International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 3, Issue 2, pp 6-21, February-2019

Online Security Framework for e-Banking Services: A Review

[1]Dr. Oye, N. D., [2]Sarjiyus, O.

[1]Department of Computer Science, MAUTECH, Yola, Nigeria
[2]Department of Computer Science, ADSU, Mubi, Nigeria

Abstract - **The emergence of Internet banking has allowed banks to offer their customers relatively convenient and flexible banking, also known as e-banking. These services now come in a wide range, including but not limited to conducting fund transfers, managing and checking account, and bill payments. Despite benefits that banks are offering to their customers through online services, e-banking has also raised many security issues. Computer hackers have developed a variety of elusive methods for stealing Internet bankers' money. Although there are many advantages of online banking, security issues often discourage customers from using it, as many customers have found that the use of online banking could leave their financial assets at risk. The primary services that customers use via the Internet are transferring money across accounts, paying bills, checking account balances, and sending and receiving confidential information between banks and fellow customers. The rise in cyber-attacks has caused a decline in the use of online banking and has negatively affected consumer confidence in the ability of financial institutions to protect them. Consumers are questioning the safety of their money and information and are looking up to banks to fix the problem. Therefore this paper reviewed online security framework for e-Banking services.**

Keywords: Banking Services; E-Banking; Internet Banking; Online Banking; Security Framework.

I. INTRODUCTION

The Internet has been around for decades. Many people have been using the Internet to facilitate their lives and expedite their daily tasks (Razak, 2016). Of all the aspects of daily life that have benefitted from the Internet, the banking sector has been especially effective at capitalizing on Internet's features. It has introduced through the Internet many attractive ways to increase the scope of its financial services. The emergence of Internet banking has allowed banks to offer their customers relatively convenient and flexible banking, also known as e-banking. This term does not yet have a precise definition, as many researchers have defined e-banking differently. In general, e-banking refers to bank customers using the Internet to perform financial services such as financial transactions (Jolly, 2016). These services now come in a wide range, including but not limited to conducting fund transfers, managing a checking account, and bill payments. Additionally, e-banking enables customers to access their bank accounts through banks' websites without the need of travelling to the bank (Safeena, 2010). Internet banking has benefited both banks and customers. The banks are benefited because the Internet has allowed banks to diminish their operational costs in terms of decreasing physical facilities involving human resources, paperwork, and supporting staff. The customers are benefiting because e-banking has given them fast access to various financial activities, such as money transfer, payment for utility bills, checking account management (Sharma , 2016). As cited by Safeena (2010), bank customers can use banking in three overarching ways. The first use is to obtain simple information about services provided by the bank through its website, such as products and policies (Razak, 2016). The second and third uses are simple and advanced transactions, respectively. Transactional websites are types of Internet banking that enable customers to conduct simple transactions, such as account inquiry. The Simple transactions do not allow users to transfer funds. An advanced transactional website allows customers to transfer funds and access other online financial services and conduct other types of transactions. Many countries have integrated the use of the Internet into their traditional banking system. Since the introduction of the Internet, some of the banks around the world are offering Internet services, for instance, Bank of America, Centura Bank, Citibank, NationsBank, etc., (Vaciago and Ramalho,2016). These banks offer their customers convenience and flexibility of use, thus contributing to the growth of the bank and popularity of e-banking.

Despite benefits that banks are offering to their customers through online services, e-banking has also raised many security issues (Razak, 2016). Computer hackers have developed a variety of elusive methods for stealing Internet bankers' money. Although there are many advantages of online banking, security issues often discourage customers from using it, as many customers have found that the use of online banking could leave their financial assets at risk(Balk, Yap, Loh, and Wong 2009; Leukfeldt, Kleemans, and Stol, 2016). Since most banks are now offering services to their customers through the Internet, an increasing number of hackers have found it worthwhile and appealing to dedicate their time to conduct frauds through online banking system. It has been observed in many research studies that security issues, such as “phishing attacks,” have been used by hackers to breach e-banking customers’ accounts (Chiu, Chiu and Mansumitrchai, 2016; Arachchilage, Love and Beznosov, 2016).

