ISSN 2047-3338

Security Issues Analysis on Online Banking Implementations in Nigeria

Emeka Nwogu[1] and McChester Odoh[2]

[1]Directorate of Information and Communication Technology, Michael Okpara University of Agriculture, Umudike, Umuahia, Abia state, Nigeria

[2]Department of Computer Science, Michael Okpara University of Agriculture, Umudike Umuahia, Abia state, Nigeria

[1]nwogu.emeka@gmail.com, [2]oguzuruodo@gmail.com

***Abstract*– A study of the Nigerian internet banking system was conducted. The study analyzed the levels of internet banking with an in-depth analysis of their security needs and associated issues. A particular reference was made on the attacks and vulnerabilities in the current systems. Next, is an analysis of the current defense mechanisms and how successful they have been in counteracting the occurrence and effects of Internet banking attacks in Nigeria. We established from the study and research, that the current defense mechanisms have not been very effective, as they still have vulnerabilities which have been exploited by attackers severally.**

***Index Terms*– E-money, Automated Teller Machines, Internet Banking, E-banking and Online Banking**

I. INTRODUCTION

INTERNET banking has become an inevitable means of financial transactions in this ever changing world. It involves conducting financial transactions over a secure website. Nigeria as a Country has not been left out of this trend. Currently, most Banks in Nigeria have embraced this technology and have gradually deployed it in their mainstream operation. The central Bank of Nigeria on the other hand as the apex financial institution in the Country has also championed a cashless economy, which has led to a renewed interest in this wonderful but security -threatened technology.

The advancement of Internet banking and its associated technologies has been related to the ease of access the technology presents to its numerous users. Simpson J (2002) writes that the motivation of investment in electronic banking is largely the prospects of minimizing operating costs and maximizing operating revenue. Thus it is seen that cost saving has been a driving factor in the quick adoption of this system. Bank branches have been shut down and subsequently, savings made from reduced staff remuneration and branch office maintenance budgets (Nwogu Emeka Reginald, 2012).

The massive adoption and deployment of the Internet banking system has been followed by increased probability of attack. Abaenewe Zeph et al. (2013) write that the adoption of electronic banking (e-banking) has brought major challenges to the banking industry in terms of risk exposure. The volume of deposits has increased as well as the fraudulent practices experienced by Nigerian banks since its adoption in the economy. According to Hole et al. (2012), the trend of growth of Online Banking brings many security issues and increasing cost of implementing higher security system for both Online Banking users and the banks. Hackers and Internet fraudsters are forever devising new means of crippling the security features embedded in the Internet banking systems. Consequently, there has been a renewed interest in a more robust system that would not only protect end user transactions from fraudulent attacks, but also prevent attacks like “Denial of Service” (DOS) attacks.

At different times, most of the defenses on Internet banking attacks have been reactive (Mathew Johnson, 2008). Security systems developers tend more to develop defense against well known attacks that probably have been over sung in the media and as such, less attention is given to research on current Internet banking system’s vulnerabilities; which definitely need adaptive solutions.

These days, attackers have become wiser, and several steps ahead of security systems developers. Sophisticated attacks have become the order of the day. Vulnerabilities on online transaction systems are continually searched for by these ever hardworking attackers and when found, heavily exploited. This has resulted in heavy losses by end users, who often are victims of circumstance, as majority of the clients who have fallen victims of these advanced online related frauds have in most times not contributed to their woes.

This work presents an analysis of ways that have been used to secure the Internet banking systems especially in Nigeria, and there levels of effectiveness.

II. INTERNET BANKING

Internet banking can be defined as a facility that allows customers of a financial institution to conduct financial transactions on a secure website operated by the institution, which can be a retail or virtual bank, credit union or building society (www.wikipedia.org). It can also be defined as a facility provided by banking and financial institutions that enables the user to execute bank related transactions through Internet (Scholasticus K, 2011). Also Guosong Shao (2007) defines it as performing financial transactions over the Internet through a bank's website. Furthermore, Basel Committee on Banking Supervision (2003) defines electronic banking to include the provision of retail and small value banking products and services through electronic channels as well as a large value electronic payment and other wholesale banking services delivered electronically.

