International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-6 Issue-4, April 2017

Interpreting Users' Perceptions of Mobile Security Methods and Their Effectiveness

Richmond Adebiaye

Abstract: ***The increasing adoption of open source operating system (OS) platforms, such as Android and iOS, have opened up new security vulnerabilities and threats to mobile devices and other wireless access technologies. Recent statistics show that mobile networks around the globe "generate exceedingly over 86 exabytes of traffic annually". Thus, mobile security vulnerabilities and threats such as SMS spam, rogue apps, adware, malware, cyber-attacks and unlawful eavesdropping have become an ever-increasing problem for mobile users around the world. This paper proposes a quantitative research survey to investigate mobile device security and the implications of security application recommendations for its users. The objective is to identify increased security risks, and recommend best security practices for mobile users. To obtain quantitative values, web-based questionnaires using the Likert scale were used, and data processed by factor analysis, ANOVA and multiple regression analysis tabulated along a continuum in numerical form. The study thus identifies and reveals the impacts of smartphone security threats such as mobile adware, rogue application downloads, and considers the suitability of smartphone security solutions offered by various vendors. This paper provided insights into users' problems of malware, attack channels, black industry 'chain of smartphone security', and accessibility to smartphone security solutions introduced by mobile vendors. As this study adds to the available body of knowledge, it is anticipated that future research will continue to advance the available information regarding rogue applications, adware, malware, and other security threats related to mobile technology.***

Keywords: Smartphones; Mobile security; Information Security; Android O/S; Vulnerabilities and Threats; iOS

I. INTRODUCTION

The number of mobile device operating systems platforms, such as Android and iOS, has steadily increased in recent times, leading to the emergence of new software vulnerabilities and security threats to cell phone and wireless technologies. Current statistics reported by the Mobile Device Security Threat Report (2015) show that globally, mobile networks generate more than 86 exabytes of traffic per year. Christian (2014) states that 99% of software security threats target new Android devices, but recently, an 82% increase in malware threats has been reported for iOS devices. Mobile security vulnerabilities and threats, such as SMS spam, rogue apps, adware, malware, cyber-attacks and unlawful eavesdropping have therefore become an escalating issue for mobile users around the world.

Manuscript published on 30 April 2017.
***** Correspondence Author (s)
Dr. Richmond Adebiaye, College of Information Technology, Head of Information Systems Department, Ajman University, Ajman UAE, E-mail: Richmondwiz@yahoo.com

Mobile device security refers to the protocols implemented on mobile devices for the protection of data or applications. The methods deployed, and their effectiveness, are contingent on the device's operating system platform, such as Android and iOS compatibility. Conversely, mobile security threats refer to applications or software-based incursions that interfere with or intrude into private data on a device, without the consent of the user. These threats can cause malicious intrusion on the device and its data, as malware typically does (Yaseen& Tariq, 2012). Malware (malicious software) targets specific device and user information, and can sometimes lead to device breakdown, which can result in the user's device data being violated or misused (Pg.6). Most malware attacks are engineered through social networking scams, wireless attacks, mobile phishing and ransomware, and use infected mobile device systems to infiltrate other devices (Mobile Security Threats Report, 2014). Greenberg (2010) concurs that malware practices are common, and notes the prevalence of cross-platform cyber-attacks on both PCs and mobile devices and attributed the most common types of malicious software threats to be worms, spyware, Trojans and other unknown viruses. Because of the exponential increase in the instance of events of security compromise in mobile devices, security innovations have so far proven inadequate in addressing these security threats, and the extent to which security advances can be applied to cell phone technology remain limited. For these reasons, mobile devices remain largely vulnerable to security incursions. In order to address the issue, Christian (2014) posits that the encryption of mobile devices is a necessary development. Encryption of mobile devices helps to protect against loss of data, and given the difficulty of preventing individuals from utilizing their smartphones and tablets in public places, such a measure may be necessary. Yaseen & Tariq (2012) also suggest that smartphones and tablets can secure wireless connections with WPA by encouraging Information Technology experts to download versatile applications to track basic data, which, in the long run, may prevent mobile device and wireless technology intrusions. This security may be achieved by ensuring there is adequate server and system encryption and record exchange capacity on every individual's gadget coming from the network provider.