Banks will put their customers at risk and eventually drive them away if they do not strengthen the security of their e-banking. The primary services that customers use via the Internet are transferring money across accounts, paying bills, checking account balances, and sending and receiving confidential information between banks and fellow customers (Sharma, 2016).

According to Alsayed and Bilgram (2017), financial institutions should pay particular attention to protecting the information of their own organization, their users, and their finances, which are all forms of sensitive information of which hackers can take advantage. In terms of phishing, banks must protect their users’ confidential data from unauthorized individuals or groups who could inquire after users’ bank accounts to conduct fraudulent activities such as stealing customers’ private information, data and ultimately the money. Unfortunately, the current lack of security protection amongst most online banking is conducive to phishing attacks.

Essentially, online banking transactions involving sensitive customer data are carried out via public network and this introduces challenges for security and trustworthiness. Hackers can take advantage of any security lapse on a public network and launch attacks. Hackers are becoming increasingly active and proficient in carrying out major attacks like spoofing, phishing, pharming and keystroke capturing (Devadiga, Jain, Kothari and Sankhe, 2017). Any online banking system must solve the issues of authentication, which means it must ensure that only qualified persons can access an online banking account; Confidentiality, which means that the information viewed remains private; Integrity, which means the information cannot be modified by third unauthorized parties; None repudiation, which means that any transactions made are traceable and verifiable. All banking authentication methods can be classified according to their resistance to major forms of attack such as offline credential stealing attacks, online channel breaking attacks and content manipulation (Man-in-the browser).This research review focuses on designing an online security framework that solves the issues of authenticity, confidentiality, integrity and non-repudiation.

II. STATEMENT OF THE PROBLEM

Online banking is a highly profitable channel for financial institutions. It accords customers the convenience and flexibility to complete money transfers, pay bills, and access critical information online. However, it is now facing major challenges due to the risks of Phishing, Pharming, dns other forms of attack resulting from the activities of Internet criminals and fraudsters attempting to steal customer information. The rise in cyber-attacks has caused a decline in the use of online banking and has negatively affected consumer confidence in the ability of financial institutions to protect them. Consumers are questioning the safety of their money and information and are looking up to banks to fix the problem. Therefore, this study will engage in designing an online security framework that would increase online banking transaction safety and raise customer confidence.

III. SIGNIFICANCE OF THE STUDY

The need for stronger Online Security System in an Internet Banking Environment has become necessary to ensure customer security, confidence and acceptance of this widely used channel for financial institutions.

For instance, the standard means of user authentication, such as username and password are no longer strong enough to ensure appropriate access control to customers’ account and personal information; Hence, the need for financial institutions to be able to strengthen user authentication and address other Security Challenges in an online environment to protect customers and maintain confidence. Thus, the study is significant in the following ways;

i. To provide guidance for industry professionals to utilize when planning and implementing stronger authentication for financial institutions.

ii. To enable banks to critically assess their services, their competitor services, determine the extent of matching key factors in Internet customer expectations, and identify areas and means for possible improvements.

iii. The study is also significant in assessing the security of online banking application which requires specialized knowledge on vulnerabilities, attacks and countermeasures, to gain an understanding of the threats, how they are realized and how to address them. In view of the above, the use of attack trees should facilitate the work of auditors, security consultants or security officers who wish to conduct a security assessment of an online banking authentication mechanism.

IV. OPERATIONAL DEFINITION OF TERMS

Building online security: This is the process of developing and strengthening the existing Secured Socked Layer (SSL) with two other tunnels, namely, Application Layer Security (ALS) and Internet Protocol Security (IP sec) to make online transactions secure.