The biggest advantage of Internet banking is that people can expend the services sitting at home, to transact business; meaning, the account holder does not have to visit the bank to be able to access the service.

With the help of Internet banking, many transactions can be executed by the account holder. When small transactions like balance inquiry, record of recent transaction, etc. are to be processed, the Internet banking facility proves to be very handy. The concept of Internet banking has thus become a revolution in the field of banking and finance.

Internet banking has progressively evolved with the development of the World Wide Web. Its origin could be traced back to 1980 when Programmers working on banking databases came up with ideas for online banking transactions. The creative process of development of these services was probably sparked off after many companies started the concept of online shopping which promoted the use of credit cards through Internet (Scholasticus K, 2011).

Sometime in the 1980s, banking and finance organizations in Europe and United States started suggestive researches and programming experiments on the concept of 'home banking', which before the Internet and computers made use of fax machines and telephones (Scholasticus K, 2011).

In 1983, the Nottingham Building Society (NBS) launched the first online banking service in the United Kingdom. This service formed the basis for most of the online banking facilities that followed, though, it restricted the number of transactions and functions that account holders could execute. The facility introduced by Nottingham Building Society was said to have been derived from a system known as Prestel, which was deployed by the postal service department of the United Kingdom (www.wikipedia.org). In the United States, the first online banking service developed by Stanford Federal Credit Union was introduced, in October 1994. However, it was on October 6, 1995 that Presidential Savings Bank first announced the facility for regular client use. The idea was quickly snapped up by other banks like WellsFargo, Chase Manhattan and Security First Network Bank (A. Mannan & M. Wagas, 2010).

A) Internet banking in Nigeria

The introduction of e-payment products in Nigeria commenced in 1996 with the Central Bank of Nigeria's granting of approval to Allstates Trust Bank to introduce a closed system electronic purse (Sanusi, 2002). Following this, was the introduction of a similar product called "Paycard" by Diamond Bank in February 1997. The card based e-money products assumed an open platform with the authorization in February 1998, of Smartcard Nigeria Plc, a company floated by a consortium of 19 banks to produce and manage cards called valucard and issued by the member banks (Ahmad Bello, 2006). Between 1998 and 2000, many Banks established their presence online by launching their websites in preparation for Internet banking.

A consortium of more than 20 banks under the auspices of Gemcard Nigeria Limited obtained CBN approval in November 1999 to introduce the "Smartpay" scheme.

Also, the CBN has granted approval to a number of banks to introduce international money transfer products, telephone banking and online banking via the Internet, (Abdulhakeem, 2002). Automated Teller Machines (ATMs) have been made available everywhere in Nigeria.

Recently, the Central Bank of Nigeria has been championing a cashless economy. This has ultimately paved way for the large scale deployment of Internet banking and associated services.

B) Levels of Internet banking

Abdul Mannan & M Wagas (2010) write that Internet banking has the following service areas:

1) Informational Level

This level is the most basic of the Internet banking systems. The Bank owns a standalone Server with information about the Banks services and products.

Normally, information systems would periodically receive such information from the Server. The risk is quite low as there is no direct connection between information systems and the Bank's internal network. However, appropriate control must be in place to prevent unauthorized access to the Server. This service can be outsourced or hosted by the Bank.

The diagram below explains this. Here, there is no direct connection between the bank's internal network and the public network. The Server containing information about the bank's products and services is periodically updated with the latest information on Bank's products and services.

