THE USER'S SKILLS, CAPACITY ON SECURITY FOR MOBILE COMPUTING IN UNIVERSITIES

Daniel Otanga; Kibabii University
Frankin Wabwoba; Kibabii University
Leonard Wamocho Samita; Masinde Muliro University

Abstract

Universities are shifting from partially computerized to fully automated environments and technology is equally shifting from point to point to broadcasting options. These trends are resulting in mobile computing for most university users with systems accumulating enormous amount of public, private as well as confidential data on employee, students and the institution. However, mobile computing systems normally come with security issues and different vulnerabilities that make users hesitate adopting them despite the many benefits they bring. The purpose of this paper was to establish the user skills capacity on security in mobile computing environment in universities. This part of the study was undertaken using survey design and scrutiny of literature review. Stratified random sampling and purposeful sampling was used to select respondents from six public and two private universities. The study found out the users skills capacity in the universities to be fairly moderate. The findings will help the university management determine the skills required in handling information on mobile computing in universities. The findings will also enhance the existing security approaches to mobile computing in universities and mitigate on the future trends in security for information systems.

Key words: Information System Security, Information Technology, Trends, Security Approaches, Threats, Vulnerability.

1.0 Introduction

Security in information systems is posing challenges to organizations as they adopt new technologies such as mobile computing and as the trends in technology change. According to Artjom, (2010) Mobile computing is the most current technology, where mobile phones can do everything a computer could, including web browsing, document processing, and playing games among others. Mobile computing is a means of using a computer or any computing device while outside or within an office setup. According to Archer, (2012) the means to perform mobile computing involves using mobile devices to remotely connect to corporate office, home computers, laptops, tablets or smartphones. Mobile computing is becoming increasingly important due to the increase in the number of portable components and the desire to have continuous network connectivity to the internet irrespective of physical location of the node, (Goswami, 2013).

Demand by users of university services have put pressure on the management to provide services 24 hours a day. In order to achieve these, universities have made effort to automate processes for efficient and effective operations. The Universities have also adopted and even developed information systems which operate in networked environments through point to point as well as broadcast options. Most staff and students are using their own mobile devices such as ipad, tablets, smartphones, and laptops among others to carry out some of transactions using university information systems while in their comfort zones. According to IBM, (2008) mobile devices represent the greatest intersection between opportunities and risk among the available technologies. The mobile devices are diverse in design and use and are capable of delivering data applications and services anytime anywhere. The devices offer a new prevalent channel for conducting business and primary means for authentication (IBM, 2008).

Security approaches for the mobile computing devices and applications in organizations are also becoming a crucial undertaking for the organizations due to the dynamic technology. Mobile computing technology is being adopted for various operations in universities by individuals and university management. As a result of these operational trends in the organizations, security in the mobile computing is increasingly becoming a challenge for those responsible in ensuring confidentiality, integrity and availability of information within the universities information systems.

Safeguards approaches

One of the main challenges that mobile devices pose to organization is distinguishing between employee-owned and organization-issued equipment. BYOD may seem cost effective solution for an organization but the ability to manage and control such devices is a challenge, especially trying to apply security policies and corporate software (Archer, 2012). Some of the security mechanisms applied according to Archer, (2012) include; user-oriented methods outlined as ; physical control, user authentication, data backup, wireless interfaces, deactivate compromised devices among others. The other approach is organization oriented which includes; mobile device usage policy, deployment and operation plans, risk assessment and management, security awareness and configuration and control management. NIST 800-124 guideline is a generic technical document for organizations to help protect mobile devices. It lists threats and safeguards without any connections.

According to Flo and Josang (2009) user's guidelines limit the cover area, listing possible attacks without grouping them or leave one without knowledge of other similar attacks and where they may come from. Access to LAN by unauthorized mobile devices can be prevented by establishing Message Authentication Code (MAC) addresses, a unique number that identifies its Network Interfacing Card (NIC). Unknown computers can then be denied access if their MAC address is not on an authorized list (McKimmy, 2003). In the area of telecommunication, network security, the IBM Blandecenter PN41 provides customizable deep packet inspection (DPI) based security capabilities that telecommunication networks can use to protect mobile devices from malware and other security threats. According to Wambugu, (2015) there are a number of approaches that can be used to protect laptops, besides physically locking your laptop to an immovable object; you could use a new breed of security software now in the market.

