African Scientist Vol. 11, No. 1 March 31, 2010
Printed in Nigeria

1595-6881/2010 $12.00 + 0.00

http://www.klobex.org/afs

AFS 2009125/11104

Evaluation of Security and Reliability of Automatic Teller Machines Usage in Kano Metropolis, Kano State, Nigeria

L. Abdulwahab

Department of Mathematics and Statistics, University of Maiduguri, P.M.B 1069, Boron State, Nigeria
E-mail:abd_wahhb@yahoo.com; Tel: 08034980173

(Received October 22, 2010)

ABSTRACT: ATM services provided by banks and non financial institution have appeared as the most E - Banking instruments that had become so popular in Nigeria. The belief that ATM is dependably provided by a bank, the transactions and the data being transmitted must be secured. This belief might hold in the past, but at the moment ATMs are now able to use operating systems, such as Microsoft windows and Linux. These operating systems do expose ATM to vulnerability akin to the same kind of problems displayed by conventional computers. Field survey was carried out among the Bank's customers' in Kano metropolis with a view to evaluate security and reliability of automatic teller machine usage by customers .The data collected was analyzed using 5-point Likert - type response scales. From the results obtained, the availability of host system refers to as network services was (47.8%) and accessibility of ATM cash point was (62.8%). The study also revealed that, one of the major hindrances to the use of ATM as a banking instrument in Nigeria is the issue of security of depositors' funds. The number of internet-based crimes and misdemeanors' carried out every day results in stolen data and cost many huge financial lost. Enhancing network and security of ATM usages has become imperative for the customers' to have trust in this very useful tool of information technology.

Keywords: Automatic Teller Machine, Security, Reliability, Financial Institution, Nigeria

Introduction

An automatic teller machine is a computerized telecommunication device that provides the customer of a financial institution with access to financial transaction without the need for a human clerk or bank teller (Wikipedia, 2009). There is a growing rate of adopting the technology of Automatic Teller Machine (ATM) globally (Antonella *et al (2004), Wole and Louisa (2009)).* Majority of ATMs allow customers' to execute some basic banking transactions such as cash withdrawal, account inquiry and recharge of a prepaid GSM phone. There are ATM services providing more function such as: providing updated account information, converting currency, stock market and securities information, buying cinema tickets and postage stamp (Ammenheuser, 1999).

The numbers of ATMs in used exceed 1.5 million (www.atmmarketplace.com). In recent times, owing to considerable computing needs and the declining price of computer like architectures, there has been realignment of ATM from early hardware architectures using microcontrollers and/or application-specific integrated circuits to adopting a hardware architecture that is very similar to a personal computer (Robert, 2009). As a result of this development many ATMs are now able to use operating systems such as

Microsoft windows and Linux. Even though it is enormously economical to use commercial off-the-shelf hardware, it does expose ATMs to vulnerability akin to the same kind of problems displayed by conventional computers. These shifting from using proprietary hardware and software and being connected via a proprietary network to using over the counter hardware and software and working via IP connectivity, the result is that security of consumers' personal details and their exposure to intruders by both human and associated computer virus are increasingly becoming an issue.

ATM running Microsoft Windows XP are vulnerable to an automated attack that can engrave bank account numbers and personal identifying number PIN codes As with any machine holding precious objects, ATMs and the systems they rely on to operate are susceptible targets of attack. Generally ATMs are connected to inter banks networks enabling people to withdraw and make other basic services from machines not necessarily belonging to where they have their account. In Nigeria inter banks is connected by Interswitch. (www.interswitchng.com). ATMs typically connects to their ATM controller via a high speed internet VPN connections become more universal, using triple-DES encrypted PIN numbers for the IP- ATM connected to a payment processor across a TCP/IP connection. Three primary threats were identified as factors facing IP-ATMs Mark (2009). These are Internet Protocol worms and other malicious code penetrating the defenses of the ATM itself or the IP network it is connected to; disruption of the IP network and denial of service; and passive collections of transaction data for malicious purposes, resulting in hackers being able to collect a consumer's card number, account balance and transaction history. According to Robert (2009), several variants of the malicious software were discovered on hacked ATMs in Eastern Europe.

Fraud against ATMs takes several forms. For a low technological form of fraud, the easiest is to simply steal a customer's card. A later variant is to trap the card inside the ATM's card reader with a device often referred to as a Lebanese loop (Wikipedia, 2009). When the customer gets frustrated by not getting the cards back and walks away the criminal is able to remove the card and withdraw cash from the customer's account. This paper therefore aims at evaluating the security and reliability of Automatic Teller Machines usage in Kano metropolis.

Material and Methods

Study Area

The study was conducted in Kano Metropolis, one of the most populous states and the economic nerve centre of Northern Nigeria. According to the 2006 National population and Housing census, the state had an estimated population of 9,383,682, (NPC, 2006). Field survey was conducted between January 2009 and September 2009.

Sampling procedure

The samples comprised of 113 respondents that were selected during the investigation. The gender distribution was male 82.3% and Female 17.7%. Convenience sampling distribution techniques Joy *et al* (2003) was used in selecting the participants. This technique allows more personal contact and so more in-depth information can be obtained.

Research instrument and data collection

The primary data were sourced through the use of well structured questionnaires. Section A was used to collect information on the demographic data of the respondents, like gender, age educational attainments, and occupation so that their effect on technology used could be explored. While section B was used to investigate basic aspect of respondents technology utilization as conducted by Joy *et al* (2003). Respondents were asked to rate their opinion about each item using a five point Likert-type rating scale, as conducted by (Abdulwahab, 2009). The rating used were strongly agree (SA) = 4, agree = 3 (A), strongly disagree (SD) = 2, disagree (D) = 1 and neutral (N) = 0. The administered questionnaire can be found in the appendix 1.

Data Analysis

Descriptive statistical techniques such as frequency distribution and percentage were used to achieve the objective of the study Joy *et al* (2003). The data collected was analyzed using Microsoft excel (statistical package) application software (Appendix 1).

Results

The preponderance of the respondent are the 21- 40 age group, which corresponded to 57(50.4%) of the person investigated. Only 31(27.4%) of the respondents had secondary education, as shown in (Table 1). Furthermore, a significant number of the respondents are civil servants 76(67.3%). Table 2, presents reliability of services as offered by the service providers 54(47.8%) of the respondents indicate that ATM Network is reliable and 71(62.8%) can access their accounts at any time including public holidays. Customers can gain access to their accounts via ATM only by using card having an encrypted numbers referred to as PIN usually four digits, 80(70.8%) of the respondents are reluctant in changing their PIN (Table 3).

The Telephone banking has being around before the advent of ATM but the adoption of text message through GSM on any transaction made has popularized the uses of a telephone as a banking instrument 69(61.0%) of customers' received text message on any transaction made on their accounts as indicated in (Table 3) . On human or machine error which may be as a result of malfunction of hardware or software (as a result of virus or malware) or even made as a result of improper stocking of bank's note on the cassettes of ATM, a significant number of the respondents 71(26.5%) not at all experienced over payments or underpayments. At times due to network failure during transaction customers experiences debiting of accounts without issuing physical cash 45(39.9%) of the respondents depicts this (Table 4).

Due to problems of human or machine error, some customers ingeniously adopted to only access the ATM belonging to the bank, where their account reside 33(29.2%) of the respondents adopted this measure (Table 5). A major challenges to both the customers' and ATM service providers is issue of internet hacker's 36(31.9%) of the respondents have experienced of the exploits scammers that randomly send out a spam messages urging customers to update the information on their ATM card (Table 6). .

Discussion

The finding has shown that majority of the respondents are adult further corroborating the works of Rogers *et al (1996)* on the usage of ATM. There was a high level of literacy among the respondents as shown in (Table 1), the implication of this, is that the respondent has little difficulty using the ATM interface. The benchmark typically expected by ATM is producing 98.3% customer accessibility and 99.9% availability for host system (Wikipedia, 2009). From the results obtained the availability of host system refers to as network services was (47.8%) and accessibility of ATM was (62.8%). This is far below the international benchmark typically expected of ATM.

The concepts and various methods of copying the contents of an ATM card's magnetic stripe on to a duplicate card to access other people's financial information was well known in the hacking communities (Wikipedia, 2009). The need to guard the secrecy of PIN is a vital aspect of security and integrity on customers accounts. As a measure of security, an emergency text message is adopted when ever there is a transaction in customer's account, where the banks send a text message to account holder in response to any transaction. This facility enables customers to monitor their accounts and in addition lodge complaint whenever the integrity of their accounts is being threatened (Table 3). Not all errors are to the detriment of customers, there have been cases of machines giving out money without debiting the account, or giving out high value note as a result of incorrect denomination of bank note being loaded in the money cassettes or error that can occur may be mechanical or down to operator error (Wikipedia, 2009). The prevalence of human and machine error is low as shown in (Table 4). Because of the problems of network failure leading to cash trapping, some customers adopted the use of ATM belonging only to the bank where their account

reside to minimize inter banks delays of responses to complaint (Table 5). Hackers' desperate attempts to access customer's bank account had led to them to ingeniously duplicate the Interswitch website. That exploits has enabled the scammers to randomly send out a scam message via e-mail or GSM urging customers' to register their ATM cards in a cloned site claiming also that InterSwitch was upgrading its networks. The scammers have quietly collected the cards details including pins to access customer's accounts. Many Nigerians were swindling through this scam (Table 6).

Table 1: Demographic Data.

Variable	Category	Frequency	Percentage
Gender	Male	93	82.3
	Female	20	17.7
Age	Under 20	13	11.5
	21 – 40	57	50.4
	41 – 50	41	36.3
	51 – 60	2	1.8
	Above 60	0	0
Qualification	Primary/Secondary	31	27.4
	Tertiary	76	67.3
	Others	6	5.3
Occupation	Student	30	26.5
	Civil Servant	76	67.3
	Business	5	4.4
	Others	2	1.8

n = 113
Sources: Field Survey (2009)

Table 2: Evaluation of ATM Networks Reliability.

Question	SA	A	N	D	SD	Mean
Is Automatic Teller Machine (ATM) Network reliable?	31.0	16.8	8.0	25.7	18.6	2.58
Can you access ATM service throughout the day?	40.7	22.1	9.7	15.9	11.5	2.97

Sources: Field Survey (2009)

Table 3: Evaluation of Security/Integrity of ATM by the respondents

Question	SA	A	N	D	SD	Mean
Do you occasionally change your PIN?	15.9	8.8	4.4	41.6	29.2	1.99
Do you get alert through GSM phone or any other means?	38.9	22.1	4.4	20.4	14.2	2.83

Sources: Field Survey (2009)

Table 4: Evaluation of Human and Machine Errors.

Question	SA	A	N	D	SD	Mean
Did ATM ever issue higher or lower notes due to incorrect denomination of bank notes loaded into it?	16.8	9.7	10.6	37.2	25.7	2.07
Did ATM ever debit your account without issuing physical cash?	25.7	14.2	8.0	31.0	21.2	2.38

Sources: Field Survey (2009)

Table 5: Safety measure adopted by some respondents.

Question	SA	A	N	D	SD	Mean
Do you stick to accessing ATM restricted to your bank?	18.6	10.6	10.6	35.4	24.8	2.14

Sources: Field Survey (2009)

Table 6: Evaluating Hackers' desperate attempts to access customer's account .

Question	SA	A	N	D	SD	Mean
Did you ever receive a message through your e-mail urging you to update your PIN or any other information on your ATM card?	20.4	11.5	8.8	34.5	24.8	2.19

Sources: Field Survey (2009)

Conclusion and Recommendations

The study revealed that the availability of host system refers to as network services was (47.8%) and accessibility of ATM was (62.8%). A customer has come to expect high reliability in their ATMs because of the conveniences and accessibility associated with its usage. From the study the major impediment to the utilization of ATM as a banking instrument in Nigeria is the problem of security of depositors' funds. Most of the fraud people encounter these days come to them via internet. The number of opportunistic and targeted internet-based crimes and misdemeanors' carried out every day result in stolen data and damaged systems and cost many institutions huge financial lost. However with enlightenment the vast majority of customers' day to day experiences are positive and being aware and prepared, this can help prevent them from falling victim to cyber crime.