2) Communicative Level

This level of Internet banking system allows some interaction between the bank's information system and the customer. Normally, this interaction is limited to account

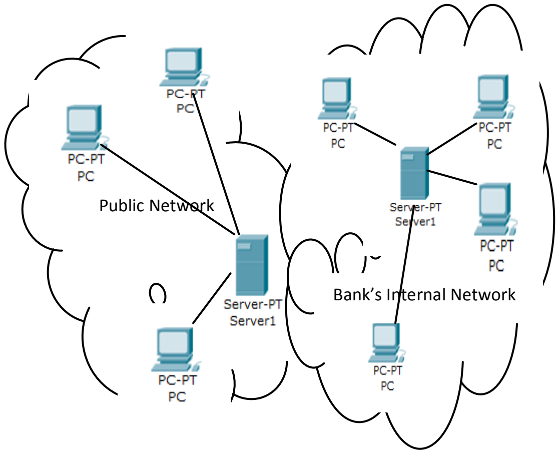

Fig. 1: Informational level of Internet banking

inquiry, loan applications, electronic mail notifications and customer information update. Risks are higher in this level of Internet banking system since there may be direct connection between the Server and the bank's internal network. Appropriate controls should be in place to prevent, monitor and alert Bank management of any unauthorized attempt to access the bank's internal networks and computer systems. Such devices for this would be an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS). Normally, the public Server will be located in a Demilitarized Zone (DMZ).

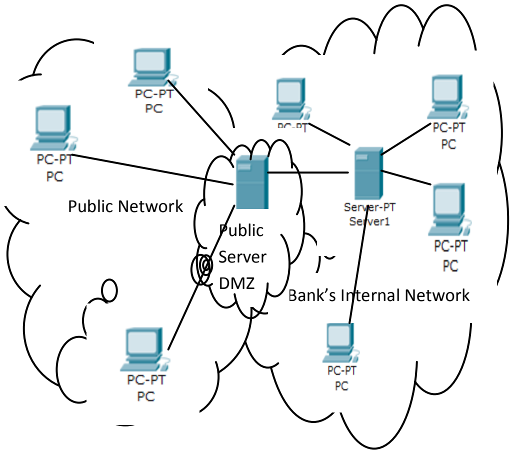

Fig. 2: Communicative level of Internet banking

3) Transactional Level

This is the highest level of Internet Banking. It allows customers to execute transaction. Customers can perform such transactions as account access, fund transfer and payment of bills. A path exists between the Internet banking Server and the Bank's internal network. The most risks exist at this level of internet banking, and thus the strongest control is provided at this level.

C) Advantages of Internet banking

Internet banking has so many advantages to the Customers and even the banks. Some of the advantages are as follow:

i. Time is saved on queuing in banks.
ii. It removes geographical limitations for small and medium size Banks, giving them access to international presence without limits.
iii. No time limits, as transactions can be done at anytime of the day, provided the customer has access to the Internet.
iv. It cuts down on the resources needed to perform a transaction such as time, labour and capital.
v. Provides efficient cash management for interest organizations.
vi. Banks can save money on branch expansion and staff remuneration.

D) Issues with Internet banking

Despite having so many advantages, Internet banking has got its problems. These problems, when not properly addressed normally lead to heavy losses on the sides of both customers and banks.

The main problem with Internet banking has been that of securing the system from unauthorized access.

There have been concerns about customers' knowledge of the system's operation and use. Most customers are still oblivious of the security challenges associated with this service; as a result, the vulnerability of these customers to Internet banking attacks continues to grow. There have been cases of incomplete sign out from such systems by ignorant users, often leading to attacks resulting in heavy fund transfer from customer's account to an attacker's choice account.

Another problem with Internet banking has been the unavailability of the Internet service. Most African localities do not have Internet service facilities. This limits the accessibility of this service to potential users.

E) Major forms of Internet banking attacks

According to Mathew Johnson (2007), there are four main types of attack on Internet banking services and facilities. All attacks seen at the moment fall into the following categories:

- Getting authentication credentials from the victim
- Modifying the victim's legitimate transactions
- Denying the victim access to a banking service
- Observing the transactions of the victim.

Getting authentication credentials from the victim

In this category of attacks which is sometimes referred to as credential harvesting, victims are convinced to divulge their online banking credentials to a third party. This class of attacks is carried out using the following tools and techniques; trojans, social engineering, shoulder surfing, phishing and vishing.