The approaches mentioned above are not clear on the current wireless technology which facilitates mobile computing. This study sought to identify and address the security vulnerability and threats brought by the use of mobile devices on university systems. Universities also have employees and students all with their own mobile devices which they use for information processing and access, a security approach for such devices is not very clear. Previous studies also do not address the issue of determining the level of security of information in organizations. This study sought to address this situation by an evaluation model which was developed.

Adoption of mobile computing system

Information systems are experiencing speedy change owing to the recent evolution of the ubiquitous computing network, and as a result YoonJung, (2006) noted that, information system products are showing diversification and rapid change. Organizations of all types are struggling to understand how to embrace innovation without creating new security gaps or widening known ones. More employees are using their smartphones and tablets for work in the organization, creating a surge of consumer mobile devices accessing corporate networks and storing corporate data (Dekker, 2013). According to CISCO report (2014), the year 2013 also brought the issue of trust to the forefront. Users of all types are now even more likely to question the trustworthiness of the technology they rely on every day whether at work or in their personal lives.

Ensemble devices with integrated tools are developing rapidly and these ensemble mobile devices are turning into a ubiquitous environment that gives rise to the option of mobile computing (Sheila et al. 2015). According to a study by Rapetti et al. (2011), mobile devices are pivotal in students' every life and mobile technology is the element that unites informal and formal patterns of scholarship.

Enterprises are opting for new enterprise mobility management capabilities that complement device management by mobilizing and containerizing business apps and content. According to the whitepaper, (2015) many organizations realization of full potential of mobility still lies over the horizon. According to computer world, (2015) forecast study; many companies adopted MDM as a means to solve an immediate problem. The report further noted that organizations are looking to move beyond problem solving and utilizing mobile as a key element in their business strategies. According to Reed, (2015) the key issues determining mobile management strategy are identifying the roles that are being mobilized, determining what tasks they need to be able to do with a mobile device and finding a way to securely provide the mobile apps that will enable tasks and workflows on mobile devices.

In an effort to computerize services Universities are adopting information systems acquired through purchasing or developed from the scratch and customized to suit their needs. Most of the universities borrow technological ideas from each other because most of the services offered in these universities are similar. Thus most of the information systems adopted by the universities are the same in one way or the other. This study examined the various information systems that are being adopted in the universities to establish whether such systems are secured appropriately.

Impact of ICT Policies to computing

Policies guide organizations in proper management processes, resources and other issues that require order. According to Gordon, (2010) structural policy challenges are normally on policy development. Gordon, (2010) further looks at the representation in the making process and whether the members involved have the capacity to develop a policy. Process ICT challenges include the underlying assumption driven by the managers of the institutions developing the policy and how they identify those involved in policy development.

In all cases the production of an objectively appropriate ICT policy and its effective implementation is important.

Ramsey, (2010) observed that good leadership is a solution to a good working policy. Universities have ICT policies that guide the employees on how to address key issues in mobile computing. This study scrutinizes some of the policies available to establish whether they are addressing security in mobile computing in those universities. A policy that is intended to manage the risks of mobile computing and manage privately owned mobile devices that access the university systems will make the mobile computing processes in the university effective.

Finding and Discussions

User skills

The researcher sought to find out the respondents' agreement with the following statements on the scale ranging from 1 for yes and 3 for don't know. The results are as shown in table 1,

The study wanted to establish the users understanding capabilities on the emerging security challenges in their institutions and how they handle such challenges.

Table 1 Descriptive statistics on user skills

Descriptive Statistics	**Yes**	**No**	**Don't know**	**Mean**	**STDV**
Challenges in security measures application	37.5	55	6.5	1.7071	0.62682
Formal training conducted	43.4	49.5	7	1.6364	0.6137
Existence of security policy in the University	60.5	18	20.5	1.9899	0.9090
Are all employees and external parties informed about the security policy	30.3	46.5	23	1.9293	0.7319
Have you read and understood your institutions information systems policy	37.4	47.5	15.2	1.7778	0.69334
Are there repercussions for violating the information systems security policy	60.6	5.1	34.3	1.7790	1.1064
Does existence of security policy have an impact	58.6	25.2	16.2	1.6970	1.1064

The study established that 37% of the respondents had challenges in applying security measures on university system, 55% of the respondents had no challenges in applying security measures on the security systems in the university this explains why there is need to determine the approaches of handling the various attacks in the current technological advancement, 6.5% of the respondents did not understand the concept. The statement on challenges of applying security measures had a mean of 1.7071 and a standard deviation of 0.62682. Based on the findings majority 55% of the respondents had no challenges in security measures applications for their information systems. With mean of 1.7071 and a standard deviation of 0.62682, it shows that there were small variations on the respondents view on challenges encountered in security of information systems.