II. METHODS

This research study purposively seeks to identify the most common forms of mobile security threats and vulnerabilities, and to propose possible smartphone security solutions and adaptations that can, and should, be offered by mobile device vendors.

To achieve this, a survey was carried out concerning usage of mobile devices and their operating systems, download rates of various apps, identifiable software security practices in mobile downloads, and related factors that bear influence on the usage and security of mobile device systems.

2.1. Research Target

The following are the research targets for the objectives of the study:

i. To identify the most common forms of software security threats and vulnerabilities that affects usage of mobile devices such as smartphones and tablets.

ii. To test the effectiveness of mobile security solutions offered by mobile device vendors in addressing these software security threats and vulnerabilities.

iii. To establish the total number of downloads per mobile device user for each operating system of mobile devices.

iv. To determine whether mobile device security threats and vulnerabilities are affected by the total number of downloads per user for each type of mobile device operating system and user demographic factors.

2.2. Sample frame

Samples are users of mobile devices who are faced with mobile device security threats and vulnerabilities concern. Due to the large population involved, and the lack of sufficient time and resources, a sample size of 150 individuals was deemed appropriate for this study. Simple random sampling practices were used to select the sample group, so every person faced with mobile device security threats and vulnerabilities had an equal chance to be selected for the sample grouping. From the 150 individuals who received the web-based questionnaire, 119 participants responded to the questionnaire. These 119 participants represent a 79.33% response rate for the anticipated sample size.

2.3. Study Variables

The variables associated with the study were classified as either dependent, independent, or intervening. The identified dependent variable was whether a participant had experienced or encountered any mobile device security threats, while the numerous independent variables included -: the type of mobile device used; the number of downloads per mobile device user; the types of mobile device security threats and vulnerabilities; and the type of mobile device operating systems. The identified intervening variables were mainly demographic factors, such as age, gender, education and socio-economic index.

2.4. Data collection

Data collection was based on the descriptive research method. Survey design was deemed appropriate for this particular study, given its objective of gaining insights into related phenomena in the area of mobile device usage and mobile software security. The survey design not only assisted with data collection, but also facilitated the provision of reliable and appropriate information about how to handle matters concerning mobile device security.

The survey data was collected using web-based questionnaires. These questionnaires were developed objectively, in order to ascertain data that would generate valid and reliable information from the population under study. The structures of the questionnaire were classified into two sections: demographic data, and data relating to the five research questions as indicated above. The questions set out were specific, measurable, reliable, brief, and grammatically correct, to avoid any ambiguity or confusion in answers. Some of the questions had a choice of answers, which were scaled using the 5-point Likert scale.

2.5. Data analysis processes

The collected data was entered into an SPSS spreadsheet and then edited, in order to check for missing or abnormal values before carrying out data analysis. The demographic data was analyzed using frequency tables and graphical methods. The data relating to the research objectives was analyzed using the Analysis of Variance (ANOVA) technique, as well as factor analysis through descriptive statistics and multiple regressions. The F-ratio statistic (F), the factor loadings, and the beta values (β), in conjunction with their respective p-values, were used to test the significance of the findings for each research question as related to Mobile application security. The results of data analysis were then interpreted in order to ascertain findings of the study that would be used to generate the conclusions of the study.

III. DATA ANALYSIS AND INTERPRETATION OF RESULTS

3.1. Reliability, Bias and Validity Tests

The research tools (in this instance, questionnaires) were checked for validity and reliability using test and pretest methods as well as piloting methods. This was accomplished using Cronbach's Alpha, a recognized measure of reliability. Table 1.1 below shows the results of reliability and validity tests relating to the dependent variable (Mobile Device Security Threats), independent variables (Mobile Device System and Security factors), and intervening variables (demographic factors).

Table 1.1: Reliability and Validity Statistics

Software Security		Demographic Factors		Mobile Device Factors	
Cronbach's Alpha	N of Items	Cronbach's Alpha	N of Items	Cronbach's Alpha	N of Items
0.871	119	0.918	119	0.83	112

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The results showed that the Cronbach's Alpha score for Mobile Device Application/Software Security was 0.871 with a sample of 119 respondents, 0.918 for demographic factors, and 0.830 for mobile device factors. According to Everitt (2008), since the Cronbach's Alpha was more than 0.8 for all results, this established that the survey data was highly reliable and valid.

