INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

A Detailed Study of Electronic Banking Security Techniques and Safety Measures

Eneji, Samuel Eneji
Lecturer, Federal College of Education, Obudu, Cross River State, Nigeria
Dr. Onu, Fergus Uchenna
Senior Lecturer, Ebonyi State University, Abakaliki, Nigeria
Ibe, Walter Eyong
Lecturer, Department of Computer Science, Federal College of Education, Obudu, Cross River State, Nigeria

Abstract:
Banking security has been challenged over times. Worst is the modern banking systems which make use of communication technology and gadgets. Fraudsters these days don't need to surface physically in the banking premises to cart away monies, they stay in their convenient and cart away huge some of monies from the banks, or their victims with less stress. This calls for concerns. This paper reviewed security measures needed to combat such ugly security trends with the modern banking systems, analyze attacks on the electronic banking systems as well as safe practices by customers as a preventive measure against electronic banking fraud.

Keywords: *Electronic, Banking, Security, and Technique*

1. Introduction

The banking system is one of the major aspects driving the economy of a country. Variety of the banking systems and operations has been the synergy that classifies the modern banking system. The bank houses one of the valuables, the "almighty money", the force that drives both the good and the bad conceptual ideologies of the world today. The might of money and what money can do has made its desire and demand second-to-none. Money is a deity that rules the world. Today, no money invariably means no nation, no man, so bad such that, some people exchange integrity, even life all to have money. Rubbers will bring down buildings, take away peoples' lives; do all forms of atrocities all for money. Politicians can run down a whole system just to embezzle public funds for personal sake. Worst is in the developing countries where the slogan for livelihood is "survival of the fittest", which implies the elimination of the unfit [iv].

The quest for money by all class of citizens has made money essential commodity such that, the legal means to acquire money has been bastardized. Today, you can rub, murder, steal, burgle, kidnap or commit fraud to get money. Based on this, wherever money is housed, is endangered, who ever owns much money and is publicly known is also at risk of those who will want to forcefully own the money.

Because of the numerous problems associated with the safe keeping of money, monies are kept in strong rooms with maximum security, convey in a security tide van with adequate and well-equipped security men, and the amount of money own, accessed, deposited, withdrawn or transfer at any point in time by individuals or corporative is being regulated by money laundry policy nationally and internationally [xvi].

Statutorily, monies are kept in the bank for safe keeping, though; there are instances of breaking into banks and carting away with huge sum of money. This would have been worst if monies were kept by individuals at homes in large sum. The convenience of managing bank customers satisfactorily necessitated the introduction of electronic banking such as internet banking, mobile banking SMS banking, phone banking, etc. where the banking system is 24 hours a day, 7 days a week, 4 weeks a month, and 12 months in the year at the customers convenient and disposal, provided he or she has the gadgets to effect same. Electronic banking has been integrated with evolving securities in accordance to evolution in knowledge, and technology, but still, fraudsters take advantage of the social engineering vulnerability, and the lack of trust and integrity of the bankers to defraud banks and bank customers through the electronic banking platform. For instance, the USA lost about $3.5 trillion daily through three payment network which dwarf the bank of New York's [ix]. In February, 2005, a Miami businessman sues his bank for the loss of $90,000, which was stolen from his online banking account by an unauthorized transaction. On investigation of the matter, it was discovered that the transaction was affected from his computer that was

infected with Trojan capable of logging keystrokes invading his full account details [xviii]. According to, [xviii], the prevalence of malicious applications that steal financial account information has measured dramatically over the years, which often result in victims losing huge amount of money.

Electronic banking fraud gain momentum in the early years probably due to the higher chances to succeed than expected. At these times, Trojan was the prevalent avenue used in stealing financial account information targeted only on handful of online banks.

Wùeest, [xviii] analyzed Trojan used in stealing financial details of individuals as follows;

- ✓ PWSteal: it is a Trojan that was discovered in April 2005 that stole account information from five banks. It contained a list of 2,764 URLs from 59 different domains
- ✓ Trojan.Goldun: this was another Trojan discovered in April 2005 which steals account from online payment service called e-gold. The Trojan. Goldum disguised itself as a security update for e-gold organization. It presents a deceptive file named security e-gold.exe. Once a user executes the deceptive file, the Trojan will register itself as a Browser Helper Object (BHO) where it monitors for visits to the pre-defined URLs from which it gathers account information of victims. The account information gathered was transmitted through a PHP script to a domain mounted by the attacker.

