View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by International Institute for Science, Technology and Education (IISTE): E-Journals

Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.4, No.5, 2014
www.iiste.org

Lack of Awareness by End Users on Security Issues Affecting Mobile Banking: A Case Study of Kenyan Mobile Phone End Users

Anthony Luvanda[1*] Dr Stephen Kimani[1] Dr Micheal Kimwele[1]

1. School of Computing and Information Technology, Jomo Kenyatta University of Agriculture and Technology, PO Box 62000-00200 Nairobi Kenya

* E-mail of the corresponding author: luvanda@gmail.com

Abstract
The use of mobile phones in African has seen a formidable growth. The use of mobile phones to perform business and financial transactions seems to be on the increase as well. The rise in use of mobile phones to perform financial transactions also increases the risks associated with such transactions and especially man in the middle attacks. These compounded with lack of awareness among users means that they (the users) are highly exposed to such attacks. Due to the popular use of mobile banking in Kenya and the third world in particular, securing communication between the mobile device and the back end server has become a fundamental issue. This is due to the fact that hackers have the ability to steal banking information using various techniques, particularly the duping of mobile phone users to believe that they are communicating with a genuine program from their bank while in reality a user is simple giving away sensitive information to the hacker.
This paper aims to investigate the level of awareness among users of mobile banking transactions in regards to man in the middle attacks and whether the awareness or lack of it can increase or deter such attacks
Key words: mobile phones, Mobile banking services, Security, man in the middle attack,

1.0 Introduction

The use of mobile phones to perform banking transactions continues to grow at a rapid rate in Kenya. Especially with the advent of M-Pesa and the various mobile banking applications made available by a number of banking institutions. M-Pesa (M for mobile and Pesa being a Swahili word for money) is a mobile-phone based money transfer and micro financing service for Safaricom, the largest mobile network operators in Kenya. It is urguably the most developed mobile Payment system in the world. (CCK 2012) M-Pesa allows users with a national ID card or passport to deposit, withdraw, and transfer money easily with a mobile device which in almost all cases will be the simplest of mobile phones.
Most banks operating in Kenya, the likes of Standard chartered bank, Kenya commercial bank, commercial bank of Africa, Barclays banks and even micro finance institutions such as Faulu Kenya do provide mobile banking services for their customers. This services will range from viewing of mini-statement, Funds Transfers, Credit Card Information in regards to available balance and payments due dates, Customer Service Requests for adhoc statements, Banker's cheques, New PIN requests for Card or internet banking and information services such as branch locations, ATM locations, Foreign exchange rates and contact details. All the aforementioned banks have even gone a step further and integrated the M-Pesa application to their mobile banking services where they enable their customers to withdraw money from their personal bank accounts and deposit it into the M-Pesa application on their mobile phones. From there the customer can make further financial transactions such as pay bills, purchase items and even transfer money to another individual using the M-Pesa application on their mobile phone handset.
This convenience in banking, based mainly on mobile applications, does offer security challenges however, with the highest potential threat being a man in the middle attack. A Man In The Middle attack is one in which the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other. (Chellegati 2009) the intruder uses a program that appears to be the server to the client and appears to be the client to the server. The attack may be used simply to gain access to the message, or enable the attacker to modify the message before retransmitting it. (Koutney 2010)
The main question therefore is whether the majority of the users of mobile banking applications are aware of the existence of such threats and how the awareness or lack of it can affect the perpetration of such attacks.

2.0 Method

2.1 Respondents Profile

Age				
18 - 24 Years	25 - 34 Years	35 - 44 Years	45 - 55 Years"	55+ Years
20	30	20	20	10

Work status					
Full-time	Part-time	Casual / piece jobs	Student	Unemployed	Housewife /taking care of home Full-time
65	24	2	6	1	2

Professional	Business / retail traders	Government officials	White collar workers (clerks/ assistants/ teachers etc)	Skilled workers	Unskilled workers
43	51	1	1	2	1
100%	100%	100%	100%	100%	100%

No Formal Schooling	Some Primary Education	Primary Education Completed	Some Secondary / High School	Secondary / High School Completed	Post Secondary / College Education	Some University	University Complete I.E. Degree	Post Graduate Degree
1	3	9	7	21	30	14	12	2

Marital status		
Married/living together	Single/Unmarried	Separated/divorced/widowed
62	34	4

Gender	
Male	Female
50	50

2.2 Reasons for unsuccessful interviews

Refusal outright	5
Not in after 3 calls/ Nobody at home	7
Language barrier	2
Dogs	0
Security/ not allowed in/ gate locked	0
Inaccessible roads/ roads under construction/ bad road surfaces	0
Empty house/ apartment	2
Ill/ in hospital/ mentally disabled	0
Unsafe	0
No one in Household over 18	4
Other (specify)	0
Total	**20**

2.3 Sampling

The population (universe) under investigation was made up of all Nairobi County persons aged 18 years and older.

