PERCEIVED SMART-PHONES SECURITY IN DIGITAL LIFE

Abstract. Smart phones and services have been providing modern life with great flexibility. Mobile phones are widely used for personal and business purposes and may include critical and private information. This makes these devices targets of attackers. These threats and vulnerabilities should be considered when using these devices in all aspects of life. The purpose of this study was to examine the perceived security in mobile devices and compare these results with that of previous studies. An important finding of this study is that Turkish users seem to give higher importance to security features although are not aware of the current threats to their smartphones.

Keywords: Mobile Security. Mobile phone, Information Security

1 Introduction

The digitalization era has led to an increase in the popularity of smart phones and more and more applications and services are available for mobile operating systems (OS). These devices are playing a much more important role in personal and business life storing critical and personal information. These devices are with users at all times and include exploitable features such as cameras and microphones. These features can be used to violate private information should they be compromised.

Mobile devices have become increasingly popular as they are powered by better hardware and supported by several mobile OS and platform such as Windows Mobile, Symbian, and BlackBerry at the beginning, and android and IOS later. The mobile devices as microcomputers support many business applications such as ERP and CRM. These applications are easily installed by device owners. A related study shows that that only 60% of smart phone users are concerned that mobile payments could put their financial and personal security at risk (Chin, 2012).

There have been several researches investigating the psychological and behavioral factors that influence the concept of new technology adoption. One of the models developed with the aim of explaining how users accept and use a technology is the Technology Acceptance Model (TAM) (Venkatesh and Davis, 2000). TAM states that ease of use and usefulness has a great role on intentions to adopt a technology. The study of (Cope, Rock and Schmeiser, 2013) suggests that risk perception and tolerance is important for encouraging users to adopt a new technology. The study of Phan and Daim (2011) shows that usefulness and ease of use should be taken into consideration to structure the attitude toward using mobile services.

Gorlenko and Merrick (2003) divide the usability challenges of mobile device use into three groups, technical; which is related to network connectivity issues and security hazards, environmental; involving issues like variation in temperature, noises and distractions, mobility of the user and social challenges; that includes personalization, comfort, acceptance and adoption issues as well as privacy concerns, particularly in applications based on location-awareness.

Smart phone's network feature is the combination of Internet and telecom networks. Threat for attacks mainly come in two forms, downloading content or SMS and phone calls. Also, some attacks may rise from WLAN and Bluetooth vulnerabilities (Li and Im, 2019).

Mobile security has become an important issue due to particular concern about the security of personal information stored on smart phones. According to Kaspersky (2019), the number of attacks using malicious mobile software has doubled in the past year from 66.4 million in 2017 to 116.5 million. There are various threats that might attempt to exploit the vulnerabilities in mobile OS or applications such as spying or modifying and transferring personal data. Another possible threat is location tracking of the smart phone user. A specialized malware called diallerware infects financial applications and steals credit card numbers and online banking credentials. Such a spyware app that resembles a useful app may be installed by a careless user. Jailbreaking of mobile OS and unsecured WI-FI networks also leads to vulnerabilities (Ponemon Institue, 2011).

Each platform has strengths and weaknesses. We can examine the most popular platforms Apple IPhone, Google Android, and Microsoft Windows Mobile from the headlines of Delivery, Trust Levels, and System Isolation point of view. Studies show that Apple has a high security level in Application Delivery while a low security level in Trust Levels and System Isolation. Google Android shows the best performance in System Isolation and Trust Levels while medium in Application Delivery. Windows Mobile and Symbian OS has medium protection in all levels (Oberheide and Jahanian, 2010). Several other studies have focused on this important topic (ENISA, 2010; Montjoye et al. 2018; Shen, Gong and Bao, 2018; NQ Mobile and NCSA, 2012; Mensch and Wilkie, 2018; Ramanen, 2011; Stammberger, 2010).

The aim of this study is to examine the perceived security in mobile devices and compare mobile OS security and user preferences related to OSs and application download sources. This study also aimed to gain insight regarding security perceptions of legacy mobile OSs such as Symbian and Blackberry. The basis of this study was the 2011 surveys of Ponemon Institute (2011) and Ramanen (2011). The purpose of these studies was to understand user perceptions regarding privacy and security risks as well as if these users give importance to these risks enough to take precautions. Utilizing the survey questions previously asked in these studies, we aimed to clarify the change if any of security perception of mobile devices as well as between cultures. This study also aimed to answer the following research questions:

RQ1: Does users demographic affect smart phone usage?

RQ2: Does the frequency of Internet usage affect perceived security?

RQ3: Does the frequency of smartphone usage affect the privacy perception of smartphones.