It has become imperative for banks which offer online banking to integrate efficient security models [xiv]. In the past years, the growth of malware and exploits targeting online banking vulnerability has been growing steadily [xiv]. In 2009, it was reported that the 50 main electronic threats were bank Trojans [xiv].

In an attempt to provide a more secured security to electronic banking was the introduction of several security techniques such as the use of PIN, digital certificate, virtual keyboards, Browser protection, etc, [xiv]. Data validation technique was proposed in 2014 by Aljawarneh and co. in their work title Usage of data validation techniques in online banking: A perspective and case study. The essence of the work was to consider the integrity of data (i.e. authentication of source of data) to ensure that it is from a reliable source before it is given access to be used in electronic banking platform [iii]. Proposed also was the use of biometric security to ensure that the user of electronic banking application is the only one who can access his account, using biometric authentication [xvii].

[ii] suggested the inclusion of Geographical Position Location (GPs) with real time security system to unveil criminals' anonymity.

This paper takes a critical examination on electronic banking system techniques.

1.1. Attacks on Electronic Banking System

Attacks on electronic banking system simply referred to measures or techniques used in breaking into electronic banking transactions fraudulently. [xii] analyses online electronic banking attacks to include;

i. Social Engineering: attacks based on tricking customers to divulge their secret identities to fraudsters through social media. The fraudsters make use of customers' limited knowledge of computer systems to their fraudulent advantage. They send text messages, calls, or links (phishing and spooling) to customers demanding their secret banking information through which they take advantage of their victims and defraud them.
ii. Port Scanners: Attackers use various techniques to steal customers' information by using port scanners to ascertain entry points of customers into a system. Here, they place software which do repeated scanning of the information going through the targeted port until they are able to sniff customers banking information.
iii. Packet Sniffers: Attackers mount surveillance on the connection between the user's computer and the web server to sniff customers' information including credit card information and password. It therefore becomes possible to defraud such victims.
iv. Password Cracking: This involved the use of Brute Force and other vulnerability decrypting techniques to crack customers' user name and password for a specific website by scanning thousands of common terms, words, activities and names until a combination of them is granted access to a server.
v. Trojans: A Trojan is software that masquerade a host system requesting for a gateway before access is granted. Trojan is said to be the most dangerous security threat to electronic transactions due to its ability to secretly connect and send confidential information about customers' secret information. Trojans are developed with the intention of anonymity. They can be used to filter data from many different clients, servers and database systems. They can be installed as surveillance on emails, internet messages, database communications, and other services.
vi. Denial of Service Attacks: The attack is used to overload servers and render it vulnerable. The technique is to place heavy chunk of task on the server repeatedly until the server could no longer function well. The attacker then uses the vulnerability of the server at the moment and install virus or Trojan onto the users' PCs and instruct them to carry out specific attack on the server.
vii. Server Bugs: Server bugs are used to confuse the server intrusion detection system, thereby allowing attackers the opportunity to generate threads with millions of web servers in use around the world. This renders the server vulnerable to onslaught of server bugs and threats.

viii. Super User Exploits: This is a technique which allows the attackers to gain control of the system as if they were the system administrator. This is achieved by the use of scripts by the attackers to manipulate the database or buffer overflow that cripples the system.

1.2. Electronic Banking Security Techniques

The advances in technology such as the super-fast broadcast broadband connections for real time transmission, the high definition of 3D and 4D video content to personal homes, the emergence of cloud computing, the complemented physical network infrastructure such as WiFi, 3G, 4G, Wimax, etc, has enhanced and encourage the application of technology in information processing and online businesses [xi]. On same technology, electronic banking finds its operation. For the sensitive nature of electronic banking, the following security measures have been put in place as stated by, [xiv] and, [xii]), [x].