According to Mathew Johnson (2007), Phishing websites are the most commonly seen form of credential harvesting attacks in the world. This form of attack has become very popular in Nigeria.

There are different ways by which credential harvesting is achieved. They include:

1. Typo-squatting – a technique where an attacker registers similar domains to the target website, either through simple spelling mistakes or common typing errors. The attacker subsequently sends mails to people directing them to the fake website where their credentials are harvested.
2. Sub-domain attacks – in this, attackers take advantage of the fact that users may not tell the difference between seemingly related URLs such as *www.zenithbank.com* and *www.zenithbanking.com*. An average Internet user will assume the two sites are owned by the same company and thus overlook the difference. This is made easier by the fact that many companies use URLs outside their normal domain for legitimate sites.
3. Image/3-D Spam – similarly, in Image/3-D spam, Spam producers have also invented techniques to foil classifiers which inspect their emails. There are spams that have the real text in an image rather than the email body. There are also reports of spams in which the text is distorted by applying 3-D transformations to make text-extraction from the image more difficult (Mikko Hyppnen, 2007).
4. Shoulder surfing is another method where an attacker surreptitiously observes someone entering their credentials in person by looking over their shoulder (Mathew Johnson, 2007). This attack is normally associated with observing the personal identification number (PIN) for a debit or credit card issued by a bank and subsequently stealing the card either by force or pick-pocketing.
5. Hardware keyloggers – these are devices that are inserted at the back of the computer to capture keyboard inputs. They are normally cheap and easy to produce. Hardware keyloggers are used on public computers, such as Internet Cafes' and will require data processing to find any credential.
6. Vishing is another term and tool used by attackers to harvest customers' credentials. An attacker phones the victim and uses social engineering to trick them into divulging secret information such as credit card information. Today, Voice-Over-IP (VoIP) has been used in carrying out these attacks together with automated answering systems. An attacker can dial several numbers and use an automated system to request for details, especially credit card information. Once someone has fallen victim to the automated system, the attacker would involve a human being.

Modifying the victim's legitimate transactions

These involve attacks that modify a victim's transactions or operations, with the intention of defrauding the victim. One way that has been used to achieve this is Traffic Injection. This refers to attacks that modify transactions being made by the user in order to redirect funds or change the amounts concerned. It is done by hacking a router through which the traffic passes, manipulating the Internet routing systems or forging packets. There have been many defenses against this attack, and as a result, it has become uncommon.

Denying the victim access to banking service

Similarly, most attacks are done with the intent of denying the user access to the services they need. "Denial of Service" is a good example of such an attack. It refers to any attack which stops the user from carrying out legitimate transactions. The various schemes have been used to achieve this include:

Synchronous (SYN) flooding, where a flood of packets are sent to a server requesting a client connection. These packets contain invalid source IP addresses, and consequently the server becomes occupied trying to respond to these fake requests, therefore greatly reducing its chances of responding to legitimate ones.

There is also "Ping of death", where a packet greater than 65,535 bytes which is the maximum allowed by Internet Protocol is sent to a device. This can cause the receiving system to crash.

Observing the transactions of the victim

In some attacks, the attacker only observes the victim's transactions and may not be able to alter the transaction or defraud the victim. However, observing a victim's transactions may still be harmful to the transaction, as the attacker could get very useful information that may be used in other forms of attack.

F) Internet banking attack vectors

Attack vectors simply refer to the ways in which attacks are carried out. Marco Morana and Scott Nusbaum (2008) define attack vector as a path or means by which a hacker can gain access to a computer or network server in order to deliver a payload or malicious outcome. These vectors include Social Engineering, Public Web Proxy/Anonymizer, Rogue Access Points, Hacking en-route Routers, etc.