2 Methodology

An online survey using questions from the Ponemon Institute and Ramenan studies was used to collect the necessary data for analysis. This survey was answered by Turkish users. The questions were of quantitative and qualitative nature including Likert Scale type questions. Participants were asked to rate the relative importance of more than 20 questions based on past literature. Responses were measured on a 5-point scale with values ranging from (1) “not at all important” to (5) “very important”. Multiple choice questions were used for collecting demographic information.

202 valid responses out of 202 questionnaires completed were reached. SPSS was used for the reliability analysis, analysis of variance (ANOVA) and Pearson Correlation between statements and factors, Independent T-Test, Chi Square and Crosstab analysis. For the Cronbach’s Alpha values above 0.6 were considered as (Hair et al., 1998) suggest the values of 0.60 to 0.70 to be the lower limit of acceptability. Group differences were also analyzed in order to answer the research questions of the study.

3 Findings

This study explored perceived security in smart phones. The findings show that perceived security in smart phones is important for smart phone users, and it is capable of considerably influencing the intention to use certain smart phone services. This study provides evidence to the assumption that security concerns associated with mobile services that are more pronounced than those associated with the more traditional services used with a computer.

Figure 1 below shows the demographic features of the survey participants. As can be understood from the figure, the majority of participants are between the ages of 18-24, studying for their bachelor’s degree and have an income between 0-1000.

GENDER	Female	Male				
	98 (48.51%)	104 (51.48%)				
AGE	18-24	25-34	35-44	45-54	>55	
	109 (53.96%)	78 (38.61%)	14 (6.93%)	1 (0.49%)	0 (0%)	
EDUCATION	High school and below	Associate	Bachelor	Master	Doctorate and above	
	8 (3.96%)	9 (4.45%)	156 (77.22%)	27 (13.36%)	2 (0.99%)	
INCOME	0-1000	1000-2000	2000-3000	3000-4000	4000-5000	>5000
	74 (44.57%)	29 (17.46%)	10 (6.02%)	15 (9.03%)	7 (4.21%)	31 (18.67%)

Fig. 1. Demographic features of the participants

4 Results of the Research

Figure 2 compares the smart-phone usage purposes with the (Ponemon Institute, 2011) survey. Looking at this figure, it can be said that users are still using smartphones for personal purposes as well as business. However, the use of smartphones for only business purposes is very unpopular among the Turkish users.

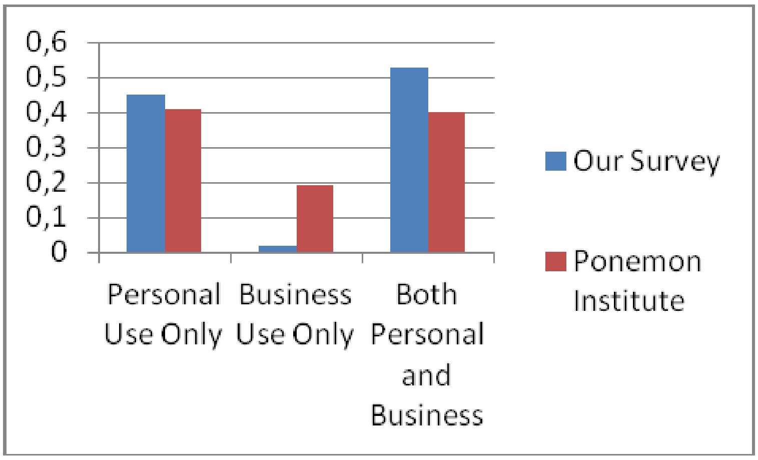

Fig. 2. Comparison of smart-phone usage purposes literature comparison

Figure 3 compares smartphone usage frequency with (Ramenan, 2011). This figure shows that the survey participants use their smartphones every day and this number has grown significantly throughout the years.

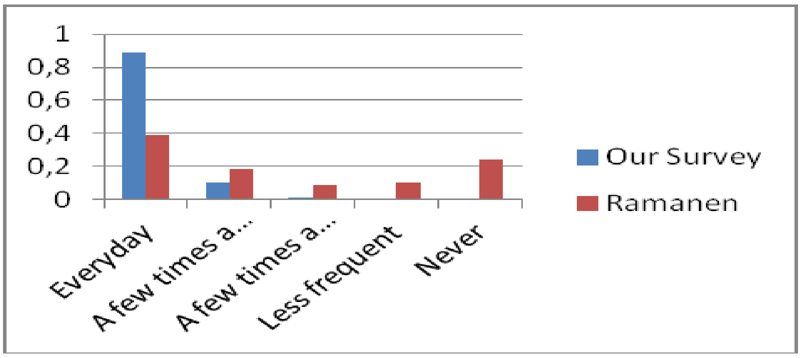

Fig. 3. Smartphone usage frequency

Figure 4 compares the awareness related smart-phone security threats with (Ponemon Institute, 2011). The percentage of insecure wifi (%35) is greater than our survey's percentage (%15.31). However, in both survey participants find spyware an equal risk.

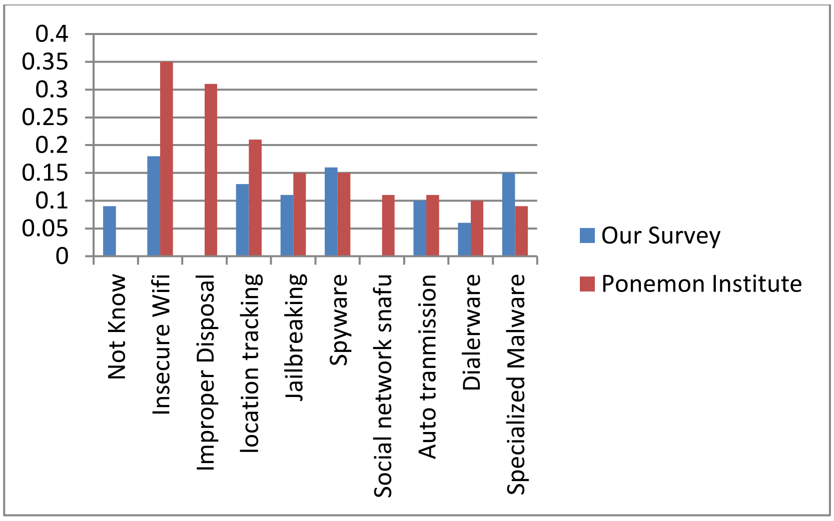

Fig. 4. The awareness of smart-phone security threat literature comparison

Figure 5 shows that US survey respondents in 2011 are more aware of marketing abuse and cross-over. However, Turkish respondents are more oblivious to the risks or have not encountered any risks.

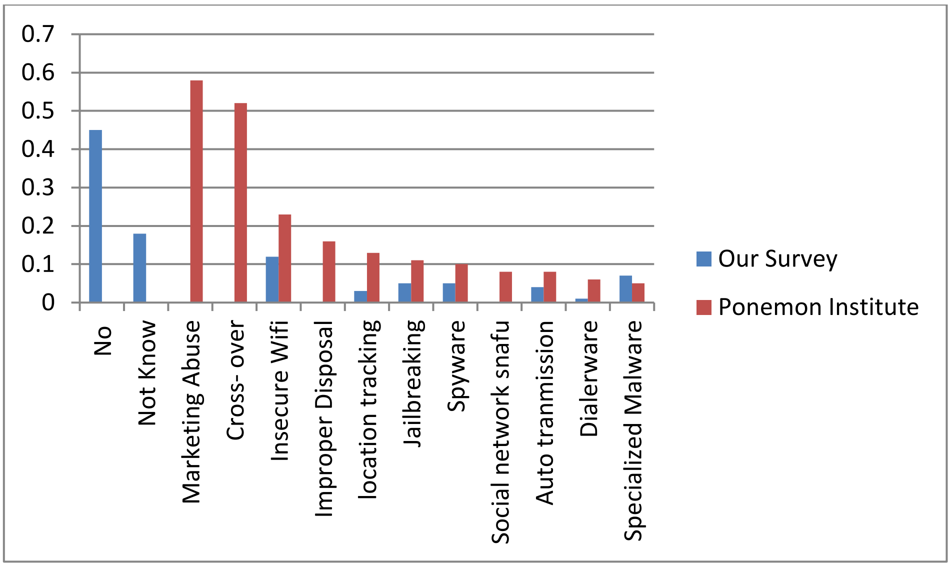

Fig. 5. Smart-phone security threat encountered literature comparison

When we look at the importance of smart-phone security as a feature, it can be said that more than half of the respondents (%52.48) find security as a feature very important and second majority of them (%40.1) find security important. The minority of them do not care about the security as a feature. When we examine the other study (Ponemon Institute, 2011),a great number of people (%43) find security as a feature important and the rest of them (%57) find security unimportant. In light of these results, it can be said that while Turkish users seem to give importance to security as a feature, according to figure 5 they are not aware of the threats pertaining to smartphones.

Figure 6 presents the frequency of user experiencing a security violation. Both study participants have found to frequently experience violations.