3.2. Demographic Data Analysis

Table 1.2: Frequency Distribution of Demographic Factors

Factor	Attribute	Frequency	Percent	Cumulative Percent
Gender	Male	71	59.7	59.7
	Female	48	40.3	100.0
	Total	**119**	**100.0**	
Age (years)	less 20	18	15.1	15.1
	21-30	39	32.8	47.9
	31-40	50	42.0	89.9
	41-50	9	7.6	97.5
	51+	3	2.5	100.0
	Total	**119**	**100.0**	
Level of education	High school	31	26.1	26.1
	Associate Degree	44	37.0	63.0
	Undergraduate degree	34	28.6	91.6
	Graduate/Post graduate	10	8.4	100.0
	Total	**119**	**100.0**	
Socio-economic level	Low	59	49.6	49.6
	Average	43	36.1	85.7
	High	17	14.3	100.0
	Total	**119**	**100.0**	

Table 1.2 above shows that 59.7% of survey respondents were male, while 40.3% were female. This shows that there was no gender parity among the users of mobile devices, and that the most users affected by mobile device security threats were Males. The above results can also be analyzed with the use of a pie chart.

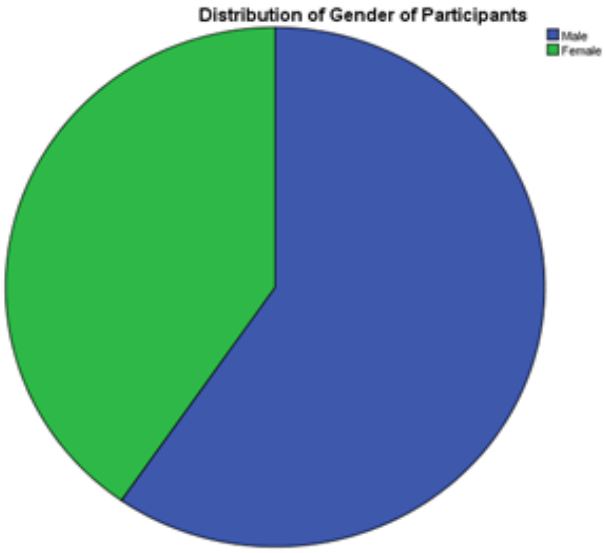

Figure 1.1: Pie Chart Showing Gender Distribution

Table 1.2 also indicates that most mobile device users affected by security threats were aged between 31 and 40 years (42%), followed by those aged 21-30 years (32.8%). Other groups represented in the sample were those aged less than 20 years (15.1%), those between 41-50 years (7.6%) and lastly those aged 51 years and above (2.5%). The frequency distribution of age can also be shown using a histogram inscribed with a normal curve.

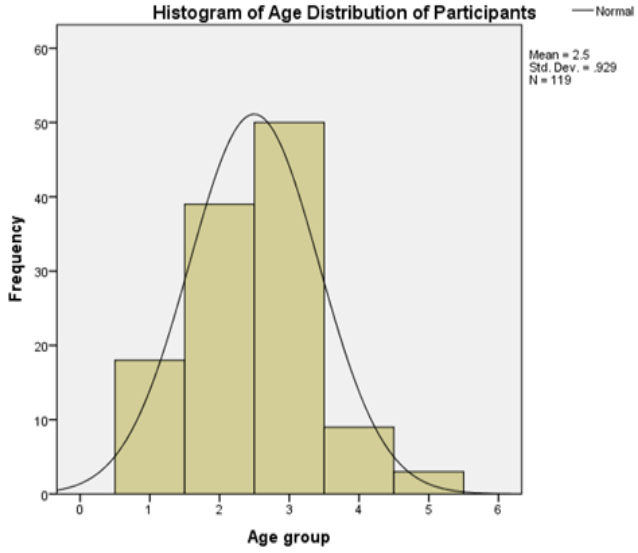

Figure 1.2: Histogram Showing Age Distribution

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Concerning the level of Education of the study participants, Table 1.2 shows that 37% of the respondents had Associate degree-level education, 28.6% had obtained degree-level qualifications, 26.1% had completed high school education and 8.4% had graduate/post-graduate level education. These results thus establish that most respondents had College diploma-level education. The distribution of study participants' level of education can also be displayed with the use of a bar graph.