This means that there was consistency from the respondents' views with a mean of 1.7071 a majority of respondents had no challenges in applying security measures on security systems of the university. The various security approaches on university systems vary from one university to the other depending on a number of factors including management involvement and support, security policy development and implementation among others thus each user in their area of operations are guided in their operations by the existing conditions at their place of work.

The study further found out that 43% of respondents had a formal training to enable them safely operate the existing systems, 49% of the respondents did not go through formal training for the existing systems while 20% of the respondents did not know the existence of the training. These results explain why there are frequent attacks on the university information systems. The response on this statement had a mean of 1.6364 with a standard deviation of 0.6137. Skilled and qualified personnel are important to the development and utilization of technology (Munyua, 2010). Formal training equips users with skills to enable them handle the information security challenges in the ever changing technology, 43% of the respondents confirmed going through formal training on security matters while 49% did not go through the training . The mean of 1.6364 and a standard deviation of 0.6137 means there was a small variation for the respondents view about formal training on security issues in the university and a majority of the respondents were positive about the formal training to enable them acquires skills on safeguarding information systems. The lack of formal training on security issues by majority of respondent's points to staff lack of vital information on system security in mobile computing environment

On the existence of security policy, 60% of respondent confirmed the existence of security policy in the university, 18% of respondent had not seen the security policy, while 20.5% were not aware of the security policy in the university. This statement had a mean of 1.9899 and a standard deviation of 0.9090. Based on this mean and standard deviation on the existence of security policy, there was slightly high deviation of respondents view on existence of security policy in the university.

According to Abdullah, (2010) the internet and computer networking requires new security measures and policies to reduce the threats and challenges from the new technologies and software applications and network mobile devices. The respondents were positive about the existence of security policy in the universities to address the emerging security challenges. This is evidenced by the mean of 1.9899. Findings show that most university have already developed a security policy that guides them on matters of security for their systems in computing environment, however some staff are not aware of the existence of the document implying that they have no guidelines in their security operations exposing the information systems to security risks.

The study sought to establish whether other employees are informed about the security policy in the university, 30.3% of the respondents confirmed that staffs are made aware of the security policy in the university, 46.5% of the respondents indicated that staff are not made aware of the security policy while 23% of the respondents did not know the existence of the security policy. This statement had a mean of 1.9293 and a standard deviation of 0.7319. Having knowledge about existence of security policy would ensure that staffs utilize the policy for the sake of safeguarding information systems in the university. Findings further shows that there were minimal deviations from respondents at 0.7319 standard deviation and majority of the staff were positive about knowing the existence of security policy in the university. The results show lack of staff awareness on matters of security policy in the university and thus the staff inability to handle security challenges they are not aware of and as such exposing information systems to security risks and in the process increasing security attacks on university information systems.

As to whether the respondents had read and understood the security policy 37.4% of respondents had read and understood their institutions systems security policy, 47.5% of respondent had not read and understood the institutions system security policy, while 15.2 % of the respondents were not aware of the institutions system security policy. The findings reinforce the fact that staffs were not adequately informed about the security policy in their institutions. The response in this category had a mean of 1.7778 and a standard deviation of 0.69334. This means that a majority of staff were aware about the security policy but they had not read and understood the document. The respondents were fairly consistent at standard deviation of 0.69334. Though universities have security policy, majority of staff have not read and understood the document. These findings also points at the lack of staff awareness on matters of security that could help them address the security challenge issues on the university information systems and handle high frequency of attacks on such systems.

On having repercussions for violating information system security, 60.6% of the respondents confirmed punishment of some sort to those violating the policy, 5.1% of the respondents did not confirm any punishment for those violating the system security policy while 34.4% of the respondents did not have any idea for the actions taken when one violets the policy. This statement had a mean of 1.7790 and a standard deviation of 1.1064. This means that there was a large deviation at 1.1064 from staff response to the statement at the same time majority of staff respondent to the statement at 1.7790. Findings show that majority of staff are aware of consequences of not complying with security policy but some still go against some of its provisions exposing the systems to security risks.