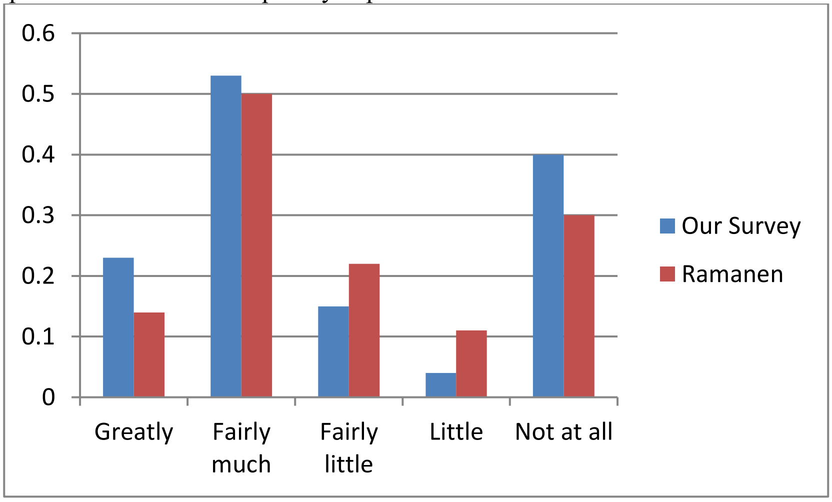

Fig. 6. The result of smart-phone security software/applications literature comparison

Table 1 answers the question, which mobile phone security system is perceived to be the most secure? It can be said that IOS is perceived as most secure followed by Android.

When looking for difference among gender groups, the p values have been calculated as 0,01. This value is smaller than 0,05 so it can be said that security perception towards smartphones change according to gender. Males frequently find iOS more secure while females find Android more secure. Moreover, there is a minority opinion about legacy mobile OS RIM (Blackberry Platform) and Linux that is not a mobile OS.

Table 1. Most secure operating systems according to gender

Which mobile phone security system do you think most secure?		Gender		
		Male	Female	Total
No idea	Count	29	49	78
	% of total	14,4%	24,3	38,6
iPhoneOS	Count	48	23	71
	% of total	23,8%	11,4%	35,1
Android	Count	14	23	37
	% of total	6,9%	11,4%	18,3%
RIM	Count	3	0	3
	% of total	1,5%	,0%	1,5%
Windows Mobile	Count	2	2	4
	% of total	1,0%	1,0%	2,0%
Bada	Count	1	0	1
	% of total	,5%	,0%	,5%
Symbian OS	Count	2	1	3
	% of total	1,0%	,5%	1,5%
Linux	Count	5	0	5
	% of total	2,5%	,0%	2,5%
Total	Count	104	98	202
	% of total	51,5%	48,5%	100,0%

5 Hypotheses

5.1 Smart-phone Privacy Information Risk

H_1: There is a difference between gender groups regarding perception of smartphones’ privacy risk.

The result of the t-test is that there is an important difference between genders in view of feeling about the smart-phone privacy risk and also males’ degree of mean is greater than females. Since the significance level (.035) is lower than 0.05, we accept the hypothesis.

5.2 Application Download Control

H_1: There is a difference among age groups regarding doubting the source of application while downloading

The result of the ANOVA is that there is no controlling difference between demographical values(ages) in view of applications whose source is reliable, and the interval of 25-34 ages' mean is greatest one. The significance level (.035) is less than 0.05. Therefore, we accept the null hypothesis.

5.3 Operating System Running on Smart-phone and Income Level

H_1: There is difference in users' smart-phone OS preferences according to their income level.

The result of the Chi-Square Test is that there is an important difference between income level and people's knowledge about the operating system running on their smart phones. Most of the users' income level (44) are under 1000 and the significance level (.031) is less than 0.05. Therefore, we accept the hypothesis.

5.4 Usage Purposes of Smart-phone Users and Importance of Smartphone Security Features

H_1: There is a group difference among smartphone usage purpose and the given security feature importance.

The significance level in the second table at last column is .030 which is lower than significance level "0,05". Since 0.03<0,05 we can claim that, there is a difference between the groups in security.

First Group ,"Just for business users", only 4 participants out of 202 sample, with Mean 4,25 and a high value of standard error with 0,479 while second group "only for personal users" with , Mean 4,28 but "both business and personal users" group with Mean 4,55 , 4 participants is not enough to support this hypothesis on the first group directly. However, we can claim that "Business Purpose" is a factor which increases the importance of security features on a mobile phone. Both "Business and personal users' mean 4,55 > "only for personal users" 4,28 with significance level 0,05. As a factor Business usage boosted the mean of this group. Therefore, we accept the hypothesis.