The migration of the financial industry to commodity hardware, operating systems and protocols gives the industry advantages of cost performance, flexibility, standardization and enhanced functionality, however, the threats through these migration leads to increase in exposure as far as security risk is concerned the risk of virus that may lead to disruption of IP network thereby leading to denial of service. To reduce ATM fraud, biometrics technology should be integrated with new valve card this would guarantee that information stored would not be accessible to unauthorized person. Recruiting high caliber of information security personnel is essential for any organization wishing to be protected from internal and external threats.

References

1. Abdulwahab, L: An Assessment of Billing Electricity Consumers Via Analogue Meter In Kano, Nigeria, by Kano Electricity Distribution Plc, Bayero journal of Pure and Applied Sciences 2009 ; 2(1): 27-33.
2. Antonella, D., Lynn, C and Graham, I, J: ATM's Adoption in Developing Countries. (2004)
3. Available at http://www.antonella_de_angeli. Talk talk-net/../
4. Ammenheuser, M: Citibank bulks up ATM power, Bank System and Technology 1999; 36(2):26. Available at http://www.gerontechnology.info/journal/pdf.php
5. Joy, G, Audrey, S and Roos, E: Age-Old Questionnaire. (2003). Available at http://www.computing.dundee.ac.uk/
6. Mark, W: ATM Security leaves customers vulnerable to hackers. Network box security service, Network box corp. Ltd Hong Kong. (2009). Available at http://www.daniweb.com
7. Robert, M: Malware steals ATM accounts and PIN codes, Insecurity firm Trust wave Spider labs. (2009). Available at http://www.spiderlabs.org
8. Rogers, W.A., Cabrera, F.B, Walker, N. and Gilbert, K.G: Survey of ATM Usage across adult life Span. Human Factors 1996; 38(1): 156-166. Available at http://www.questia.com
9. Wikipedia: Automatic Teller Machine- The free encyclopedia. [Online]. Available at *http://wikipedia.org/wiki/ATM*
10. Wole, M.O and Louisa, J. I: The Adoption of ATM in Nigeria: An application of theory of Diffusion of innovation Issues in Information Science and Information Technology 2009; 6: 374-352. Available at http://www.docs.google.com

Appendix: Questionnaire administered to respondents.

Dear Respondent

This questionnaire is designed for research work on the usage of Banks Automatic Teller Machine (ATM). Please tick appropriate column below. All information will be treated confidentially and the information in this questionnaire is for the purpose of research work only.
Please tick [ ] or fill where appropriate.

Section A

1. Gender (A). MALE [ ] (B). FEMALE [ ]
2. AGE (A). 15-20[ ] (B). 21- 40 [ ] (C). 41 – 50 [ ] (D). 51- 60[ ] (E). ABOVE 60 [ ]
3. QUALIFICATION (A). PRIMARY [ ] (B).SECONDARY [ ] (C).TERTIARY [ ] (D). OTHERS[ ]
4. OCCUPATION (A). STUDENT [ ] (B).CIVIL SERVANT [ ] (C).BUSINESS [ ] (D). OTHERS[ ]

Section B

	Question	Yes	No	Neutral
1.	Is Automatic Teller Machine (ATM) Network reliable?			
2.	Do you occasionally change your PIN?			
3.	Do you stick to accessing ATM restricted to your bank?			
4.	Did ATM ever debit your account without issuing physical cash?			
5.	Did ATM ever issue higher or lower notes due to incorrect denomination of bank notes loaded into it?			
6.	Do you get alert through GSM phone on any transaction made?			
7.	Can you access ATM service throughout the day?			
8.	Did you ever receive a message through your e-mail urging you to update your PIN or any other information on your ATM card?			