Policies allow an organization to set practices and procedures in place that will reduce the likelihood of an attack or an incident and will minimize the damage caused (Charl, 2001). According to Gordon, (2010) policies guide organizations in proper management processes, resources and other issues that require order. For a security policy to have impact on information system, it must be well coordinated. Based on the findings the existence of security policy had an impact on information system security implementation in the university, 58.6% of the respondents agreed that the existence of the policy had an impact on implementation of information security in the university, 25.2% of the respondents said there was no impact on information security implementation in the universities, while 16.2% of the respondents did not know if there was any impact. This statement had a mean of 1.6970 and a standard deviation of 1.1064. Majority of staff were aware of impact to system security implementation as a result of security policy, thus the respondents were very positive about the statement; however large deviations were witnessed from the findings on staff response on the statement at 1.1064. Security policy if well implemented goes a long way in protecting the information security in the universities. The proposed model has put emphasis on the need to have a security policy incorporated in the model and at the same time train and make the users aware of the policy provisions. This will enable the users effectively handle security issues in mobile computing environment.

Users knowledge on Security in University

The researcher further wanted to establish the extent of agreement to various statements on the scale ranging from 1 strongly disagreed and 5 strongly agreed by the respondents concerning their knowledge of security in university. The findings are as shown in table 2.

Table 2 Descriptive statistics on user skills- policy development and implementation

Descriptive statistics	SD	D	UD	A	SA	Mean	STDV
Installation security system is a sound investment for University	16.2	9	5	30	30	3.6768	1.4766
The security needs of a University differ depending on information system and their devices	15.2	19.2	2	49.5	14.1	3.2828	1.34043
Extra security features focus on integrating safety into the system or allow user to monitor it via mobile or remote	13.1	11.1	3	48.5	24.2	3.5960	1.3242
Every security system should have basic features	17.2	6.1	3	47.5	26.2	3.5960	1.3918
Security system manufacturers are continually making products more effective and user friendly	11.1	13.1	2	52.5	21.2	3.5960	1.2690

Key **SD** Strongly disagree **D** Disagree **UD** Undecided **A** Agree **SA** Strongly Agree

The findings shows that 30% of the respondents strongly agreed and agreed respectively that installing a security system was a sound investment for a university, 16.2% of respondent strongly disagreed with the statement of installing security system in the university being sound investment in the university, 6% of the respondents disagreed with the statement while 5% of the respondent did not have an idea about the statement. The statement had a mean of 3.6768 and a standard deviation of 1.4766. The response rate for this statement was high meaning that more staff gave their views regarding the installation of security system in the university; however there were large deviations at 1.4766 from the response on how each of the respondents viewed the statement. The staffs were therefore positive that installing of security system in the university was a sound investment for the university. This also means that there is need for management support on the provision of the required funds for the security system installation and implementation in universities. From the findings the management support to ensure proper security systems are put in place is vital and that such security systems are updated from time to time to reflect the dynamics in mobile computing environment.

The study also sought to find out the views of the respondents on the statement that the security needs of a university differ greatly depending on information systems and their devices, 49.5% of the respondents agreed with the statement, 14.1% of the respondents strongly agreed with the statement, 15.2% of the respondents strongly disagreed with the statement, 19.2% of the respondent disagreed with the statement while 2% indicated that they did not know the concept. The statement had a mean of 3.2828 and a standard deviation of 1.34043. This means that more staff agreed to the fact that security needs of universities differ depending on information systems and their devices. Though there is a common ground regarding issues of security of information systems in mobile computing for universities, different universities might be having different hardware systems which might require different approaches to secure such systems. There was a deviation of 1.34043 on the respondent's views on universities having different security needs depending on information systems and devices for the universities showing consistency from respondents.

On the instances of theft of information and other crimes being lower in the universities that have a security system installed, 24.2% of the respondents strongly agreed with the statement, 48.5% of the respondents agreed, 13.1% of the respondent strongly disagreed with the statement , 11.1% of the respondents disagreed while 3% of the respondent did not know. The statement had a mean of 3.5960 and a standard deviation of 1.3242. From the findings, most University staff noted that there was a decrease in instances of theft of information and other crimes in the universities installed with a security system. By having the most advanced security systems that can address security issues in the current technological advancements, university reduces to a great extent incidences of information theft and other related crimes in its computing environment. The statement had slightly high deviations at 1.3242 from the respondents indicating consistency in their views.

The study also sought to establish whether some extra security system features also focus on integrating safety into the system or allowing the user to monitor it via remote or mobile devices. The findings shows that 48.5% of the respondent agreed with the statement, 24.2% of the respondents strongly agreed with the statement, 13.1% of the respondent strongly disagreed, 11% of the respondent disagreed while 3% of the responded indicated that they did not know. The statement had a mean of 3.5960 with a standard deviation of 1.3342. Integrating safety into information systems as they are developed enhances the systems effectiveness in one way or the other. Majority of the staff in the university were in agreement with this concept while a few strongly disagreed. There were slightly high deviations from the respondent's view of the statement at 1.3342. Current technology in system development has seen most software developers integrate security functionality as they develop the systems.

The staffs were also required to confirm whether every security system should have some basic features. The findings show that 26.2% of the respondents strongly agreed that every security system should have some basic features, 47.5% of the respondent agreed with the statement , 17.2% of the respondents strongly disagreed with the statement , 6.1% of the respondent disagreed while 3% of the respondent did not have an idea on the statement. The statement had a mean of 3.5960 and a standard deviation of 1.3918. Majority of staff agreed that there was need for every system to have some basic features, the deviations from respondents for the statement was also minimal which means most of the respondent's views were positive. Some of the basic features that are required for the security systems include among others help, user's manual for ease of use for such systems.

The study stated that security system manufacturers had continually working to not only make their products more effective but also increasingly easy to use. The findings show that 21.2% of the respondent strongly agreed with the statement, 52.5% of the respondent agreed with the statement, 11.1% of the respondent strongly disagreed with the statement, 13.1% of the respondent disagreed with the statement while 2% of the respondents did not understand the statement. The statement had a mean of 3.5960 and a standard deviation of 1.2690. Majority of new systems have improved interface making them friendlier to users. Most of the respondents were in agreement with this statement as it can be seen from table 4.9. The standard deviation of 1.2690 shows there was minimum variations on views from the respondents on the statement. The current technology has been geared towards ensuring that there is no memory loads on users of such systems to ensure also that the users are encouraged and eager to use the security systems to enhance security in mobile computing environment. Systems that are hard to operate are avoided by users and thus expose the information systems to security risks. The component on user skills and technical operations are captured in the proposed model and have direct links on the way manufacturers of the security systems design and develop such systems to make them easy to use.

Operationalization of Security policy

The study wanted to find out how universities were utilizing the security policy. The findings are as shown in Table 3. This was to establish whether users actually understand how the policy operates.

Table 3 Descriptive statistics on security policy operationalization

Opinion Statement	Yes	No	Don't Know	Mean	STDV
Have information security policies and standard been developed and implemented	44.4	33.3	22.2	1.8788	0.9822
Do employees receive training on information security policies and standards	38.4	49.5	12.1	1.7374	0.6637
Have response procedure been established	42.6	40.4	17.0	1.8081	0.7912
Are third parties who connect your systems required to comply with your information security policies and standards	63.6	20.2	16.2	1.5859	0.83312
Are appropriate personnel notified in real time if a high risk threat is detected	56.5	22.2	21.2	1.7273	0.9348

The results from the table show that security policies have been developed and implemented in most universities at 44.4%. Those who indicated that the security policy had not been developed and implemented in their institutions were 33.3% while those who indicated that they had no idea of the whole process were 22.2%. The statement had a mean of 1.8788 and a standard deviation of 0.9822. This means that the majority of the staffs are aware of the utilization of the policy in the university. Security policy is a document that guides users on operation of information systems in a manner that does not expose the system on security risk. Lack of awareness can hinder technology implementation (Apulu & Latham, 2009). Awareness in regard to security policy is one of the key components that the proposed system contains and will be used in addressing this requirement. The response rate was high meaning that there was consistency from respondent's views.

On the employees training on security policy, 38% confirmed there being training, 49% of the respondents said there was no training for employees on security policy, while 12.1% of the responded did not know the existence of the process. This statement had a mean of 1.7374 and a standard deviation of 0.6637. Meaning that the response rate was high, Training on the utilization of a security policy is vital to the users to be able to understand the provisions of the policy and apply them, findings show that a majority of staff are not trained on the utilization of the security policy, and thus such staff are not able to apply the policy provisions appropriately exposing information systems to security risks. Training is a key component in the evaluation tool and proposed model and will thus be addressed at this level. There was minimal variation from the respondent's views on the staff training

On whether there was any response procedure if a system breach , virus infection or other information security occur, 42.6% confirmed that there was a response procedure, 40% of the respondents said there was no response procedure while 17.0% seem not to have any idea. This statement had a mean of 1.8081 and a standard deviation of 0.7912. To ensure that staffs are aware of the breach of the system, enables the users have a way to counter the security breach to avoid loses as a result of system attack. Almost a half of staff agreed to the existence of response procedure in the university meaning that a lot need to be done to ensure staffs are ready for any security eventuality that can occur in university systems in mobile computing environment. The variation from respondent's views was also minimum given that many of the respondents had convergent views on the statement.

As to whether the third party who connect to university system are required to comply with information system policy of the university, 63.6% of the responded confirmed that they must comply with security policy, 20.2% of respondents indicated that they do not comply, while 10.2% of the respondents had no idea of the process. This statement had a mean of 1.5859 and a standard deviation of 0.8332. As can be ascertained by Sheikh, (2009) the smartphones run complete operating systems that allow installation of third party applications, Sheikh further noted that as the usage of these devices grows, the need for securing the data stored on the devices and the services that they provide becomes more vital. Third party operators who connect to university systems need to comply with information system policy to safeguard the university system from external attacks in mobile computing environment, majority of staff confirmed this arrangement based on the findings, there was consistence in the staff response because the variations from the respondents was minimum.

On whether the appropriate personnel are notified in real-time if a high risk threat is detected, 56.5% of the respondents were in agreement that personnel are notified if a high risk threat is detected , 22.2% of the respondent said personnel are not notified when a security risk is detected, while 21.2% had no idea on the process. This statement had a mean of 1.7275 and a standard deviation of 0.9348. Knowing about the possibility of attack on the information system enables the users to mitigate and prepare to counter such attacks in mobile computing environment. Majority of the staff confirmed that notifications regarding the threats are made while the response rate was slightly high from the respondents view.

Conclusion

Based on the review of literature and data collection and analysis from universities, it was established that the users skills capacity in the universities to be fairly moderate given that some respondents had gone through some formal training on the emerging security issues to enable them address such issues in university systems. It was also established that the emerging security challenges in mobile computing to be on the rise due to change in technology and staff attitude and behavior. The security challenges in the university were also due to lack of technological skills to deal with dynamic technology, lack of security policy enforcement, lack of support from management, among others.

References

Abdullah (2010). Information Systems security measures and countermeasures; Protecting organizational assets from malicious attacks

Apulu I. & Latham A. (2009). Information and Communication Technology Adoption: Challenges for Nigerian SMEs. *TMC Academic Journal, 4(2), 64-80*

Artjom, (2010). Enhancing the hierarchical framework model of mobile security; Thesis Charl van der Walt, (2001) Security Focus Dekker, (2013). Technology trends and the impact on information security; SBS special report

Goswami, (2013). Mobile computing; *International Journal of Advanced research in Computer Science and Software Engineering*

McKimmy, P.B. (2003). Wireless mobile instructional labs: Issues and opportunities. *International Journal of Instructional Media, 30 (1):111 Methods Approaches, 2nd Edition, Sage Publications*, Thousand Oaks, California.

Munyua, A. W. (2010). Kenya in A Finlay, *Global Information Society Watch Focus on ICTs and Environmental Sustainability* (pp.161-163). APC and HIVOS ISBN 92-955049-96-9

Rapetti, E., Picco, A. and Vannini, S. (2011) 'Is mobile learning a resource in higher
education? Data evidence from empirical research in Ticino' *Journal of e-Learning and Knowledge society, vol 7*

Sheila M. Faizal M. A. and Shahrin 2015, Dimension of mobile security model: mobile user security threats and awareness. *International Journal Mobile learning and Organisation Vol 9, No 1*

Sheikh, (2009). Security evaluation of windows mobile Operating System Wambugu S. (2015). Sunday Nation September 20th 2015)White Paper, (2012). State of Mobility Survey, Research, 4(11): 1361-1370.