1. Firewalls: Firewalls are computers which monitor data traffic between local networks or a single computer and other networks, such as the Internet the firewall's function is to protect the local network or computer from unauthorized access. A personal firewall is a program fulfilling the function of a firewall on your PC, meaning that it protects you from unwanted access without the need for an additional computer.

2. Java Applet: A Java applet is a small program that is interpreted and executed in a browser after being downloaded from the Internet. The Java commands are integrated into HTML pages and executed when these pages are loaded.

3. Patch: Small program developed to solve security problems detected in an existing program version as quickly as possible.

4. Pharming: Pharming or DNS spoofing is an attack in which the pharmer substitutes a false IP address for that of a well-known domain name. The URL looks legitimate although the user is on a spoof website.

5. Phishing: Phishing attacks use e-mail addresses or web pages pretending to be from familiar sources such as Internet service providers, retailers or banks with the aim of inducing customers to divulge their account details, PINS and passwords on a fake website.

6. PIN: Personal identification number, a confidential access code.

7. Rootkit: A rootkit is a software tool which subverts the core functionality of the operating system with the aim of concealing activities such as stealing confidential access codes or copying files. The rootkit enables the hacker to operate with administrator rights.

8. Spyware: Spyware is the name given to a hidden software program which sends user information to a third party without the user's knowledge, or approval. This information may include data stored on the PC, one's surfing habits or personal information such as confidential access codes for online transactions.

9. TAN: Transaction number; a one-time password used to authorize a transaction.

10. Trojan horses: Trojan horses are program that, unknown to the user, carry out operations compromising the security of a PC. The objective of most trojans is to capture sensitive information such as passwords and send them by e-mail or via the Internet to the trojan's owner the backdoor trojans give hackers remote access to computers, which they can then control.

11. Virus: Computer viruses are programs that replicate themselves and spread over the Internet by e-mail, for example. Viruses can sometimes inflict considerable damage on infected PCs.

12. Worms: Worms are self-replicating programs that spread from computer to computer across a network. The aim of a worm is to infect as many computers as possible within a network and inflict damage.

V. CONCEPTUAL FRAMEWORK

Online Banking System is a service for customers to do financial transactions. Online banking implements software that allows customers to access information regardless of where the customer is located. A unique aspect of online banking software is that it is able to track different transactions (deposits, withdrawals, transfers, etc.) and when these transactions take place. By creating an online banking system, customers have unique access to utilize all of the unique features anywhere without having to physically go to the bank. In addition customers are able to receive a comprehensive over view of their financial status and actively engage in various transactions such as transferring of funds.

E-banking (or internet banking) is the term used for new age banking system. E-banking is also called online banking and it is an outgrowth of PC banking. E-banking uses the Internet as the delivery channel by which to conduct banking activity, for example, transferring funds, paying bills, viewing, checking and savings account balances, paying mortgages and purchasing financial instruments and certificates of deposits (Mohammed, Siba and Sreak., 2009). It is difficult to infer whether the Internet tool has been applied for convenience of bankers or for the customers' convenience. But ultimately it contributes in increasing the efficiency of the banking operation as well providing more convenience to customers. Without even interacting with the bankers, customers transact from one corner of the country to another corner.

Electronic banking has experienced explosive growth and has transformed traditional practices in banking (Gonzalez, 2008). As per prediction of Maholtra and Singh (2007), the e-banking is leading to a paradigm shift in marketing practices resulting in high performance in the banking industry. Delivery of service in banking can be provided efficiently only when the background operations are efficient. An efficient background operation can be conducted only when it is integrated by an electronic system. The components like data, hardware, software, network and people are the essential elements of the system. Banking customers get satisfied with the system when it provides them maximum convenience and comfort while transacting with the ban Internet enabled electronic system facilitate the operation to fetch these result.