Social Engineering is the art of getting people to comply with ones wishes in order to gain access to computer systems and information that is contained in it (Rajendra Maurya, 2013). The goal of social engineering is to obtain information that allows a hacker to gain unauthorized access to a system to commit fraud, identity theft, disrupt or compromise a network, or to commit industrial espionage (Rajendra Maurya, 2013). It involves a situation where an attacker tries to convince targets to do something they shouldn't do ordinarily. Social engineers can be internal or external to an organization. One method used to achieve this attack is Pretexting or Blagging. This is the act of creating and using an invented scenario (the pretext) to engage a targeted victim in a way that increases the chances of them divulging information or performing actions that would be unlikely in ordinary circumstances (Faraz Davani, 2011). In the United States, this is known as "Pretexting" while in the United Kingdom it is referred to as "Blagging".

An Anonymizer, also called Anonymous proxy is a tool that attempts to make activity on the internet untraceable. It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet. It accesses the Internet on behalf of the user, protecting personal information by hiding the client computer's identifying information. This has been used by attackers to perpetrate high level attacks. If an attacker can solicit the traffic they wish to alter through their proxy, they can redirect any requests and observe any non-TLS traffic. The attacker could redirect the connection to their website, where they observe or modify the traffic. Most victims are unlikely to notice they have been redirected elsewhere and even if they do notice, most may think it is legitimate.

A Rogue Access Point is a wireless access point that has either been installed on a secure company network without explicit authorization from the local network administrator or has been created to allow a hacker to conduct a man-in-the-middle attack (Jim Geier, 2003). When a rogue Access Point is set up by an attacker, most wireless network users will connect to this Access Point, especially when access is free. The fact that some wireless cards can be run in infrastructure mode where an Access Point could be a laptop, even makes it a lot easier for attackers. For a customer, it could be very difficult to identify a real Access Point. The conventional security mechanisms do not help here either. The use of symmetric keys means that if attackers can access the real Access Point, they can also run a rogue Access Point for it. Once the victim has connected to this rogue Access Point, all traffic can be sniffed or modified by the attacker.

Hacking en-route routers/servers involves compromising of a router between the target machine and the destination of the traffic in order to intercept data. This in turn leads to observation and most times modification of the data on transit. Though lots of defenses have focused on this type of attack, it still remains a problem.

DNS Poisoning is also an attack vector, where an attacker inserts bogus entries into the cache of a recursing name Server. These entries are then returned when users access this name Server. DNS poisoning allows an attacker to redirect connection to the target domain to a machine under their control, making injection and modification attacks possible.

Lastly, Trojans/Worms/Viruses are also vectors that can be used in carrying out Internet banking attacks. A virus is by definition a computer program that spreads or replicates by copying itself (F-Secure Corporation 2001). Usually, it does this by attaching itself to an already existing file, program or drive on the Computer. A virus will mostly be designed with the sole intent of disrupting the smooth operation of the program or drive where it is attached to, thereby resulting to a "Denial of service" attack.

A Worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer. Worms, unlike computer viruses do not need to attach themselves to an already existing file, drive or program. When worms are introduced on the network or Internet banking server, they tend to take up the bandwidth available to legitimate users. This can result in excessive delays or outright "Denial of service" attacks.

III. RESEARCH METHODOLOGY

This work followed a simple analytical and scientific procedure. First, was the choice of this work as a research work; and then the sourcing of the basic information required to achieve the desired goals and objectives.

The research implementation proper, started with an analysis of the current Internet banking systems, with particular interest in the vulnerabilities and security threats associated with the current system as deployed in Nigeria. Later was the analysis of the current defense mechanisms available to counteract these threats and vulnerabilities. An analysis of the limitations of these defense systems, were also carried out.

There were two main design approaches considered in this work, namely; Inductive reasoning (Bottom up) and Deductive reasoning (Top down) approaches. (William M.K. Trochim, 2006).

Inductive reasoning involves working up from the different units making up a system to the whole system (William M.K. Trochim, 2006).

Deductive reasoning on the other hand works from the more general to the more specific (William M.K. Trochim, 2006). It entails starting a research work from the conception of the whole system down to the individual units making up the system.

In this work, Deductive reasoning approach was adopted because it allowed for flexibility and made research goals actualization a lot easier.

The actualization of this research work was made possible using various tools which include:

- The Internet.
- Books, journals and other related materials sourced from different real and virtual libraries.
- Online materials published on different websites on Internet banking attack strategies.

- Questionnaire administered to bank management and Information Technology staff in Nigeria
- Interviews conducted to bank management and Information Technology staff in Nigeria.

IV. CURRENT INTERNET BANKING SECURITY MEASURES

In this section, we analyzed the current Internet banking security measures. The analysis involved the banks provided measures in Nigeria and the generic security measures. We also evaluated the effectiveness of these measures in the overall security of online banking in Nigeria.

A) Protection of user Private Identification Number (PIN)

In Nigeria, intentional and unintentional disclosure and access to user Private Identification Number (PIN) have been an issue in online banking, especially in the E-payment and Automated Teller Machines (ATMs). This has been mainly due to lack of proper user and security awareness by Debit/Credit card users in Nigeria. Banks have made efforts to protect customers against PIN snooping both with the physical architecture of the ATM points and intense customer card-use awareness campaigns.

Most ATM points are built, in such a way that people waiting on queue to use the machine would not see what the ATM user does or types on the ATM. This makes it difficult for an attacker to snoop customers' PINs.

Also in the card-use customer agreement section, customers are warned strongly to secure their PINs and not disclose it to anybody.

Once a customer is issued with their new card, the card is accompanied with the default PIN which cannot be used for any other transaction except card activation. The customer is subsequently asked to activate their card themselves which also involves change of the default PIN to a new PIN known only to the customer. This new PIN can now be used for other account transactions such as cash withdrawal and money transfer. The fact that customers sign on receipt of their new card and are subsequently asked to activate the card themselves ensures that fraudulent bank-staff do not have access to customers' account through their cards and PINs.

Also in trying to access the Automated Teller Machines, customers also see notice on the ATM display screens warning them not to disclose their card information and PIN to anybody.

Despite all these, chances are that more customers will fall victim to PIN snooping. Attackers may hide under the pretence of helping a customer work around there ATM challenges to snoop their PINs and card information. The customer in desperate need for help responds to the dictates of the attacker.

Also corrupt bank staff may collude with external criminals to carry out an attack on a customer. This corrupt bank staff snoops the account and card information of certain customers especially the ignorant customers; while their external agents wait patiently for such an opportunity to snoop the customers PIN, which when completed can give them some level of access to customer's account to carry out some attacks. This raises another question about the integrity of people hired to work in banks, as banks cannot ultimately ascertain the level of integrity of a prospective employee or even existing employees.

Attackers have also resorted to credential harvesting techniques to snoop customers' account, card and PIN information. Such techniques as phishing, social engineering and vishing have been used widely.

B) Protection of users from unauthorized use of their cards on the internet

As online banking becomes more popular in Nigeria with the introduction of Internet banking and other associated features, vulnerability becomes even more intense with these products. Today, customers can sit in the comfort of their homes and make transactions worth millions without visiting a bank or even the ATMs. Customers only need to use their card information (credit/debit card number, security code and card expiration date) together with their PIN to move money from one account to another or even pay for products online. This opens another era of possibilities and opportunities for attackers. If an attacker can get your PIN, he does not need to have the card to carry out their attacks, they only need to have just the card information and they can go online, move money from your account to another, pay for products online and even perform more complex operations.

With the help of card managers and internet banking application developers, banks have introduced measures to help stop attack operations resulting from the poor security provided by customers' PIN.

One-Time Passwords (OTP) has been used by banks to further add security on online banking systems in Nigeria. Customers are given hardware token devices which are linked to customers' accounts, this allow them supply a number from a set of pre-set numbers to enable a transaction. Once a customer has initiated a transaction, the system requests for this One-Time-Password; a customer only needs to press the generate key of the hardware token to generate a password which is subsequently entered on the system to enable the transaction. Once generated, the OTP remains valid only for five minutes, and if not used within this time, becomes useless. Also just as the name implies, a particular OTP can only be used once.