We used a multi-stage sampling design. The county was the largest administrative unit followed by locations then sub locations.

Step 1: Compile all the locations in Nairobi County.

Step 2: Compile all the sub locations in Nairobi County.

Step 3: Distribute the number of interview proportionately to the population of each sub location.

Step 3: All the sub locations in each location in Nairobi was arranged to show the Location, sub location population. The sub locations were then arranged in alphabetical order in each Location. Depending on the number of interviews required per location, the sub locations were randomly selected using a skipping method. This random method was used to determine the exact sub location that served as a PSU (Primary Sampling Unit). In each PSU a total of 10 interviews were conducted.

Quotas were set by age and gender

2.4 The Questionnaire

The questionnaire consisted of 11 questions 2 of which were open ended. The questionnaire was administered among respondents who had an active mobile phone that they personally owned. The questions centered on previous experience with mobile phone banking services

3.0 SURVEY RESULTS

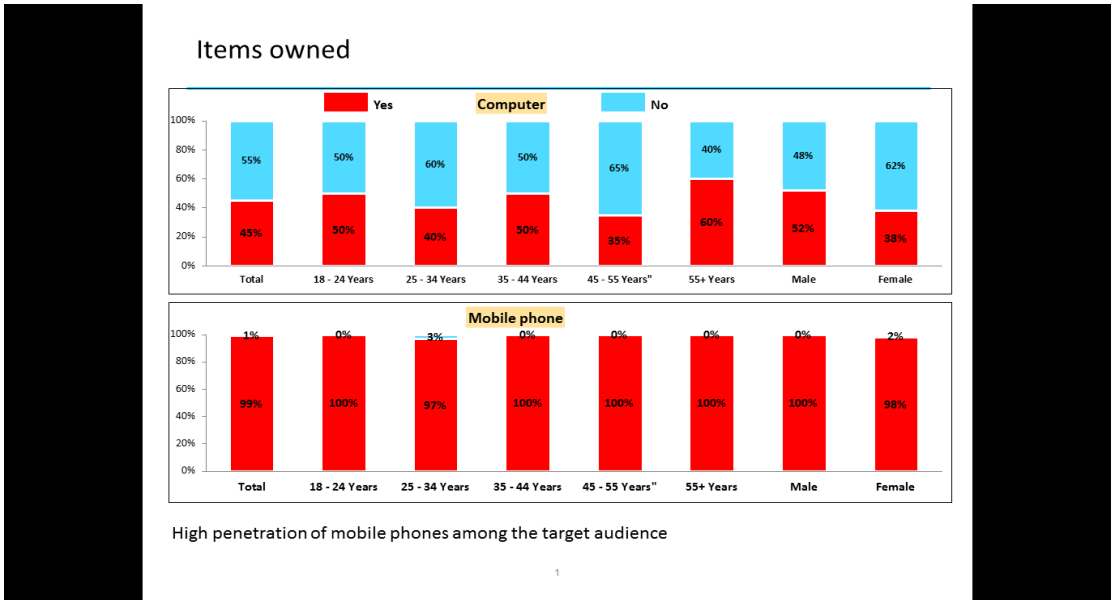


Fig. 1.1 Items owned

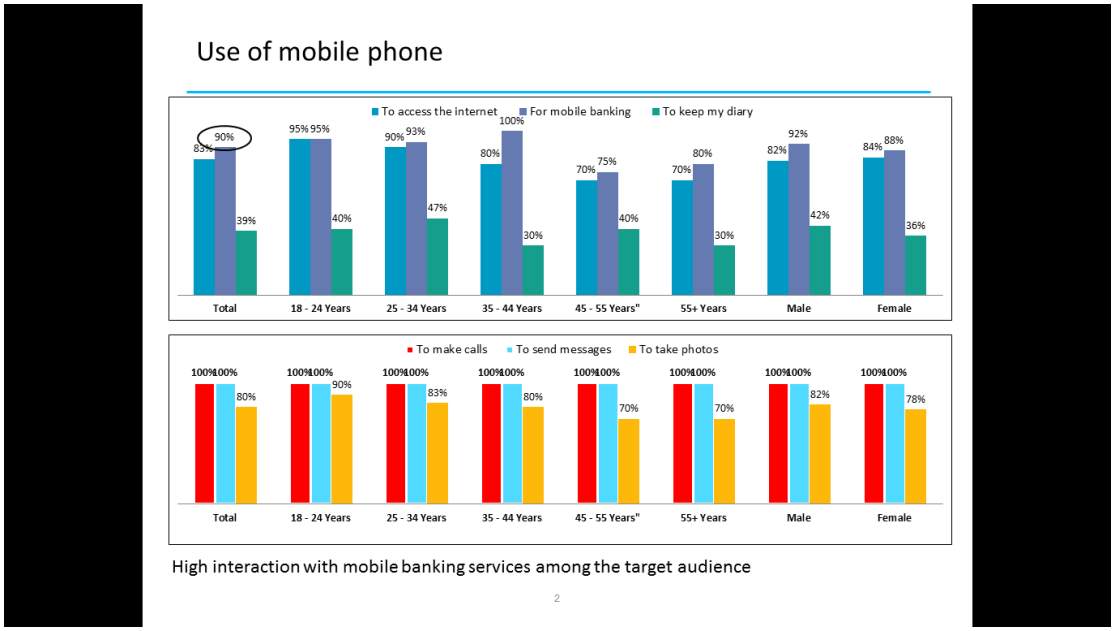


Fig 1.2 use of mobile phones

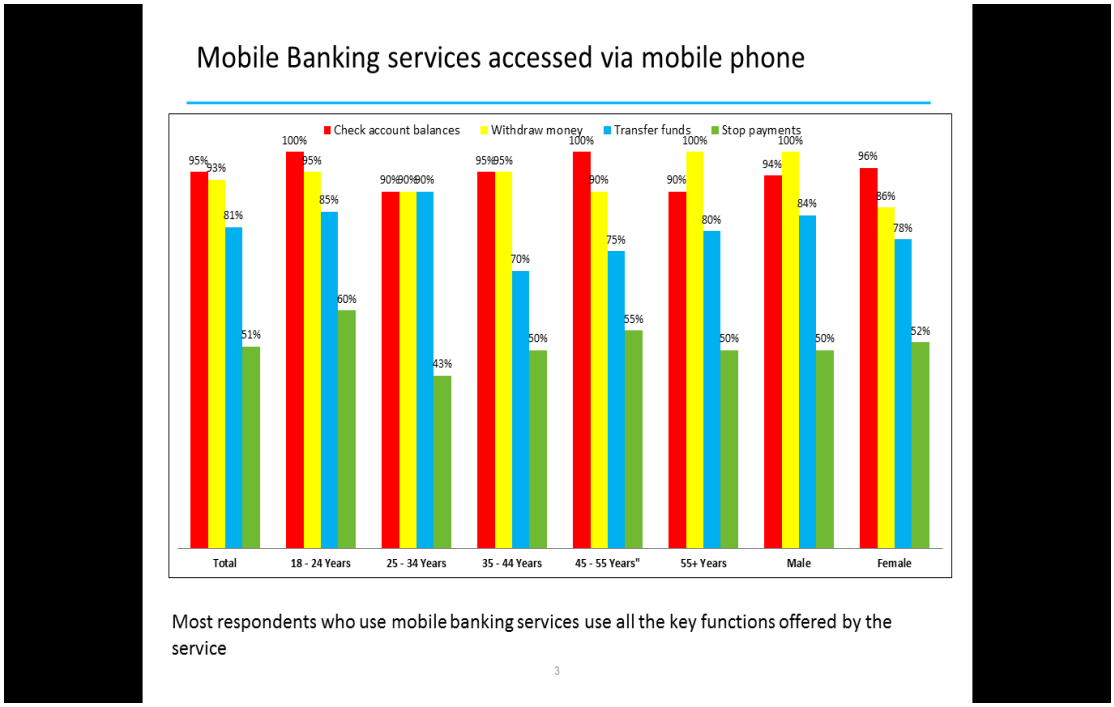


Fig 1.3 mobile banking services accessed via mobile phone

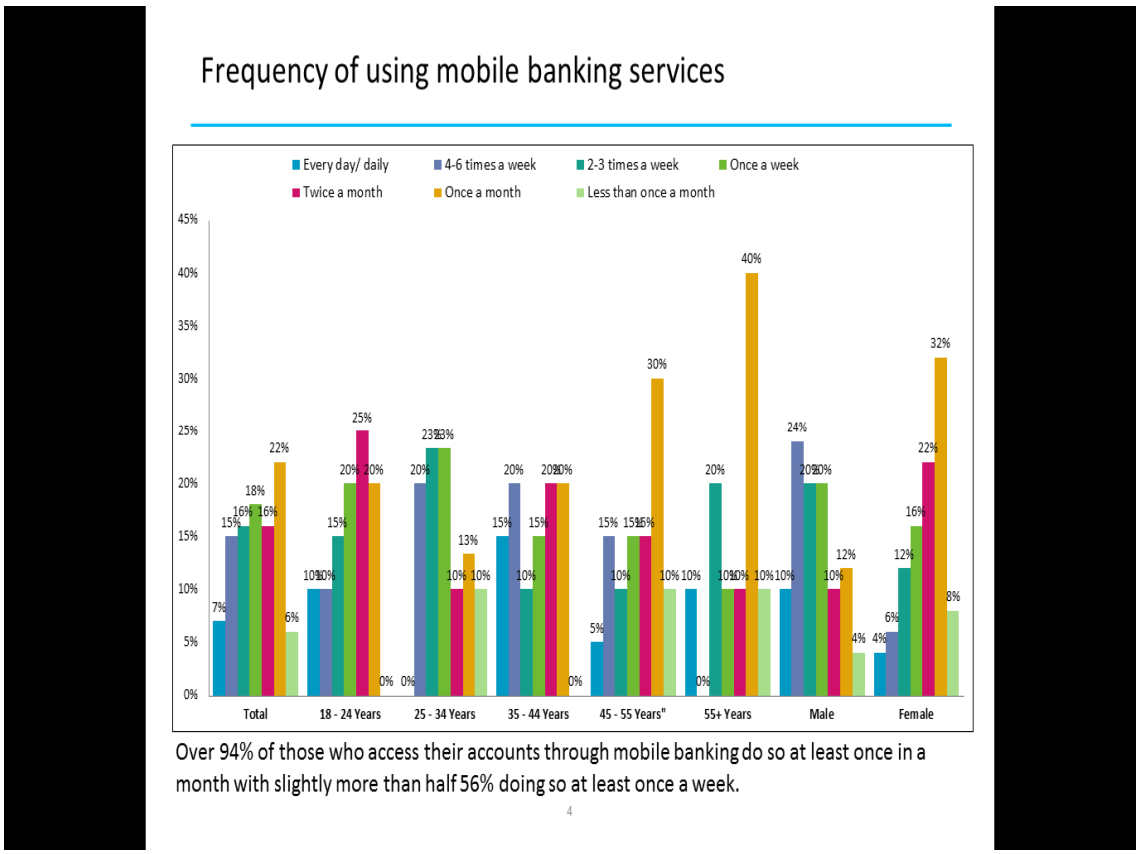
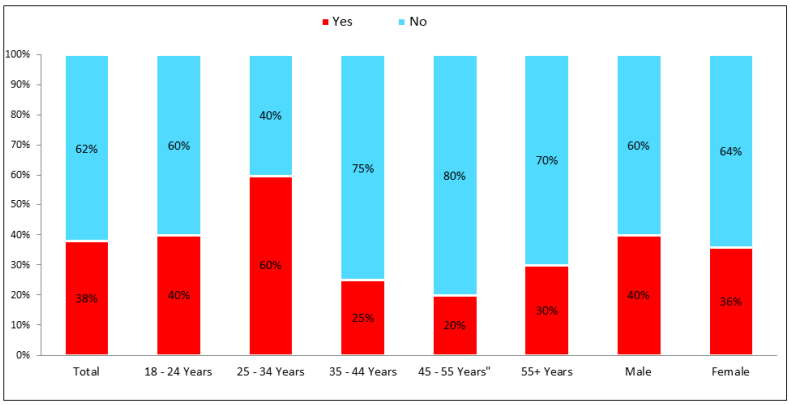