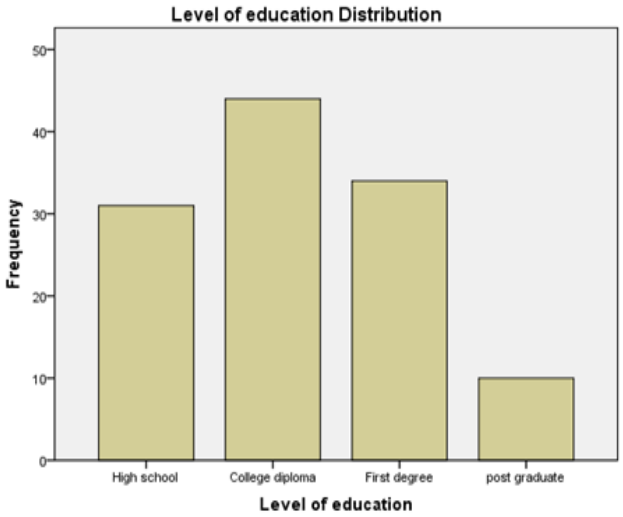

Figure 1.3: Bar Graph Showing Level of Education

Lastly, mobile device users participating in the study were also asked about their socio-economic status. According to the results in Table 1.2, 49.6% of respondents were found to be of low socio-economic status, 36.1% were of moderate socio-economic status, and 14.3% were of high socio-economic status. These results showed that most mobile device users participating in the study were of a low socio-economic background. These results can also be exhibited using a pie chart.

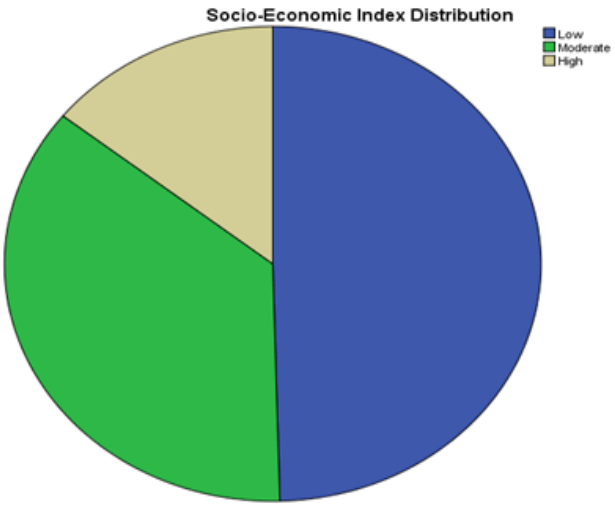

Figure 1.4: Pie Chart of Socio-Economic Status

3.3. Common Mobile Device Security Threats and Vulnerabilities

Study participants were also asked whether they had encountered or experienced mobile device software security threats and vulnerabilities while using their smartphones. Their responses were categorized into either "Yes/No /or Unsure. The results are as shown below.

Table 1.3: Frequency Distribution of Encounter with Mobile Security Threats

Response	Frequency	Percent	Cumulative Percent
Yes	85	71.4	71.4
No	24	20.2	91.6
Unsure	10	8.4	100.0
Total	**119**	**100.0**	

In research question (i), survey respondents were asked to identify common software security threats and vulnerabilities that impact mobile devices such as Smartphones, Tablets and other smart devices. Six software security threats were identified, and their effects on the usage of mobile devices were rated by survey participants. These results are analyzed in the table below.

Table 1.4: Frequency Distribution of Common Mobile Security Threats and Their Ratings

Factor	Response in %					Total
	Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree	
Rogue Application Threats	18.5	18.5	17.6	29.4	16.0	100
Adware Threats	21.0	24.4	19.3	19.3	16.0	100
Malware security threats	8.4	15.1	14.3	35.3	26.9	100
Cyber-attack Threats	7.6	21.8	24.4	30.3	16.0	100
Unlawful eavesdropping. Threats	21.0	31.9	31.1	16.0	0.0	100
SMS Spams	5.9	18.5	25.2	31.9	18.5	100

The results shown in Table 1.4 establish that most participants (29.4% and 16.0%) either agreed or strongly agreed that rogue applications are a threat to mobile device software, while a combined 37% disagreed or strongly disagreed that such posed a threat to device security.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

For adware, a majority disagreed or strongly disagreed (24.4% and 21.0% respectively) that adware constituted a security threat, while only a combined 35.3% either agreed or strongly agreed that adware posed a significant threat to mobile device security.