In online banking system customer's information is the most crucial element to be secured. The user is the most delicate link in the whole system to be attacked. As the whole system of online banking is provided with the highest security as even a small attack could bring the whole system down which could cost unexpected. In online banking system the bank's server is equipped with the highest security level techniques, so the bank server is less prone to attacks Peotta and Holtz, (2011). But the database of the bank is not kept on single server in the distributed database technique. The database is kept in parts over the network on different computers. So in case of distributed database the security concerns get increased as these are more vulnerable to the attacks. The user is the most delicate and often targeted link. User is the weakest link in the whole system as a layman user could never understand the security threats and attacks.

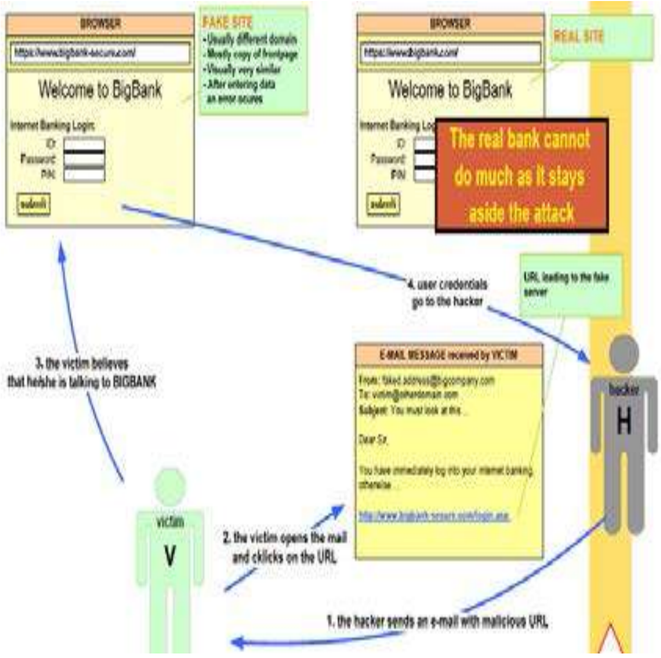

BROWSER
https://www.bigbank-secure.com/
Welcome to BigBank
Internet Banking Login:
ID:
Password:
PIN:
submit
FAKE SITE
-Usually different domain
-Mostly copy of frontpage
-Visually very similar
-After entering data an error occurs
BROWSER
https://www.bigbank.com/
Welcome to BigBank
Internet Banking Login:
ID:
Password:
PIN:
submit
REAL SITE
The real bank cannot do much as it stays aside the attack
4. user credentials go to the hacker
URL leading to the fake server
3. the victim believes that he/she is talking to BIGBANK
E-MAIL MESSAGE received by VICTIM
From: faked.address@bigcompany.com
To: victim@otherdomain.com
Subject: You must look at this...
Dear Sir,
You have immediately log into your internet banking, otherwise...
http://www.bigbank-secure.com/login.asp
hacker
H
victim
V
2. the victim opens the mail and cklicks on the URL
1. the hacker sends an e-mail with malicious URL

Figure 1: Online banking attack (Kuppuswamy, 2011)

Attacks on the bank's server are mostly unsuccessful but the most common attack is Denial of Service attack. This attack refers to such a condition when the resources are not available to its intended users. It is done by flooding the network with requests. It can also simply refer to a resource, such as e-mail or a Web site that is not functioning as usual. The user has the authentication information of his account which is the main target of the hacker. It can be hacked by using Credential theft, Social engineering, phishing, pharming and man in the middle. In credential theft the personal information of the user which is used for authentication of the account is stolen. The success of this kind of attack depends upon the type of authentication used (Kuppuswamy, 2011).The credential theft uses malicious software to steal the information from the users. The malicious software is used to disrupt the normal operations of client's computer and gather sensitive information. These are also known as malware. Malware can be in the form of code, scripts or software.