Fig 1.4 Frequency of using banking service



1.*5 whether experienced any problems with mobile banking*

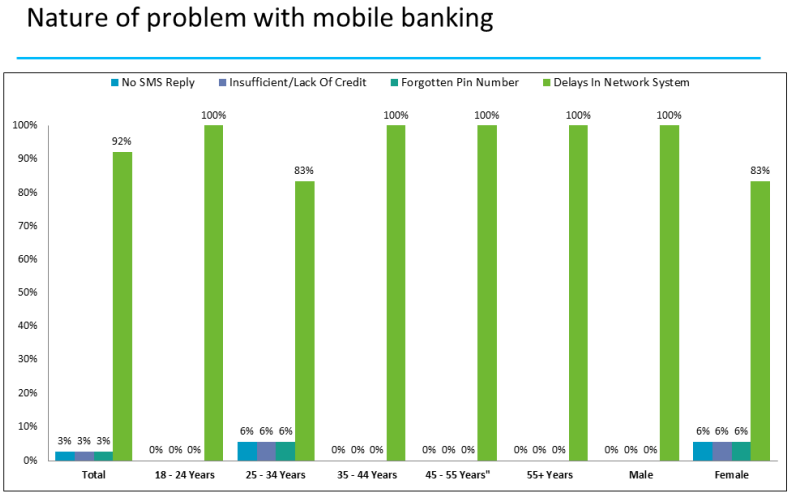


Fig 1.6 Nature of problem with mobile banking

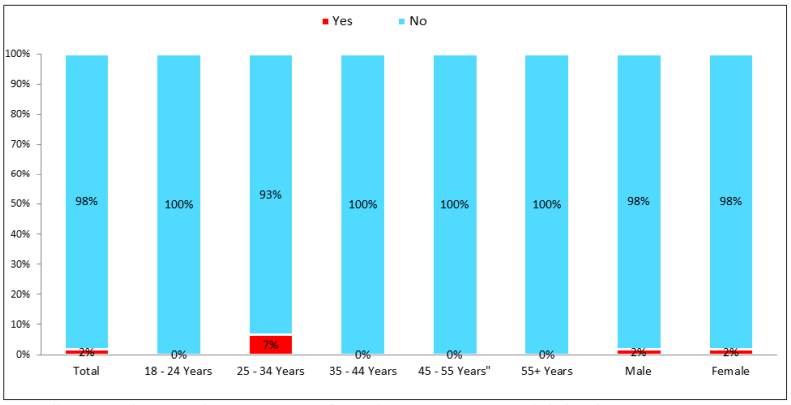


Fig1.7 whether ever lost money via mobile banking

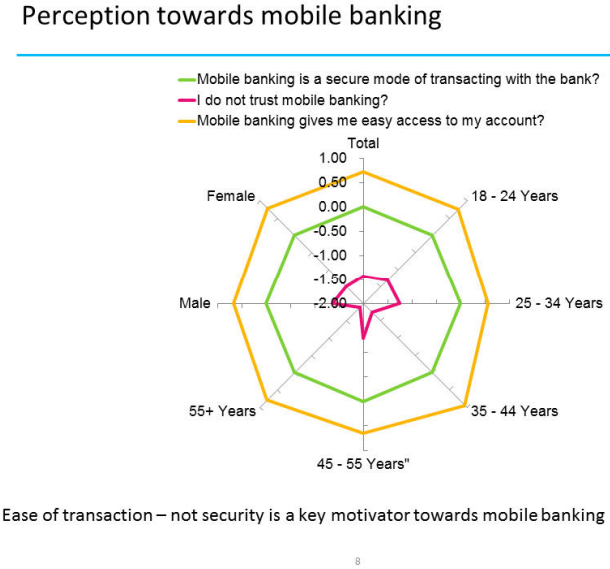


Fig1.8 perception towards Mobile banking

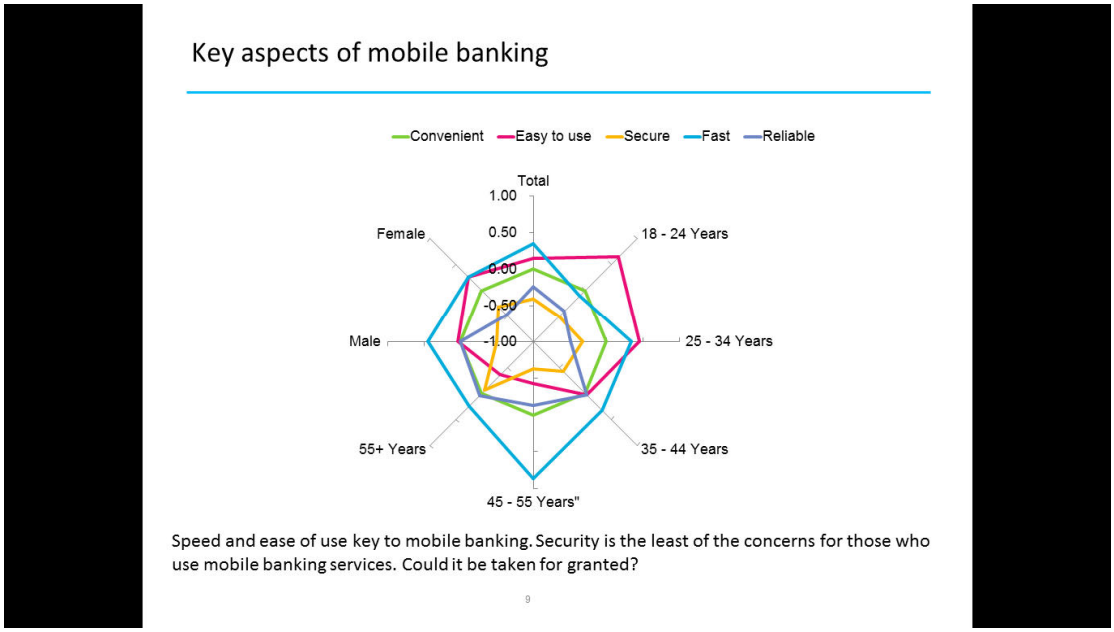


Fig 1.9 Key aspects of mobile banking

TABULATED SUMMARY OF GRAPHS

NUMBER	TITLE	OVERVIEW
Fig 1.1	***Items owned***	While 99% of the respondents owned mobile phones, only 45% of the respondents owned computers, with the conclusion being that there was a high penetration of mobile phones among the target audience
Fig 1.2	***Use of mobile phones***	100% of the target respondents used mobile phones for texting and making phone calls which is only natural. However surprisingly enough a higher percentage of the respondents used their mobile phones to access banking services as opposed to accessing the internet for other use.
Fig 1.3	***Mobile banking services accessed via mobile phones***	Most respondents indicated that they access their banking services via mobile phones to check their bank balances, this was closely followed by the action of withdrawing money with funds transfer being the third most accessed banking service via mobile phones. The action of stopping payments came in a distant forth.
Fig 1.4	***Frequency of using mobile banking services***	Over 94% of those who access their accounts through mobile banking do so at least once in a month with slightly more than half 56% doing so at least once a week.
Fig 1.5	***Whether experienced any problems with mobile banking***	60% of those that fall under the age bracket of 25-34yeras of age were of the opinion that they have experienced problems with the mobile banking services they access. Overall less than 38% of the respondents were of the opinion that they actually do experience problems with the mobile banking services they access
Fig 1.6	***Nature of problem with mobile banking***	Those who felt that they were experiencing problems with the mobile banking services they were accessing felt that their major concern was delays in network systems a problem that is more associated with the service providers as opposed to the banking services themselves.