Malware was also acknowledged to be a major threat on mobile device software. Respectively, 35.3% and 26.9% agreed or strongly agreed that malware dangerous to mobile devices, while only a combined 23.5% of respondents disagreed or strongly disagreed with this claim. For cyber-attacks,

a combined 46.3% agreed or strongly agreed that cyber-attacks posed a threat to mobile device security, against a combined 29.4% who disagreed or strongly disagreed with this claim. A majority of 52.9% either disagreed or strongly disagreed that unlawful eavesdropping constituted a threat to mobile device security, against 16.0% who agreed. Lastly, a majority of participants, with a combined 50.4%, agreed or strongly agreed that SMS spam poses a significant threat to mobile device software, while only a combined 24.4% disagreed or strongly disagreed with this threat. This study also sought to quantify the mean and standard deviation of mobile software threats at a rated Likert scale of 5. The results are shown in the table below.

Table 1.5: Mean and Standard Deviation of Common Software Threats

Factor	N	Minimum	Maximum	Mean	Std. Deviation
Rogue Application Threats	119	1	5	3.06	1.367
Adware Threats	119	1	5	2.65	1.382
Malware security threats	119	1	5	3.57	1.266
Cyber-attack Threats	119	1	5	3.25	1.188
Unlawful eavesdropping. Threats	119	1	4	2.42	.996
SMS Spams	119	1	5	3.39	1.158

The results held in Table 1.5 show that rogue applications (μ=3.06, σ=1.367), malware (μ=3.57, σ=1.266), cyber-attacks (μ=3.25, σ=1.188) and SMS spam (μ=3.39, σ=1.158) were the most significant software threats affecting mobile device users, since their mean scores were greater than 3.0 on a scale of 1 - 5.

3.4. The Total Number of User Downloads per Operating System of Mobile Devices

In this section, the study sought to identify the number of downloads per user, as well as the type of mobile device operating system used, and determine whether a disparity exists in exposure to security threats based on these factors. Cross tabulation and analysis of variance (ANOVA) techniques were used for this analysis.

Table 1.6 below shows the cross tabulation results for total number of downloads per mobile device operating systems. The number of user downloads were categorized as low, moderate or high, while two types of mobile device operating systems were identified - Android and iOS.

Table 1.6: Cross Tabulation of Operating System against Number of Downloads

			Number of Downloads Per User			Total
			Low	Moderate	High	
Type of operating systems	Android	Count	19	47	29	95
		% of total	16.0%	39.5%	24.4%	79.8%
	iOS	Count	4	11	9	24
		% of total	3.4%	9.2%	7.6%	20.2%
Total		Count	23	58	38	119
		% of total	19.3%	48.7%	31.9%	100.0%

Results from Table 1.6 shows that 79.8% of respondents operate smartphones or tablets which utilized the Android Operating System, while 20.2% utilized devices with iOS. Furthermore, 16.0% of participants who used the Android operating system devices had lower number of downloads as compared. 39.5% of Android Device users had a moderate number of downloads, and 24.4% had a high number of downloads on the same software platform. Conversely, 3.4%, 9.2% and 7.6% of iOS users had a low, moderate and high number of downloads, respectively. These results can also be shown using a clustered bar chart.