Some banks have also introduced another version of this, which they call software token. This allows a customer to send a short message service (SMS) phone challenge to a number provided by their bank through their cell phone in the course of the transaction. The bank in turn, responds by sending software generated OTP which the customer uses to enable and complete their transaction. Banks have limited the use of the software token to transactions involving a small amount of money, usually not more than a hundred thousand naira.

In a bid to harden the internet banking system, Mastercard introduced another level of security called "securecode". This allows Mastercard card users to register their card for a secret code different from the normal user PIN. This code is requested for by participating merchants anytime a transaction is made online by a card user. Once a customer initiates a transaction, a window opens, which prompts the customer to enter their securecode. Failure to enter the correct code results in the cancellation of the transaction.

All these measures can only work when the customer does their transactions on a recognized third party payment gateway. Nigerian online business community is now implementing online payment using recognized third party payment gateways, like interswitch, paypal etc. This is in a bid to ensure integrity in online transactions.

However, attackers have set up credential harvesting payment gateways where customers supply their card and account information thinking they are doing business with genuine business-people. This information when snooped is subsequently used by the attackers to defraud the customer. This makes it impossible to eliminate attacks.

C) Protection of customers against phishing

Banks have also taken measures to counteract the damages posed by phishing agents. Periodically, emails and text messages are sent to customers warning them to disregard any emails phone calls or websites requesting them to supply or disclose their account and card information to anybody. Though this has helped in stemming the frequency of successful attacks through phishing, it has not entirely eliminated it. More worrisome is the fact that, banks cannot afford to stop the activities of phishing agents.

Despite constant warnings from banks to their customers, a lot more customers continue to fall victim to this attack. Money continues to be stolen from customer accounts as a result of phishing activities.

There is also the concern about integrity. How would a customer know that the source of a warning message is their bank? There have also been reports of phishing agents achieving their aims by pretending to render help to customers and eventually clinching it with heavy attacks that leave customers suffering great losses. Some phishing agents have commenced their attacks by first warning customers of a possible attack, while pretending to be their bankers or a trusted party. The customer in return trusts the source of this message or email and subsequently falls victim to the attack that follows.

D) Transport Layer Security (TLS) protocol

Transport Layer Security (TLS) protocol uses a key-agreement protocol such as Diffie-Hellman to establish a confidential channel with integrity guarantee between two parties. Authentication of the server is provided by an X509 certificate chain rooted in one of several trusted third parties whose certificates are provided to clients out-of-band.

TLS is a very popular protocol for securing traffic on the Internet, particularly in the World Wide Web. Most financial and other sensitive data are protected using TLS while on transit across the Internet.

The bad side is that due to the costs of acquiring TLS certificates, many sites have certificates which are not rooted in the trusted certificates shipped with the browser. When presented with such a certificate, browsers will normally prompt the user to accept it. Such prompts do not provide information which will allow the majority of users to make an appropriate security decision since they do not understand the terms used. In such cases, the user, who only wants access to the content, would simply accept. Another problem with the user understanding TLS certificates is that even when they are valid and rooted in a trusted third party; it is not always clear what they are authenticating.

E) Protection against keyboard sniffing

As a result of keyboard sniffing programs and devices such as the hardware keylogger, most internet banking and e payment applications and websites have introduced PIN entry with the mouse through an on-screen keyboard. Examples of these are online shopping and payment gateways. Banks have also implemented PINs and security codes entry via the on-screen keyboards on their internet banking sites and applications. This has limited attacks through the hardware keystroke loggers since no keys are pressed.

However, these techniques do not protect against Trojan horses which have the ability to capture screenshots and mouse movements. The on-screen keyboard also has several other problems; it makes 'shoulder surfing' attacks a lot easier.

Though it has been argued that victims of online banking attacks have been the ignorant customers, there is still a general belief that more needs to be done to protect customers from these attackers.