Fig 1.7	***Whether ever lost money via mobile banking***	Only 2% of the respondents have ever lost money from their accounts or if they have then they just did not notice it
Fig 1.8	***Perception towards mobile banking***	Majority of the respondents are more interested with the ease at which they can perform transactions using their mobile phones. They are less concerned with the security issues that may arise from such transactions; in fact most of them feel that mobile banking is a secure mode of transaction.
Fig 1.9	***Key aspects of mobile banking***	From the respondent's point of view, as end users of mobile banking they are more concerned with convenient, fast, reliable and easy to use services. Security is the least of the concerns for those who use mobile banking services. The main question here then would be, should this aspect of security be taken for granted?

Table 1.1 summary of graphical representation of survey

4.0 Discussion

As indicated previously a Man In The Middle attack is one in which the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other. (Chellegati 2009) the intruder uses a program that appears to be the server to the client and appears to be the client to the server. The attack may be used simply to gain access to the message, or enable the attacker to modify the message before retransmitting it. The aim of the survey was to investigate as to whether the majority of the users of mobile banking applications in Kenya are aware of the existence of such threats and how the awareness or lack of it can affect the perpetration of such attacks.

The survey clearly indicates that there is a high penetration of mobile phones and in relation mobile phone use among the target market. Surprisingly enough a higher percentage felt that they used their phones more to access mobile banking services than other internet services. Most however used their handheld devices to access bank balances. The act of withdrawing money was the second most performed action followed by the transfer of funds while the action if stopping payments came a distant third. All the aforementioned actions were performed at least once a week by majority of the respondents.