I. Digital Certificate: Digital certificate requires a trusted third-party who ascertains the authenticity of the transaction by signing the authentication certificates attesting their validity. The authentication depends on public key transaction (PKI) and certificate authority (CA). Digital certificate is used to authenticate both the user and the bank.
II. One Time Password Tokens: One-time password token is a second authentication factor which is a code in the form of password, requested in specific or random situation generated by the application and forwarded to a registered device of the user. The operation is authenticated and preceded if the password is entered as required within the predefined time interval. This measure renders captured authentication data by fraudsters useless for future attacks; hence the password is changed dynamically, and used once within allowable time frame.
III. One-Time Password Cards: One-Time password card is a card used in generating passwords which are used for second authentication factor like the One-Time Password Tokens. The challenge with One-Time password card is that some banks allow for a reuse of password generated over some times which makes it vulnerable for attacks.
IV. Browser Protection: Browser protection is a security model which is secured at the internet browser level used to access the banking system. In browser protection, the user and its browser are secured against known malware. This is achieved by monitoring the memory area allocated by the browser with the intention of detecting such malware, as well as hindering credential theft and capturing of sensitive information.
V. Virtual Keyboard: Virtual keyboard in recent times has been replaced with a more efficient method that requires less processing power, and slower transmission rate. Virtual keyboard is a device usually based on Java and software cryptography which allows portability between different devices. Virtual keyboard thwart the efficient use of key loggers which capture information typed into the device.
VI. Device Registering: in the case of registering with the banking system for an online transaction, the device to be used by the customer is registered with the bank database (especially in mobile banking). The bank will in the cause of transaction ensures that the registered device is the one used for such a transaction, otherwise, such transaction is refuted. For better authentication, hardware fingerprinting techniques are used in conjunction with user identification through secret credentials.
VII. CAPTCHA: CAPTCHA solution is an automated test designed to detect and render ineffective automated attacks against authentic services. CAPTCHA solution helps to safe guard the customer from password guessing attack on the identity. The method conveys information to the user in the form of scrambled images which automated robots find difficulty to recognize and process. When the user is able to enter the scrambled image correctly, it makes him or her a legitimate user.
VIII. Short Message Service (SMS). SMS is used to send short messages to a dedicated phone number of the owner of the account, seeking authorization to go ahead with such a transaction.
IX. Device Identification: This technique is used together with the device registration. The method uses the physical characteristics of the user's device to identify the original and historical information of the users.
X. Positive Identification: In positive identification, the user is expected to supply some secret information only known to him as means of identity. This information must have been provided and saved in the banking database against the customer's session at the first time of using the banking application.
XI. Pass-Phrase: Pass-phrase is likened to a password, except that it is a phrase. Pass-phrase is a second authentication factor which requires that a customer identifies himself by providing a phrase held by him as a gateway.
XII. Transaction Monitoring: Transaction Monitoring requires the use of business auditing model to monitor activity such as payment processing. The logs are monitored and reviewed to detect pattern of inappropriate transactions at the business process level.
XIII. Education: As basic requirements for electronic banking security defense, the user (customer) should have a very good knowledge of electronic banking security trends. By so doing, it becomes pertinent for the customer to provide strong passwords, and avoid all forms of internet practices which are security vulnerable.
XIV. Personal Firewalls: This is concerned with the use of firewalls to limit the types of traffic initiated and directed to your computer.
XV. Secure Sockets Layer (SSL): SSL model is a protocol that encrypts data between the customer's system and the site's server. The SSL monitors request made from an SSL protected page by;
    - Identifying the server as a trusted entity

- Initiate a handshake to pass encrypted information back and forth between the customer's system and the site's server.

The idea is to ensure that information passing back and forth between the customer's system and the site's server are encrypted to make it meaningless, incase hackers intercept and sniff the information.

XVI. Server Firewalls: A firewall houses the web server to ensure that all requests made enter the system from specialized ports only, and in some cases, ensure that all access are from certain physical machines only. Demilitarized zone (DMZ) of using two (2) firewalls is the common technique use in server firewalls security, which are;

(a) The outer firewalls that monitor the ingoing and outgoing HTTP requests while the client browser communicates with the server.

(b) The inner firewalls which sit behind the e-commerce server.

The two firewalls are built with intrusion detection software which is use to detect any unauthorized access attempt.