Social engineering is one of the mostly used methods to intrude the security (Srivastava and Gupta, 2011). In this kind of attack mostly layman users are targeted. It relies heavily on human interaction and tricking other people to break in the security. A person using social engineering to break in the security must try to gain the confidence of the user first. Social engineers rely on general helpfulness of the people also on their weaknesses. Another aspect of social engineering relies on people's inability to keep up with a culture that relies heavily on information technology. Social engineers rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it. Social engineers search dumpsters for valuable information, memorize access codes by looking over someone's shoulder or take advantage of people's natural inclination to choose passwords that are meaningful to them but can be easily guessed as seen in Fig 3. Social engineering requires less technical knowledge but require more tricks (Alyslyed and Balgrami, 2017).

Phishing is a method of gaining access to user name, password, credit card number and other confidential information (Srivastavaet al., 2011). It is carried out by generally sending e-mails containing malwares. The user is lured into a fake website which looks like the original one and is told to login. When user login onto that fake website, the confidential information gets lost. Phishing uses a fake website, actually not whole website but only login page which is similar to the original website. The link to that webpage is provided with the email which is sent to the user. If user login into that fake webpage, the personal information gets hacked. Suppose you check your e-mail one day and find a message from your bank say Big Bank (Srivastavaet al.; Alshehri, Radziszowski and Raj, 2011) You have gotten e-mail from them before, but this one seems suspicious, especially since it threatens to close your account if you don't reply immediately. This message and others like it are examples of phishing, a method of online identity theft. In addition to stealing personal and financial data, phishers can infect computers with viruses.

The difference between fake site and original site is that the domain of the fake site is different and mostly after entering the information an error occurs. Pharming is similar to phishing but an advanced technique.

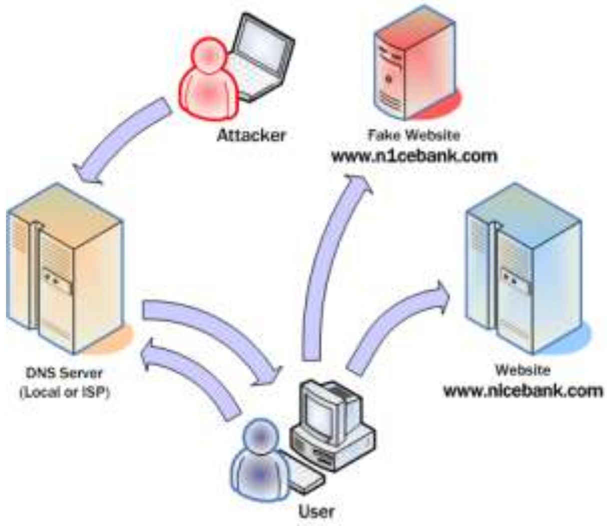
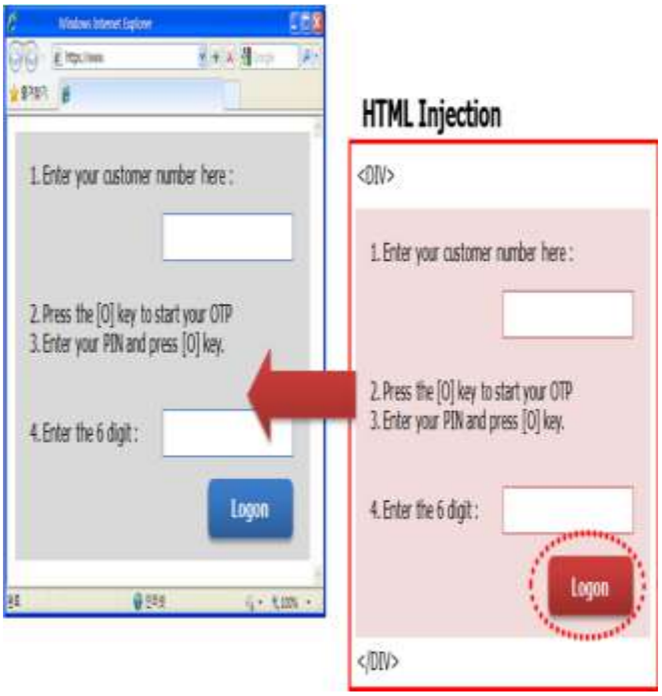