As to whether the respondents had ever experienced problems with mobile banking, only approximately 40% acknowledged that they had. Their biggest concern however, was network delays and failure as opposed to security concerns. Despite the fact that 2% of the respondents reported having lost money through mobile banking ***(this understates the fact that insecurity does exists though at a lower magnitude)*** most end users were more concerned with convenient, fast, reliable and easy to use services. In fact most of them were of the view that mobile banking is a secure mode of transaction.

Despite the perception held by most viewers, mobile banking security issues are still a major concern within the mobile computing circles. More worrying is the fact that most hackers take advantage of the users lack of awareness on security matters to perpetrate their attacks. This is most commonly achieved by the use of a Trojan horse with the Zeus attack being the most common.

A trojan horse basically is a malware that appears on a clients mobile handset while giving the client the illusion that they are communicating with a genuine application from the banks while in real sense all its doing is obtaining financial information from the client.

Despite the fact that only 2% of the mobile banking population in Kenya has at one time or another lost money through mobile banking, the fact that majority of the population are unaware of such security issues can only mean that mobile banking security attacks within the banking industry in Kenya is a time bomb waiting to happen.

REFERENCES

"CCK releases 2nd quarter ICT sector statistics for 2011/2012". Communications Commission of Kenya. 17 Apr 2012.

Ars Technica.http://arstechnica.com/tech-policy/news/2009/08/one-minute-wifi-crack-puts-further-pressure-on-wpa.ars?utm_source=rss&utm_medium=rss&utm_campaign=rss. Retrieved 2010-06-05.

B. Yan, G. Chen, J. Wang, and H. Yin, ***"Robust Detection of Unauthorized Wireless Access Points,"*** Mobile Networks and Applications Journal, vol. 14(4), pp. 508-522, Aug. 2009.

Bangdao, C., & Roscoe, B ***Mobile Electronic Identity: Securing***. (2011)

D. Jiang, L. Xinghui, and H. Hua, ***"A Study of man-in-the-Middle Attack Based on SSL Certificate Interaction,"*** 2011 First International Conference on Instrumentation, Measurement, Computer, Communication and Control, pp. 445-448, Oct. 2011.

F. Callegati, W. Cerroni, and M. Ramilli,, "***man-in-the-Middle Attack to the HTTPS Protocol,"*** Security & Privacy, IEEE, pp. 78-81, 2009.

http://www.passmarksecurity.com/BofA.jsp

http://www.wifialliance.org/knowledge_center_overview.php?docid=4486.Retrieved2008-02-06.

Joshua Bardwell; Devin Akin. ***CWNA Official Study Guide*** (Third ed.). McGraw-Hill. p. 435. ISBN 0072255382. 2005

Kevin Beaver, Peter T. Davis, Devin K. Akin. ***"Hacking Wireless Networks For Dummies"*****.** Prentice hall 2009

Lachu Aravamudhan, Stefano Faccin, Risto Mononen, Basavaraj Patil, Yousuf Saifullah, Sarvesh Sharma, Srinivas Sreemanthula. ***"Getting to Know Wireless Networks and Technology"***, *InformIT 2009*

Lance J. Hoffman, ***Rogue Programs: Viruses, Worms, and Trojan Horses***, *1990* http://www.wikidsystems.com

Innovative Demand Models for Telecommunications Services FINAL TECHNICAL REPORT Contract Number R8069 Dr. Kevin McKemey (Gamos) Dr. Nigel Scott (Gamos) Professor David Souter (University of Strathclyde, former CEO of CTO) Dr. Thomas Afullo (ex University of Botswana) Mr. Richard Kibombo (Makerere Institute of Social Research) Dr. O. Sakyi-Dawson (University of Ghana) Funded by: Department for International Development (DFID)

Internet Incident Response Support Center, ***"Internet Attack Trends and Analysis,"*** Korea Information Security Agency, pp. 22-37, Jun. 2007

K. Cheng, M. Gao, and R. Guo, ***"Analysis and Research on HTTPS Hijacking Attacks,"*** 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, IEEE, pp. 223-226, Apr. 2010.

K. DongPhil, K. chulbum, and K. Sangwook, ***"Rogue AP Protection System Based On Radius Authentication Server,"*** Korean Institute of Information Scientists and Engineers, vol. 31(1), April, 2004.

K. kuofong, L .ien, and L. Yuehchia***, "Detecting rogue access points using client-side bottleneck bandwidth analysis,"*** Computers & Security, vol. 24(3-4), ELSEVIER, pp. 144-152, May. 2009.