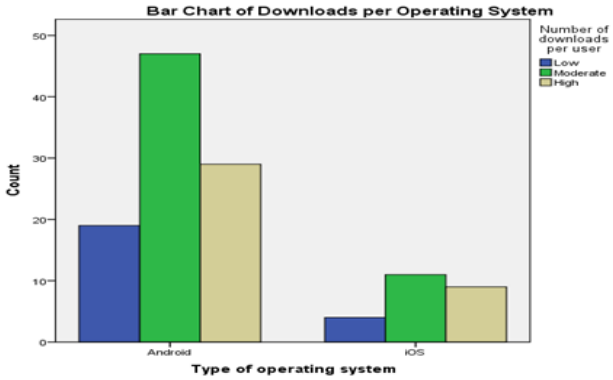

Figure 1.5: Bar Chart Showing Number of Downloads vs Operating System

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

It is difficult to make accurate comparisons from the results above, given that a large majority of respondents use devices with the Android Operating System, hence Android has a significantly higher number of downloads. In the subsequent section, this study analyzes whether there is a difference in the prevalence of mobile device security threats between the two operating systems with reference to the number of downloads per user.

Table 1.7: Analysis of Variance (ANOVA)

		Sum of squares	DF	Mean square	F	Sig.
Type of Operating Systems	Between groups	6.182	2	3.091	18.848	0
	Within groups	18.978	116	0.164		
	Total	19.16	118			
Number of Downloads per user	Between groups	12.927	2	6.464	12..928	0
	Within groups	58.182	116	0.502		
	Total	59.109	118			

Table 1.7 shows that the type of operating systems used significantly influences the rate of Mobile Device Software Threats, with an F-statistic of 18.848 and a p-value of 0.000. Therefore, we can conclude that Android Mobile Device operating system is significantly more vulnerable to software security vulnerabilities and threats when compared to the iOS operating system. These results also indicate that the number of downloads per mobile device user affects the security status of a device. The statistics show an F-statistic = 12.928 and a p-value of 0.000, this indicates that the total number of downloads per user determines the extent of mobile device security threats and vulnerabilities for any given device.

3.5. Impact on Mobile Device Security of Software Security and Demographic Factors

This section addresses research questions (iv) and (v), which determines whether mobile device security threats and vulnerabilities are influenced by demographic factors, and whether device security is affected by the total number of downloads per user and the type of mobile device operating systems prevalent. The data relevant to this section was analyzed using multiple regression analysis.

Table 1.8: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
Regression	.792[a]	.627	.615	.041

a. Predictors: (Constant), number of downloads per user, age group, gender/ sex, type of operating system, socio-economic index, level of education

Table 1.8 shows that the R statistic for this regression analysis is 0.792, while the R-squared value is 0.627. Therefore, the results show that mobile device security is strongly dependent on the stated variables (device factors and demographic factors). The explained variation in the mobile device security statistic is about 62.7%, arising from the R-squared statistic. Relying upon these results, it can be concluded that 62.7% of mobile device security can be predicted with reference to mobile device and demographic factors. Similar conclusions are reached using ANOVA of the regression analysis:

Table 1.9: ANOVA of Multiple Regression

Model		Sum of squares	df	Mean square	F	Sig.
Regression	Regression	9.766	6	1.628	3.971	.001
	Residual	45.965	112	.410		
	Total	47.731	118			

a. Dependent variable: Whether user has experienced /suffered MDS threat
b. Predictors: (Constant), number of downloads per user, age group, gender/ sex, type of operating system, socio-economic index, level of education

The results of this ANOVA show an F-ratio of 3.971, with a p-value of 0.001. Since the p-value is less than 0.05, the regression can be deemed significant for both prediction and explanatory purposes. Lastly, it is useful to examine the coefficients of the model that explain and predict the outcomes of mobile device security. Table 1.10 below shows the coefficients of the model.

Table 1.10: Model Coefficient

Model		Coefficients		t	Sig.
		B	Std. error		
Regression	(Constant)	1.869	.414	4.512	.000
	Age group	-1.312	.064	-2.496	.001
	Gender/ sex	-.064	.121	-.527	.299
	Level of education	-1.191	.065	-1.905	.013
	Socio-economic index	.083	.083	.997	.121
	Type of operating system	-2.112	.148	-1.757	.041
	Number of downloads per user	2.066	.084	1.783	.035

a. Dependent variable: mobile device security threat

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table 1.10 shows that the constant (t=4.512, p=0.000), age group (t=-2.496, p=0.001), level of education (t=-1.905, p=0.013), type of operating system (t=-1.757, p=0.041) and number of downloads per user (t=1.783, p=0.035) have p-values less than 0.05. Therefore, these factors are significant in modeling mobile device security. The other variables, including gender (t=-0.527, p=0.229) and socio-economic status (t=-0.997, p=0.121) have p-values of less than 0.05, and hence they have no significant influence on mobile device security. From the β coefficients, the model is made up of the following significant variables: constant (β=1.869), age group (β=-1.312), level of education (β=-1.191), type of operating system (β=-2.112), and number of downloads per user (β=2.066). Gender (β=-0.064) and socio-economic status (β=0.083) are non-significant in the model.

This model can be written mathematically as:
MDS=1.869-1.312AG-1.191ED-2.112*OS+2.066ND-0.064GE+0.083SE
Where: MDS is mobile device security
AG is Age
ED is Education
OS is Operating systems
ND is Number of Downloads
GE is Gender
SE is Socio-Economic Status

IV. SUMMARY OF RESULTS

Table 1.11 below offers a summary of the Data Analysis results with reference to the research objectives of the study.

Table 1.11: Summary of Results

	Research objective	Result
1	Identify the common software security threats and vulnerabilities that affect usage of mobile devices.	Rogue applications (μ=3.06, σ=1.367), malwares (μ=3.57, σ=1.266), cyber-attacks (μ=3.25, σ=1.188) and SMS spam (μ=3.39, σ=1.158) were identified as significant software threats on mobile device usage.
2	Determine the effectiveness of mobile security solutions provided by device vendors in addressing software security threats.	The type of operating system used significantly influences the mobile device software threats with F-statistic of 18.848 and p-value of 0.000. Number of downloads per mobile device user also affects the devices' security status. According to the results, F-statistic=12.928 and p-value is 0.000.
3	Establish the number of downloads per mobile device user and the operating systems of mobile devices.	• 16.0% of participants who used the Android operating system had a low number of downloads, while 39.5% had a moderate and 24.4% a high number of downloads • 3.4%, 9.2% and 7.6% of iOS users had low, moderate and high numbers of downloads respectively.
4	Consider the effects of the number of downloads per user, the type of operating systems, and user demographic factors on mobile device security.	The optimal regression model found constant (β=1.869), age group (β=-1.312), level of education (β=-1.191), type of operating system (β=-2.112) and number of downloads per user (β=2.066) to be significant variables. $$MDS = 1.869 - 1.312AG - 1.191ED - 2.112 * OS + 2.066ND - 0.064GE + 0.083SE$$

V. CONCLUSION

In terms of the most common security threats for mobile device users, the study concluded that a majority of mobile device users (29.4% and 16.0%) are affected by rogue applications, compared to 37% who are not. Another common security threat that was identified by the study is malware, with 62.2% of users affected, compared to only 23.5% who were not affected. These results are in agreement with Yaseen & Tariq (2012), who indicated that malicious software poses an immense threat to users of both Android and iOS Operating systems.

In terms of cyber-attacks caused by rogue applications or unwanted pop-up SMS and intrusion, a combined 46.3% of mobile device users generally agreed that cyber-attacks constituted a threat to mobile device software, compared to a combined 29.4% who disagreed with this claim. Lastly, most mobile device users (50.4%) agreed that SMS spam was a frequent threat to mobile device users, while only 24.4% disagreed that such constituted a threat. This assertion is also supported by Gao & Liu (2013), who indicated that SMS spam could easily be manipulated to allow infiltration of mobile device viruses into other systems. Regarding the assessment of the effectiveness of mobile security solutions by mobile device vendors in addressing software security threats and vulnerabilities, this study Found that, the type of device operating system significantly influences the susceptibility of a mobile device to software threats (F=18.848 and p-value=0.000). The Android mobile device operating system was deemed highly affected by software security threats when compared to the iOS operating system.

The study also concluded that the total number of downloads per mobile device user has an impact on a device's security status (F =12.928 and p-value=0.000). This finding implied that the number of downloads per user determines the extent of mobile device security threats and vulnerabilities. These results were in agreement with those outlined in the Mobile Device Security Threat Report (2015), which held that the number of mobile software security threats in a used device increased with number of downloads. The results of the study also found that the age group and level of education of mobile device users were the only demographic factors that significantly influenced mobile software security, while gender and the socio-economic status had no significant influence. The type of operating system and number of downloads per user were also found to be device factors affecting software security. From the established β coefficients, the mathematical model obtained was:

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

MDS=1.869-1.312AG-1.191ED-2.112*OS+2.066ND-0.064GE+0.083SE

This model clearly establishes that that mobile device security threats (MDS) will decrease by 1.312 when the age factor (age group) increases by one, while other factors held constant. Similarly, when education level increases by one, the MDS decreases by 1.191, and when operating system changes from one level to another (Android to iOS) the MDS decreases by 2.112. The final significant variable in the model showed that, when the number of downloads increases by one level, the MDS also increases by 2.066.

REFERENCES

1. Christian, M. (2014). Integrating Cloud Computing and Mobile Applications: A Comparative Study Based on Cloud and Sanscode, Journal of Cloud Computing. 2(14) 1-9.
2. Gao, C, and Liu J. (2013). Modeling and Restraining Mobile Virus Propagation. IEEE Transactions on Mobile Computing, 12(3): 529-541.
3. Greenberg, A. (2010). Google Pulls App that Revealed Android Flaw, Issues Fix, http://news.cnet.com/8301-270803-20022545-245.html.
4. Harris, M, and Patten, K. (2013). Mobile Device Security Considerations for Small- and Medium-Sized Enterprise Business Mobility Integrated Information Technology, Information Management and Computer Science, 22(1): 97-144
5. Liu, D, Zhang, and Hu, K. (2013). A Survey on Smartphone Security, Applied Mechanics and Materials, (Vol 347-350): 3861-3865.
6. Mavridis, I., & Pangalos, G. (2012). Security Issues in a Mobile Computing Paradigm. In I. Mavridis, & G. Pangalos, Communications and Multimedia Security (pp. 61-76). Springer US.
7. Park, J., Yi, K and Jeong, Y. (2014). An Enhanced Smartphone Security Model based on Information Security Management Systems, Electronic Commerce Research, 14(3): 321-348.
8. Patten, K and Passerini, K. (2007). Next Generation Small and Medium Enterprises Mobility Strategy Roadmap, Proceedings of ISOneWorldConference, Las Vegas, NV, 11-13 April.
9. Waltz, M. (2011). Mobility Threats, Mobile Enterprise, 7 March, Accessed 9 Februrary 2013, http://mobileenterp rise.edgl.com/top-stories/Mobility-Threats71022
10. Wei, J and Ozok, A. (2009). Development of a Mobile Commerce Security Analysis Method. Journal of Information Privacy & Security 5: 1; 28.
11. Yaseen, B, and Tariq, M. (2012). Technical Comparison Between Android And IOS With Respect to Their Architecture. Technical Report Documentation Page, Punjab University College of Information Technology, University (PUCIT), Report No:BCSF09A: 1- 16.
12. Lookout, 2013. "2013 Mobile Threat Predictions", Accessed 11 Februrary 2013,https://blog.lookout.com/blog/2012/12/13/2013-mobile-threat-predictions/
13. Stat counter, 2013. "Top 8 Mobile Operating Systems in the United States from Jan 2012 to Jan 2013", Stat Counter Global Stats, accessed 12 February 2013,http://gs.statcounter.com/#mobile_osUS-monthly-201201-

About the Author

Dr. Richmond S. Adebiaye is currently an Associate Professor and Head of Information Systems in the College of Information Technology at Ajman University, UAE. He was the former Program Director of Computer & Information Science at Parker University, Dallas, Texas USA, former Program Chair, CS/IT, Denver Campuses of Colorado Technical University and former Program Director at the University of Maryland University College. Dr. Adebiaye earned his Doctorate (PhD) in Information Systems and Communications from the prestigious Robert Morris University, Moon Township, PA and also author of four (4) best-selling textbooks – (1) Object-Oriented Methods - ISBN-13: 978-1482792782, (2) Information and Network Security Management: ISBN-13: 978-1491236338, (3) Network Systems and Security (ISBN-13: 978-1492130796 and (4) Network Systems Management - ISBN-13: 978-14826267 . He also authored a novel named "Efun" ISBN-13: 978-1534981720, which has been ranked a best seller in the fiction category by Amazon.com. Dr. Adebiaye's extra-curricular activities include reading, researching and watching American Football Sure is

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)