V. CONCLUSION

The implications of the study presented here are quite enormous and positive. The study presented here has been able to expose us to most of the attacks that have been seen in the Nigerian online banking platform. Again, it has highlighted the threats and vulnerabilities that are prevalent on Internet banking systems as deployed in Nigeria. We have also done a detailed study of the effectiveness of the defense mechanisms currently in use on Internet banking systems. Findings reveal a lot more needs to be done to protect customers from the activities of these ever hardworking attackers.

Although the Nigerian public has not embraced online banking fully, but with the campaigns by the Central Bank of Nigeria for a cashless economy, analysts forecast mass acceptance and reliance on online banking and its associated services in Nigeria; which has reawakened the concern for a secure online banking system that not only protects customers from possible attacks, but also takes care of customers' service needs.

There has been a generally shared school of thought by operators that maybe a proper user education may go a long way in stemming most of the popular and dangerous attacks on user accounts.

REFERENCES

Nwogu Emeka Reginald (2012, December). Internet Banking Implementation in Nigeria; Security Issues Analysis and Solutions.

Abaenewe Zeph, Ogbulu Onyemachi and Ndugbu Michael (2013 March). Electronic Banking and Bank Performance in Nigeria. West African Journal of Industrial & Academic Research Vol. 6, No. 1.

Simpson, J. (2002). The Impact of the Internet in Banking: Observations and Evidence from Developed and Emerging Markets. Telematics and Informatics, 19, pp. 315-330.

Basel Committee on Banking Supervision (2003). Risk Management Principles for Electronic Banking. Switzerland Bank for International Settlements. Retrieved 13th June, 2012, http://www.bis./pub/bcbs/pdf.

Hole, Moen and Tjostheim (2013). An Analysis of the Online Banking Security Issues. Department of Computer Science, University of Auckland.

Matthew Johnson and Simon Moore (2007). A new approach to e-banking. In U´ lfar Erlingsson and Andrei Sabelfeld, editors, Proc. 12th Nordic Workshop on Secure IT Systems (NORDSEC 2007), pages 127–138. Retrieved. May 14, 2012, http://www.matthew.ath.cx/publications/2007-Johnson ebanking.pdf.

Wikipedia. Online banking. Retrieved Sept, 15, 2013 from http://en.wikipedia.org/wiki/Online_banking

Scholasticus K. (July 2011). History of Internet Banking, Retrieved Septemberl 1, 2012 from http://www.buzzle.com/articles/history-of-internet banking.html

Guosong Shao (2007). The Diffusion of Online Banking Research Trends from 1998 to 2006. Journal of Internet Banking and Commerce, August 2007, Vol. 12, No. 2.

Abdul mannan and M. Wagas. (2010). Online banking and role of IT in online. (Sanusi, 2002).

AbdulHakeem, A (2002, May 6), "Smartpay to Launch T-Commerce", ThisDay Newspaper, Vol. 8, p.9

Mikko Hyppnen. (2007, Sept).3D spam. F-Secure Weblog. Retrieved July 8, 2014, from http://www.f-secure.com/weblog/archives/archive

Faraz Davani (2011, August). HP pretexting scandal. Retrieved August 18, 2013, http://www.scribd.com/doc/62262162/HP-Pretexting

Rajendra Maurya (2013, May). Manipulating the human mind: a guide to social engineering. Scorpio Net Security Services New Delhi India.

Jim Geier (2003, January). Identifying Rogue Access Points. Retrieved June 14, 2014, from http://www.wi-fiplanet.com/tutorials/article.php/1564431

William M.K. Trochim (2006, October). Research Methods Knowledge Base. Retrieved August 8, 2012, http://www.socialresearchmethods.net/kb/index.php

Marco Morana and Scott Nusbaum (2008). Input Validation Vulnerabilities, Encoded Attack Vectors and Mitigations. OWASP Cincinnati Chapter September 2008 Meeting. Retrieved February 20, 2014, https://www.owasp.org/images/6/6c/Encoded_Attacks_Threats_Countermeasures_9_30_08.pdf

F-Secure Corporation (2001 September). Computer Viruses – from an Annoyance to a Serious Threat. Retrieved February 14, 2014, http://www.bbox.ch/Beilagen/virus.pdf