K. Kuofong, Y.Taoheng, Y.waishuoen, and C.Huihsuan, ***"A locationaware rogue AP detection system based on wireless packet sniffing of sensor APs,"*** SAC '11 Proceedings of the 2011 ACM Symposium on Applied Computing, ACM, 2011.

L. Watkins, R. Beyah, C. Corbett, ***"A Passive Approach to Rogue Access Point Detection,"*** Global Telecommunications Conference, 2007. IEEE. pp. 355-360, Nov.2007

M. Kwiatkowska, G. Norman, and J. Sproston. ***Probabilistic model checking for deadline properties in the IEEE 1394 Fire Wire root contention protocol.*** Special issue of formal Aspects of computing, 2002

M. Moixe***, "New Tricks For Defeating SSL in Practice"***, BlackHat Conference, USA. Feb. 2009.

Man Young Rhee, Internet Security: ***Cryptographic principals, algorithms and protocols***, John Wiley and sons, 2003.

N. Asokan, V. Niemi, and K. Nyberg. ***Man in the middle in tunneled authentication protocols.*** In security protocols workshop, 2005.

Nate Anderson ***"One-minute WiFi crack puts further pressure on WPA"***.2009 ***Payment on Mobile Phones***. Proceedings of WISTP 2011.

R. Beyah, ***"Rogue access point detection_challenges, solutions, and future directions,"*** IEEE Security and Privacy Article, vol. 9(5), IEEE, pp. 56-61, 2011.

R. Meyer, ***"Secure Authentication on the Internet, "*** SANS InfoSec Reading Room - Securing Code, Feb. 2008.

Ralf Burger, ***Computer Viruses. A High Tech Disease***, 2010 Ramez Elmasri and Shamkant B. Navathe. ***Fundamentals of Database Systems***, 4th Edition. Addison-Wesley, 2004.

Robert McMillan. ***"Once thought safe, WPA Wi-Fi encryption is cracked"***. *IDG*. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9119258. Retrieved 2008-11-06.

Ross M. Greenberg, "***Know Thy Viral Enemy***", *Byte*, June 1999 Stuart McClure, Joel Scambray, George Kurtz, ***Hacking Exposed, Network Security secrets and solutions***, Mcgraw hill 2009.

Susan Kellam, "***Adapso Urges Congress to Act on Viruses***", *Washington Technology*, July 13, 1999

Tiwari, Rajnish; Buse, Stephan and Herstatt, Cornelius (2006): ***Customer on the Move: Strategic Implications of Mobile Banking for Banks and Financial Enterprises,*** in: CEC/EEE 2006, Proceedings of The 8th IEEE

International Conference on E-Commerce Technology and The 3rd IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services (CEC/EEE'06), San Francisco, pp. 522–529

Tiwari, Rajnish; Buse, Stephan and Herstatt, Cornelius (2006): ***Mobile Banking as Business Strategy: Impact of Mobile Technologies on Customer Behaviour and its Implications for Banks,*** in: Technology management for the Global Future - Proceedings of PICMET '06.

S. Yimin, Y. Chao, and G. Guofei, ***"Who Is Peeping at Your Passwords at Starbucks? - To Catch an Evil Twin Access Point,"*** International Conference on Dependable Systems & Networks (DSN), IEEE, June. 2010.

Saylor, Michael (2012). *The Mobile Wave: How Mobile Intelligence Will Change Everything*. Perseus Books/Vanguard Press. p. 304. ISBN 978-1593157203.

T. Chomsiri***,"HTTPS Hacking Protection, "*** 21st International Conference on Advanced Information Networking and Applications Workshops, IEEE, May. 2007.

T. Koutny, ***"Detecting Unauthorized Modification of HTTP Communication with Steganography,"*** 2010 Fifth International Conference on Internet and Web Applications and Services, IEEE, pp. 26-31, May. 2010.

U Black, ***Foundation for Broadband Networks,*** NJ: Prentice- hall, 2011

William A Shay, ***Understanding data communication and Networks***, Second Edition, Brooks/Coe publishing company. 2012

William Stallings, **Computer Networking with internet protocols and technology,** Peason NJ: Prentice- hall, 2006

William Stallings, ***Cryptography and Network Security,*** Prentice Hall, 2003 William stallings, **Cryptography and network security, *principles and practices,*** NJ: Prentice- hall 2011

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Recent conferences: http://www.iiste.org/conference/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar