et al., 2008).

In theory smartphones have an advantage over hard drives since the OS files are in ROM, and cannot be changed by malware. However in some systems it was possible to circumvent this: in the Symbian OS it was possible to overwrite a file with a file of the same name. On the Windows OS, it was possible to change a pointer from a general configuration file to an editable file (Figure 2)

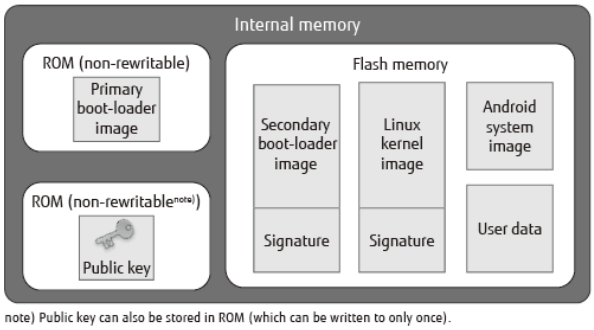


Figure 2. Example memory arrangement in Smartphones (Source: Y., Abe, and et al, Security technology for Smartphones)

User Awareness

Much malicious behavior is allowed by the carelessness of the user. From simply not leaving the device without a password, to precise control of permissions granted to applications added to the smartphone, the user has a large responsibility in the cycle of security: to not be the vector of intrusion. This precaution is especially important if the user is an employee of a company that stores business data on the device. Detailed below are some precautions that a user can take manages security on a smartphone. 1) Being skeptical: A user should not believe everything that may be presented, as some information may be phishing or attempting to distribute a malicious application. It is therefore advisable to check the reputation of the application that they want to buy before actually installing it. 2) Permissions given to applications: The mass distribution of applications is accompanied by the establishment of different permissions mechanisms for each operating systems. It is necessary to clarify these permissions mechanisms to users, as they differ from one system to another, and are not always easy to understand. In addition, it is rarely possible to modify a set of permissions requested by an application if the number of permissions is too great. But

this last point is a source of risk because a user can grant rights to an application, far beyond the rights it needs. For example, a note taking application does not require access to the geolocation service. The user must ensure the privileges required by an application during installation and should not accept the installation if requested rights are inconsistent. 3) Be careful: Protection of a user's phone through simple gestures and precautions, such as locking the smartphone when it is not in use, not leaving their device unattended, not trusting applications, not storing sensitive data, or encrypting sensitive data that cannot be separated from the device. 4) Ensure data: Smartphones have a significant memory and can carry several gigabytes of data. The user must be careful about what data it carries and whether they should be protected. While it is usually not dramatic if a song is copied, a file containing bank information or business data can be more risky. The user must have the prudence to avoid the transmission of sensitive data on a smartphone, which can be easily stolen. Furthermore, when a user gets rid of a device, they must be sure to remove all personal data first (Hollerer, T., Feiner, S., Terauchi, T., Rashid, G. and Halaway, D., 1999).

If users are careful, many attacks can be defeated, especially phishing and applications seeking only to obtain rights on a device. The reason for this difference is the differing technical resources offered by computers and mobile devices: even though the computing power of smartphones is becoming faster, they have other limitations than their computing power.

- Single-task system: Some operating systems, including some still commonly used, are single-tasking. Only the foreground task is executed. It is difficult to introduce applications such as antivirus and firewall on such systems, because they could not perform their monitoring while the user is using the device, when there would be most need of such monitoring.
- Energy autonomy: A critical one for the use of a smartphone is energy autonomy. It is important that the security mechanisms not consume battery resources, without which the autonomy of devices will be affected dramatically, undermining the effective use of the smartphone.
- Network Directly related to battery life, network utilization should not be too high. It is indeed one of the most expensive resources, from the point of view of energy consumption. Nonetheless, some calculations may need to be relocated to remote servers in order to preserve the battery. This balance can make implementation of certain intensive computation mechanisms a delicate proposition.

Therefore, the objectives of this study were to assess user satisfaction and usability evaluation of different smartphone security operating systems. Also, we were to evaluate the statistical differences in aged user’s preferences and satisfaction of the security system.

RESEARCH METHODS

Research Hypotheses and Definition of Variables

We collected eight five usability principles from previous literatures, including Nielsen`s checklist, screened a total of eighty-five usability principles among them in terms of user main interface properties, and refinedtwenty five usability principles, and usability checklist items are produced a 5-point Likert scale. The Following question should be answered with your sense of smartphone security awareness and your satisfaction on using the security programs (Table 1) (ISO 9241-11, 1998, ISO 13207, 1999), (Kim , R. H., Kwon, Y. K., et al, 2012).

The Hypothesis

This research was progressed in order to assess differences in age groups for awareness and usability of smartphone security. Therefore, the null hypothesis is ‘There is no difference in age groups for awareness and usability of smartphone security’. And the alternative is ‘There is difference in age groups for awareness and usability of smartphone security’. Independent variable is age, and dependent variables are awareness and usability of smartphone security.

Table 1: Questionnaires for awareness and usability of smartphones security depend on OS

Questions	Not at all	No	Average	Yes	Very Well
1. I feel restlessness when booting speed becomes slow					
2. Security is related with internet speed.					
3. I feel threatened about smartphone security when smartphone security reboots itself suddenly					
4. I'm interested in the field of Smartphone security					
5. There is little connection between hacking and smartphone security malfunction					
6. Hacking has nothing to do with me.					
7. Current security system is safe					
8. Downloads and security has no relations					
9. All the errors are caused because the smartphone security function is low in quality					
10. I feel threatened of smartphone security when smartphone security shuts down suddenly					
11. I'm aware of security program that I'm currently using					
12. On how security works is related to the security itself					
13. My smartphone security can repair its error easily					
14. I'm changing the approach to security of my IT products periodically					
15. I have quickly learned currently used security program					
16. I have recommended my smartphone security program to others					
17. I'm satisfied with my smartphone security measures					
18. I look for better security products for smartphone security					
19. I'm aware of usability of P2P websites					
20. P2P website are safe					
21. I'm satisfied with current interface of security program					
22. I'm satisfied with the design of current security program					
23. I can easily look for security program that is installed					
24. I'm satisfied with current method of information protection of my mobile PC					
25. I can easily solve any security error of my mobile PC					

Research Procedure and Analysis Tools

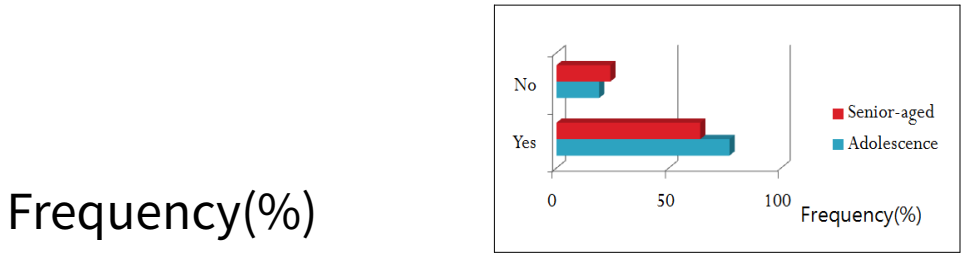
In this research, we have used district survey method to find smartphone security awareness and usability of gender and age. The selected usability principles are classified systematically using statistical method SAS 9.1,t-test (two aging groups) selected by the results of Duncan's Multiple Range Test and Principle Components Analysis (PCA) using Factor Analysis. 296 subjects (Groups: Adolescence group (20-40's), Senior-age group (45 years and over)) were divided into the two groups: Adolescence group and Senior-age group, and carried out collaborative work academic institutes. And verify the hypotheses based on the results of Principle Components Analysis (PCA) using Factor Analysis.

RESULTS AND DISCUSSION

Correlation between smartphone security awareness and age

Investigation of recognition of 'awareness and usability of smartphones security with age

In order to find correlation between smartphones security awareness and age, we have searched how many people of different age recognize the incident. We have investigated 296 randomly chosen people consist of different two age groups (155 Adolescences (20-45's), 141 Senior-ages (45 years and over)) response. In the Figure 3, for the adolescence and Senior-ages respondents, almost over 70% answered that they heard the incident.



(A) (B)

Figure 3. Investigation of recognition of awareness (A) and usage (B) of smartphones security

Relation of vaccine usage, and of setting boot password of smartphones security program based on age groups

In the age-based setting boot password of smartphones security program, adolescents and senior aged group answered to use of vaccine usage, and of setting boot passwords. In the results of age-based security-cautious relationship with the vaccine, adolescent and senior aged group showed low frequency of using the vaccine compare to not using at all. In the examination of setting boot password, adolescent and senior aged groups answered low rate of "Yes" to use passwords. Therefore, adolescent and senior aged respondent groups are not likely to set boot passwords.

The Results of awareness of smartphones security programs by age groups

In order to find the average for awareness of smartphones security programs, we have selected 5-point scale to get the average value for survey questions regarding awareness. For question number 6 (hacking has nothing to do with me), senior-aged respondents showed average of 3.6 and adolescent respondents showed average of 3.45, showing most of middle-aged respondents answered yes, while adolescent respondents answered normal. Other than this question, adolescent respondents showed higher average value than the senior-aged respondents (Figure 4, 5).

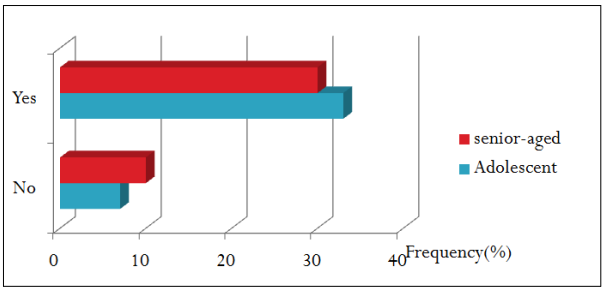
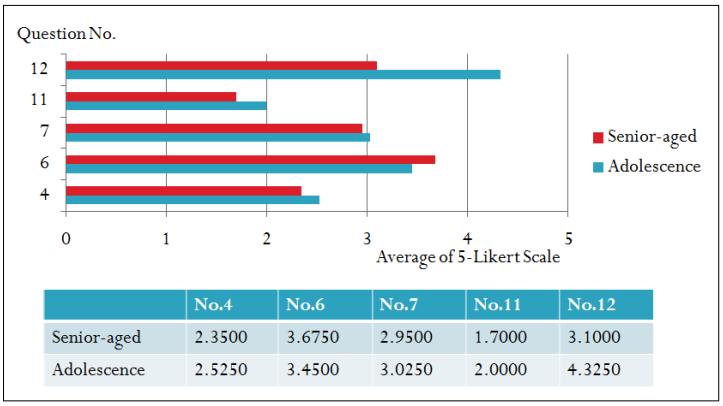


Figure 4. Vaccine usage, and of setting boot password of smartphones security program based on age groups



	No.4	No.6	No.7	No.11	No.12
Senior-aged	2.3500	3.6750	2.9500	1.7000	3.1000
Adolescence	2.5250	3.4500	3.0250	2.0000	4.3250

Figure 5. Awareness of Security programs by age groups

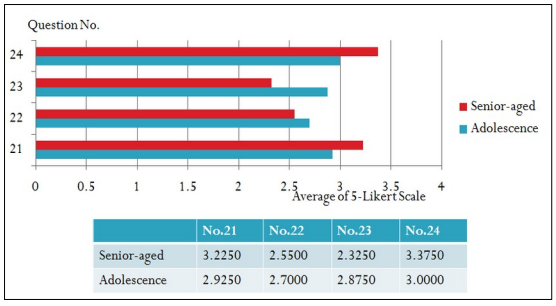
Satisfaction of smartphones security programs by age groups

In order to find the differences in satisfaction of smartphones security program on different age groups through survey questions, we have measured averages for questions 21~24. While adolescent respondents showed higher averages for questions 21~23, senior-aged respondents had higher average of 3.37 for question 24 satisfaction of currently using mobile PC's (smartphones) information security program (Figure 6).

The Heuristic Usability Evaluation of Smartphones Security Programs

The results of evaluation of smartphones security programs usability correlated with age are shown in Table 3. There are significant differences between Adolescence group and Senior-aged group for some awareness and usability items of smartphones security programs (Kim, R.-H., et al., 2012).

Also, 14 items for smartphones security programs usability evaluation are categorized into four groups according to their correlations and we named them respectively (1) Factor 1; User Interaction-support (Questionnaires No. 9, 10, 11, 12), (2) Factor 2: User Cognitive-support (Questionnaires No. 4, 5, 6, 7),



	No.21	No.22	No.23	No.24
Senior-aged	3.2250	2.5500	2.3250	3.3750
Adolescence	2.9250	2.7000	2.8750	3.0000

Figure 6. Satisfaction of smartphones security programs by age groups

(3) Factor 3: User Performance-support (Questionnaires No13, 14, 15, 16), (4) Factor 4: User Physicality (Questionnaires No.2, 3), and the other questionnaires of awareness and satisfaction of smartphones security program were excluded PCA Factor Analysis in the heuristic usability evaluation.

CONCLUSIONS

So, total usability items of 14 smartphones security programs checklists are developed with 5-point Likert scale. PCA reduced the 14 usability measurements to four factors, and the Varimax rotation more clearly distinguished the usability components. Reliability within these factors were calculated by Cronbach's alpha, Factor 1; 0.787, Factor 2; 0.752, Factor 3; 0.711, Factor4; 0.826. All of the reliability within these factors was very a high correlation respectively.

Table 2: Usability evaluation and checklist items for smartphones security program by PCA Factor Analysis

Questionnaire No.	Factor for smartphones security program were excluded PCA Factor Analysis in the heuristic usability evaluation			
	Factor 1: User Interaction-support	Factor 2: User Cognitive-support	Factor 3: User Performance-support	Factor 4: User Physicality
10	.854	.055	.077	.067
9	.868	.084	.200	.033
11	.814	.077	.180	.117
12	.642	-.347	.012	.340
5	-.106	.864	-.004	.030
6	.051	.883	-.103	.338
7	.387	.703	-.058	.026
4	-.248	.617	.455	.211
14	.500	-.006	.742	.143
13	-.088	.013	.721	.049
16	.537	-.079	.697	.086
15	.478	-.024	.694	.165
2	.088	.322	.030	.669
3	.231	.085	.333	.723

Table 3. The comparison and usability level analysis of smartphones security programs between Adolescence group (N=155) and Senior-aged group (N=141) in some awareness and preferences and satisfaction questionnaires

	Differences of value		F-ratio
	Adolescence group (N=155)	Senior-aged group (N=141)	
Awareness	4.46 A	3.98 B	7.81***
Preferences and Satisfaction	4.17 C	4.21 A	6.09***

1) * p< .05, *** p< .01

2) P. S. : Alphabet is the results of Duncan's Multiple Range Test

Also, the results of the comparison and usability level analysis of smartphones security programs between adolescence group (n=155) and senior-aged group (n=141) in some awareness, and preferences and satisfaction questionnaires are shown in table 3. According to the Duncan's Multiple Range Test, the results of the comparison

and usability level analysis of awareness between adolescence group (4.46A) and senior-aged group (3.98B) are showed, so levels of smartphones security programs in the two groups are slightly different.

In conclusions of this research, the results of the statistical comparison and usability level analysis of preferences and satisfaction between adolescence group (4.46A) and senior-aged group (4.17C) are showed respectively different values. As the experimental method, the null hypothesis is 'There is no difference smartphones security programs between adolescence group (n=155) and senior-aged group (n=141). But, The alternative hypothesis of hypothesis 2: There is difference in age groups smartphones security programs between adolescence group (n=155) and senior-aged group (n=141). We can assume that level of adolescence group's smartphones security programs is higher than level of senior-aged group.Because we can be recognized from the evaluation results of this research, we could accept the alternative hypothesis.

REFERENCES

Anderson, J. A., Wangner, J., Bessesen, M., and Williams, L. C. (2011), Usability Testing in the Hospital, Journal of Human Factors and Ergonomics in Manufacturing & Service Industries, 00 (0) 1-12 DOI: 10. 1002/hfm, Wiley Periodicals, Inc.

Becher, M., (2009). Security of Smartphones at the Dawn of Their Ubiquitousness (Dissertation). Mannheim University.

Bishop, M., (2004). Introduction to Smartphone security. Addison Wesley Professional. ISBN 978-0-321-24744-5.

Dunham, K., Abu, N., Becher, M., (2008), Mobile Malware Attack and Defense. Syngress Media. ISBN 978-1-59749-298-0.

Hollerer, T., Feiner, S., Terauchi, T., Rashid, G. and Halaway, D. (1999), Exploring MARS: Developing Indoor and Outdoor User Interfaces to a Mobile Augmented Reality System, Smartphone securitys and Graphics, 23(6), pp. 779-785.

ISO 9241-11, (1998), Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs)-Part II: Guidance on usability, ISO, Geneva.

ISO 13207, (1999), Human-Centred Design Processes for Interactive Systems, ISO, Geneva.

Ji, Y. G., Jin, B. S., and Ko, S. M., (2007), Development of a AHP Model for, Telematic Interface Evaluation, Proceedings of HCII 2007 Conference on Human compute Interaction, LNCS 4550, Beijing, China, July.

Kim, M. H. and Ji, Y. G., (2007), The Development of usability evaluation method for tangible user interface, Thesis, University of Yonsei.

Kim , R. H., Kwon, Y. K., et al, (2012), Users' Awareness of Computer Security and Usability Evaluation, 2012 AHFE ID:1192, July, San Francisco, USA.

Kim, W. K. (2001), Physical disability and depression in older adults: Predictability of structural and functional aspects of social support, The Korean Journal of Clinical Psychology, 20(1), pp. 49-66.

Nielsen, J., (1994b), Heuristic Evaluation, In, J. Nielsen and Mark, R. L. (Eds.), Usability Inspection Methods, pp. 25-62, New York: John Wiley and Sons.

Schmidt, A. D., Schmidt, H. G., et al., (2008). "Enhancing Security of Linux-based Android Devices". Proceedings of 15th International Linux Kongress.

Schmidt, , A. D., Schmidt, H. G, et al., (2009). "Smartphone Malware Evolution Revisited: Android Next Target?". 4th International Conference on Malicious and Unwanted Software (MALWARE). ISBN 978-1-4244-5786-1. Retrieved 2010-11-30.

Seong, L. K., (1998), Experimental Design and Analysis, pp.194-267, Gyunggi-Do, Korea, Free-Academy Press.

Thirumathyam, Rubathas; Derawi, Mohammad O. (2010). "Biometric Template Data Protection in Mobile Device Using Environment XML-database". 2010 2nd International Workshop on Security and Communication Networks (IWSCN). ISBN 978-1-4244-6938-3.

-http://www.tscllc.com/Small-Business-Solutions/Tablet-pc-benefits.asp

- http://www.pcbee.co.kr/it/viewer_tx.php?content_num=38044

kostat.go.kr/portal/korea/kor_nw/.../index.board (2005)