Figure 2: Example of Pharming (Tripathi and Tripathi, 2012)

In pharming DNS reconfiguration is used. For this purpose malicious software like Trojans and viruses are used. The user is lured into a fake website containing malicious code and Trojans. Man in the middle uses Trojan horse to be installed on the client's machine. It could be done by social engineering or phishing. Once the Trojan horse is installed on the client's machine the user when enters the URL of the original website Trojan does not allow to connect via a secured connection, the unsecured connection is followed and the confidential information gets hacked.

Most of the recent hacking tools are circulated throughout the Web, and they are downloaded and executed in the user's PC while the user is simply Web surfing or opening an e-mail. These hacking tools can easily capture the password, account number, and personal data which the user is inputting. They are even capable of replacing the input screen that the user is watching with a counterfeit Website of the bank which the hacker had installed in advance. The user's input data are not transmitted to the bank because these hacking tools redirect the user's input data to the hacker's server instead for illegal account transfers. Thus hackers and hacking tools can attack us using many tricks in a number of different stages during the online banking process as shown in Figure 1.

One of the examples is the Man-in-the-Browser Attacks that redirect the end user to fake sites with the intention of stealing the end user credentials. Most banks offer One-Time Password (OTP) to protect the static password that the end user inputs on the keyboard (Al-Yarimi and Minz, 2012). This is a technology that disables the attack by having the user input a new password generated by the OTP device every time the user logs in so that the hacker cannot use the password captured by using the key logging hacking tool. With the hacking tool that has been installed in the user's PC in advance, the hacker can show a fake online banking web site he made by modifying the user's hosts file, or he can also intercept the user's online banking session and steal user credentials by covering the user's web site through HTML Injection with a counterfeit site to be filled with account information.



1. Enter your customer number here :

2. Press the [O] key to start your OTP

3. Enter your PIN and press [O] key.

4. Enter the 6 digit :

1. Enter your customer number here :

2. Press the [O] key to start your OTP

3. Enter your PIN and press [O] key.

4. Enter the 6 digit :

Figure 3: Fake log-in through HTML Injection (Une and Kanda, 2011; Alsayed & Balgrami 2017)

Most of the attacks directed at online banking systems target the user (the weakest link in the chain), focusing on obtaining authentication and identification information through the use of social engineering and compromising the user's Internet banking access device in order to install malware which automatically performs banking transactions, apart from obtaining authentication data. This fact indicates that secure Internet banking systems should provide security mechanisms as user independent as possible, mitigating the risk of user related information leaks and security issues affecting the system and leading to fraud.

In the face of the current security issues and the growing number of attacks and consequent frauds, new Internet banking systems should be designed as to provide better authentication and identification methods which are less dependent on the user. The basic characteristics of such methods are introduced based on the analysis the methods currently employed. All Internet banking systems with those characteristics will render the presented attacks (and other attacks) ineffective, significantly decreasing the number of observed frauds.

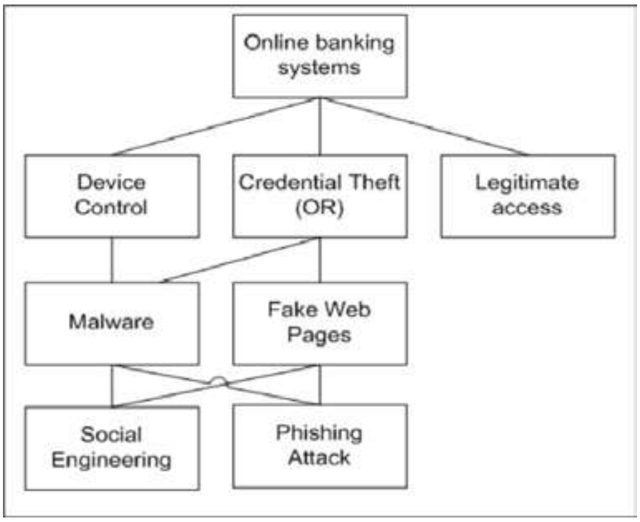


Figure 4: Attack Tree model (Dalton, Mills, Colombi and Raines, 2006)