5.5 Internet usage frequency and importance of smart-phone security features

H_1: There is a difference in importance perception of smart-phone security features in view of users' internet usage frequency.

Correlation level Sig.(2-tailed) is 0,0001 which is smaller than 0,05 so we can claim that there is strong, positive and linear relationship between the frequency of internet usage, importance of security features of a mobile phone. Moreover, correlation power in the second table, second column of third line is 0,268. Therefore, we accept the hypothesis.

5.6 Gender Effect on Smart Phone Choice

H_1: There is no gender effect on mobile phone platform choice.

As we see in the table 1, smartphone choice is almost well distributed between genders. We can’t claim a relationship between the smartphone platform choice and gender. Therefore, we accept the hypothesis.

6 Conclusion

This study focused on perceived security in mobile devices and compare mobile OS security and user awareness. In this study, we try to obtain security perception of not only current popular mobile OS such as Android and IOS but legacy mobiles OS such as Symbian and Blackberry from users previous experiences in order to give detailed security perception.

Given the findings, it is safe to say that there is no significant difference between perceived security of gender and age groups. However, there seems to be a difference in terms of income groups. Also, an important finding of this study is that Turkish users seem to give higher importance to security features although are not aware of the current threats to their smartphones. This leads to the conclusion that users although aware that smartphone security is important, their behavior shows otherwise. This shows that security awareness is lacking in detail and is only seen on the surface.

Lastly, in the 8 years between studies, the number of smartphone users and the frequency of usage has increased significantly. However, this needs to be taken with caution as this can also be a cultural effect. We can surely say that Turkish youths spend a lot of time on the smartphones, but need to be more aware of the specific threats they are open to.

As with all studies, there are some limitations. The most important limitation is that this study compares results with previous studies conducted on two different cultures. This could be the main reason of the change in frequencies. However, the time between this study and the previous studies could account for the change in answers. The culture effect prevents us from being able to specifically point to the reason for the change in answers. Therefore, this study should take this limitation into account. A further study could incorporate US and Finnish participants and compare them all.

Acknowledgement

The authors are thankful for the valuable support of A. Senel, C. Akturk and M. Derin.

References

Alice M. Cope, Alexandra M. Rock, Maximilian D. Schmeiser (2013). Risk Perception, Risk Tolerance and Consumer Adoption of Mobile Banking Services,24. US: Washington.

Bo Li, Eul Gyu Im (2011). Smart phone, promising battlefield for hackers.South Korea.

Chin E. (2012). Measuring User Confidence in Smartphone Security and Privacy. US:California.

de Montjoye, Y. A., Gambs, S., Blondel, V., Canright, G., de Cordes, N., Deletaille, S., ... & Krings, G. (2018). On the privacy-conscientious use of mobile phone data. *Scientific data*, *5*.

ENISA, (2010), ENISA Report. Retrieved June 5, 2013 from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines

Gorlenko, L. & Merrick, R. (2003). No wires attached: Usability challenges in the connected mobile world. IBM Systems Journal, 42, (4), pp. 639–651.

Hair, J. E., Anderson, R. E., Tatham, R. L. and Black, W. C. (1998). Multivariate Data Analysis. 5th Edition. New Jersey: Prentice-Hall.

Mensch, S. E., & Wilkie, L. (2018). Cell Phone Security: User Awareness of Security Issues and Mobile Device Management. *International Journal of Strategic Information Technology and Applications (IJSITA)*, *9*(3), 15-31.

Mobile Malware Evolution 2018 (2019, March 5) retrieved from https://securelist.com/mobile-malware-evolution-2018/89689/

NQ Mobile & NCSA (2012). Report on Consumer Behaviors and Perceptions of Mobile Security

Oberheide J., Jahanian F. (2010). When Mobile is Harder Than Fixed (and Vice Versa) University of Michigan

Phan K., Daim T. (2011) Portland State University (USA), Exploring technology acceptance for mobile services,342-351.US: Portland.

Ponemon Institute (2011). Smartphone Security Survey of U.S. Consumers. US:Traverse City

Raemaenen, J. (2011). Perceived security in mobile authentication. *Aalto University, Aalto University*, Finland.

Shen, J., Gong, S., & Bao, W. (2018). Analysis of Network Security in Daily Life. *Information and Computer Security*, *1*(1).

Stammberger K (2010). Mobile & Smart Device Security Survey Concern Grows as Vulnerable Devices Proliferate, Smart-phones are the Tip of the Iceberg.US: San Francisco.

Venkatesh, V., & Davis, F.D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. Management Science, 46(2), 186-204.US: Arkansas.