The server firewalls also used the honey pot server technique in addition to the DMZ. The honey pot is a resource such as a fake payment server, which is placed in the DMZ to deceive the hackers into thinking that he or she has gained access into the system. Surveillance is placed on the servers and closely monitored to detect access by an attacker.

XVII. Intrusion Detection and Audit of security Log: A good security system is the one that can detect and prevent attacks. Intrusion detection system monitors the activities of the users of the system, use the intelligent build-in- software to detect suspicious activities either base on role functions, or attempts to access resources out of sites. The intrusion detection system on detecting abnormality in the operations of the user, will block the user or log him or her out, then generate messages to the system Admin for thorough investigation and apprehension where possible.

[3], proposed data validation techniques as a measure for online banking security. In their work, they observed that the main security issue in electronic banking was the absent or insufficient data validation technique. Security issues of electronic banking caused by input validation include:

i. Parameter manipulation leading to the subversion of logic or security control.

ii. Code injection, such as cross site scripting, Structural Query Language (SQL) injection and operating system command injection attacks.

iii. Legacy CLC++ vulnerability classes, such as buffer overflows, integer wrap and format string vulnerabilities [iii]. [xiii] defines data validation as the process of ensuring that a web application operates on clean, correct and meaningful data. This implies that, a data validation rule should be applied to online banking systems to check for correctness, meaningfulness and security of data.

In support of all the proposed and implemented security measures for electronic banking, [xi], observed that biometrics is an ideal tool for person's authentication for applications on online transaction. They defined biometrics as measurable physiological and behavioural characteristics such as fingerprints iris, face, voice and handwritten signatures.

Biometrics requires the physical presence of the person as such cannot be easily guessed, forged or lost. With these features of biometrics, it therefore, becomes a very outstanding measure for online authentication.

2. Safety Measures Required by Customers as a Defence against Electronic Banking Fraud

[vii], [vi], [i], stated the following as safe practices by banks customers against electronic banking fraud;

1) End user should adopt good online habits and necessary precautions against being circumvented.
2) Customers should keep their account details as top secrets
3) Customers should be conscious of social engineering tactics.
4) Customers should be acquainted with bank security measures such as to;
   - Confirm that the URL of the website is the same with that of his bank.
   - Ensure that the SSL certificate of the website issued to his bank is by trusted certifying agent and within the validity period.
   - Ensure that the website process is the same when accessed from a different device.
5) Customers should practice safe surfing habits
6) Customers should check his bank account transaction regularly for variations.
7) Update your device regularly with antivirus software, operating system patches, firewalls, etc, and ensure that your browser is set to the highest level of security.
8) Be careful of unsolicited emails or phone calls requesting for PINs or password.
9) Always type your bank address into your web browser.
10) Never enter your personal details in a link you follow in an email
11) Ensure that before you do your online banking transactions, there is either a locked padlock or unbroken key symbol in your browser window.
12) Ensure that you double check the account number you want to use, for making payments before effecting such payments.
13) Never leave your computer idle when you are already login
14) Always logout when you are done with your online transactions.
15) Be careful of unexpected or suspicious popup windows that appear during your online banking session.

3. Conclusion

Electronic banking holds much deliverables in today's banking transactions, and the future. The banking system has been miniaturized such that, as portable as the mobile phone is, it can carry the whole banking system making banking services available to customers any-where-you-go. This is achieved by simply connecting the user's website from his portable and mobile device (i.e. from the end user) to his site in the bank server. The transaction requires a to-and-fro communication between the client's server and the host. Attackers make use of the communication gab and system vulnerabilities such as parameter manipulation, code injection, legacy C/C++ vulnerability classes, etc, to hack into customers' information which they equally use to defraud their victim [iii].

Security issue is a great concern of the modern electronic banking system. Several measures have been put in place by banks hosting electronic banking to combat the ugly trends, but the total control to electronic banking fraud is yet to be achieved.

In the event of finding lasting solution to electronic banking fraud, [iii] proposed data validation techniques for online banking. [xi], proposed the use of biometrics authentication for electronic banking.

Biometric authentication in combination with other techniques holds the promises of providing authentic security for online banking, but the application of biometric in real time application, especially in a growing database like those of banks is challenged by the weight and graphic nature of biometrics, hence, it requires a larger storage capability, and a very high, speed CPU [xiii].