The attack tree model for common attacks against online banking systems is presented in Figure 4.. This model represents the main components of banking systems authorization and authentication mechanisms and efficient attacks against them. The attacks exploit vulnerabilities inherent in the people (social engineering and phishing) then to gain control of device (malware) and credential theft legitimate user (fake Web pages and malware). The attacks description in this section is based on current trends observed in malware specifically focused on banking. It has been observed that such attacks are efficient against the authorization and authentication schemes currently adopted in online banking systems.

Wada, Olumideand Paul, (2012) Studied that a number of criminological and social theories have been postulated to explain criminal activities and the behavior of conventional criminals. However, empirical research to validate these theories in the context of cyber activities and the application of these theories to cybercrime are still very sparse in literature. With increasing use and migration of products and service such as banking, commerce and other financial services to Internet platforms, research is warranted that examines the application of these theories to addressing the problem of cyber criminality. In this discourse, our attention is directed towards appraising these theories and applying them to provide some explanation for online criminal behavior.

As a result of the Internet, electronic commerce has emerged, allowing businesses to more effectively interact with their customers and other corporations inside and outside their industries. Internet can be seen as a truly global phenomenon that has made time and distance irrelevant to many transactions. One industry that is using this new communication channel to reach its customers is the banking industry. The transformation from traditional banking to e-banking has been a "Leap" change. The electronic banking system addresses several emerging trends: customers' demand for anytime, anywhere service, product time to- market imperatives and increasingly complex back-office integration challenges. But on the other hand the increase in the use of ICT facilities result in increase of criminal activities like spamming, credit card frauds, ATM frauds, Phishing, identity theft, denial of service and most of others has lend credence to the view that ICT is contributing crime in banking sector. The challenges that oppose electronic banking are the concerns of security and privacy of information.

Peotta, Holtz and David (2011), explored that formal classification of attacks and vulnerabilities that affect current Internet banking systems is presented along with two attacks which demonstrate the insecurity of such systems, based on analysis of current security models, we propose a guidelines for designing secure Internet banking systems which are not affected by the presented attacks and vulnerabilities. French, (2012) studied that e-banking security continues to increase in sophistication to protect against threats, the usability of the e-Banking decreases resulting in poor security behaviors by the users. The current research evaluates security risks and measures taken for e-Banking solutions. A case study is presented describing how increased complexity decreases vulnerabilities online but increases vulnerabilities from internal threats and e-Banking users. Adesuyi et al., (2013) explored that the current practices in Nigeria's customer banking services with an empirical investigation into ATM fraud as well as a physical and technical implementation of security. Beranek and Jiri (2013), studied that Currently, Internet portals are an integral part of business activities on the Internet. Anyone can easily participate in online auctions, either as a seller or a buyer (bidder), and the total turnover on Internet auction portals represents billions of dollars. However, the amount of fraud in these Internet auctions is related to their popularity. To prevent discovery, fraudsters exhibit normal trading behaviors and disguise themselves as honest members. It is therefore not easy to detect fraud in online auctions.