In addition to the security system in placed or proposed, [ii] is of the view that, a model that will unveil fraudster anonymity, and a special court dedicated for quick prosecution of fraudsters, should be put in place to serve as a deterrent to prospective fraudsters. Also, there is the need for users' awareness of security threats, and practices vulnerable to electronic banking security.

It is the expectation of the researchers that if these security measures are put in place for electronic banking, then the issues of electronic banking fraud would have been a history.

4. References

i. Action Fraud/National Fraud & Cyber Crime Reporting Center (2013). Tips for safe and secure online banking Accessed from http://www.actionfraud.policies.uk.tips-for-safe-andsecure-online-banking-jun13 on 16/09/2017

ii. Agana, M. A., (2016). A model of Cyber Crime Detection and Control System. A PhD Thesis Presented to Department of Computer Science, Faculty of Physical Sciences, Ebonyi State University, Abakaliki.

iii. Aljawarneh, S, Al-Rousan, T., Maatuk, A., M., and Akour, M. (2014) Usage of Data Validation Techniques in Online Banking: A Perspective and case study security Journal, 27(1), 27-38

iv. Carther, S. (2017). Understanding the Time Value of Money. Accessed from http://www.investopedia.com/articles/03/082703.asp on 22/09/2017

v. Credit Europe Bank N. V. Corporate, (2015). Fetched from http://www.crediteuropebank.com/the-bank-online-banking-security-measures.html on 16/09/2017

vi. County, D. (2017), 10 Essential Security Measures to Keep Online Banking Safe in 2017. Dane County Credit Union Mobile App.

vii. Gosafe Online, (2017). Online Banking-How to Stay Secure. Accessed from http://www.csa.gov.sg/gosafeonline/go-safe-for-me/home.internetusers/online e-banking-how-to-stay-secure, on the 16/09/2017

viii. HDFC Bank. Security Measures Provided by HDFC Bank. Fetched from https://www.hdfcbank.com/security/security.measures on 16/09/2017

ix. Izhar, A., Khan, A., Khiyal, M., S., H., Javed, W., and Baig, S. (2011). Designing and Implementation of Electronic Gateway for Developing Countries. Journal of Theoretical and Applied Information Technology, 26(2), 84-90

x. Khusial, H., and McKegney, K., (2005). E-Commerce Security: Attacks and Preventive Strategies. Fetched from http://www.ibm.com/developerswork/websphere/library/teacherticles/0504-mckegney.html on 16/09/2017

xi. Kuselev, T., Lami, I., Jassim, S. A., and Sellahewa, H., (2010). eBiometrics: An Enhanced Multi-Biometrics Authentication Technique for Real-Time Remote Application on Mobile Devices. Mobile Multimedia/Image Processing, Security and Application. SPIE7708

xii. Omeriba, Z. B., Masese, N. B. and Wanyembi, a., (2012). Security and Privacy of Electronic Banking. IJCSI International Journal of Computer Science Issues, 9(3), 432-446.

xiii. Onu, F. U. Eneji, S. E. and Anighogu, G., (2016). The Effect of Object Oriented Programming on the Implementation of Biometrics Security Systems for Electronic Banking Transactions. International Journal of Science and Research (IJSR), 5(2), 953-941

xiv. Moccean, L. (2002). Internet Data Validation. Journal of Economy Informatics, 1(1), 96-99.

xv. Peotta, L., Holtz, M. D., David, B. M., Deus, F. G., and Sousa, R., T., (2011). A Formal Classification of Internet Banking Attacks and Vulnerabilities. International Journal of Computer Science & Information Technology (IJCSIT), 3(1), 186-197.

xvi. Sennholz, H. F., (1969). The Value of Money. Fee Foundation for Economic Education. Accessed from https://fee.org/articles/the-value-of-money on 22/09/2017.

xvii. Vassiki, A., Demetis, D. S., and Varvarigou, T. (2017). Biometric Implementations and the Implications for Security and Privacy. International Journal of Computer Science & Information Technology (IJCSIT), 3(1), 186-197.

xviii. Wùeest, C. (2005). Threats to online Banking. Dublin, Virus Bulletin, Ltd.