VI. SECURITY ISSUES IN ONLINE BANKING

Perceived lack of security is "a perceived potential loss due to fraud or a hacker compromising the security of Internet banking". Lee, (2009). So, Internet banking threats can be accomplished through network attacks or through illegal access to the customer account by means of fabricated or faulty authentication (Yoon and Occena, 2014). For this reason, security and privacy threats are constantly increasing both in quantity and quality (Dmitrienko, Liebchen, Rossow and Sadeghi, 2014).Thus, “online banking security is a primary concern”, as banks supposedly provide all measures necessary to make customers believe that information is transmitted safely and securely (Saleh, 2011). Awareness of security has direct impact on trust and usage of IB and indirectly affects perceived ease of use (Alnsour and Al-Hyari, 2011). In other words security issues have significant effects on IB use Yoon et al., (2014), having negative causal relationship (Lee, 2009; Kim, Mirusmonov and Lee, 2010). To sum up, banks and financial institutions should build and enhance confidence and trust of their Internet services and data transfer, as well as provide privacy and security protection, system reliability and financial quality information. Although there has been dramatic rise in the number of Internet users all round the world, security and trust issues still persist. The background information fundamental to this study, therefore, includes Technology Acceptance Model (TAM), system security experts and trust and their effects on usage.

Although service providers, financial institutions, the media, security organizations, and security expects have continually provided technical information and verbal assurances on dealing with online security threats, consumers are fearful of the intruder getting hold of their accounts and other confidential information and hence security preys heavily on consumers’ minds. The fear is heightened by the nature of recent trends of security breaches and attacks reported by the media which computer security experts have found highly complex and sophisticated to comprehend: e.g. the surfacing of the recent “Zeus v.3 botnet Trojan”, which was reported by the media to have been used by attackers to raid and steal thousands of pounds from UK Internet banking customers (McGuiness, 2010). Cheng et al (2006), infer that delicate information such as personal data and identity, passwords are frequently related with personal property, secrecy and may present security concerns if leaked. Illegal right of entry and usage of private data may result in consequence such as identity stealing, as well as theft of assets. Diverse causes of information security breaches include the following:

1. **Phishing:** Phishing is a kind of scam where the scammers masquerade as a trustworthy source in attempt to gain private data such as PINs, and credit card data, etc. through the Internet. Phishing frequently happens through prompt messaging, email and it fools the user by showing any financial fake site in its actual format. These forged websites are frequently planned to look identical to their genuine counterparts to avoid misgiving from the user.
2. **Internet scams:** Internet scams are patterns that betray the user in several ways in attempt to take benefit of them. This attacks are created to make the fraud with private assets of customer directly rather than personal data through false undertakings, assurance tricks and more.
3. **Malware:** Malware, mainly spyware, is malicious software camouflaged as legitimate software planned to accumulate and transmit private data, such as PINs, without the customer's consent or knowledge. They are often spread through software, e-mail and files from unofficial places. Malware is one of the most prevalent safety apprehensions as frequently it is impossible to decide whether a file is infected, in spite of the source of the file.
4. **Identity theft:** Identity theft is a crime in which a fraudster obtains key pieces of personal data, such as bank information, date of birth or driver's license numbers, in order to impersonate somebody. The personal data exposed is then used criminally to apply for credit, buying goods and services, or gain right of entry to bank accounts.

VII. INVESTMENT OR SHARE SALE (BOILER ROOM) FRAUD

Boiler room fraud is an attack in which illegal or aggressive miss selling of bogus, valueless or vastly expensive stocks are takes place by share fraudster. If the victims mistakenly invest money with this fraudster, he will surely lose his all money invested.

1. **Keystroke capturing/logging:** Keystroke capturing or logging attacks are takes place with the help of software or hardware key logger. Anything that user type on system can be captured and stored in a storage. This actually creates a log file of user activities and at a particular instance of a day mail is automatically forwarded to the attacker. This log file contains id and password of different users and attacker can use this for his own purpose. This attack mainly takes place at Internet cafes. An updated antivirus and a good firewall can protect any system from this types of attacks.
2. **Lottery fraud:** In this type of fraud attacker send fake letters or e-mail messages, which recommend the user that She have won a lottery. To take the benefits of this, they are asked to respond email message with some private Banking information of victim, this include his bank account details, complete personal information. Then, after getting

this mail from victim attacker can use this information to commit further fraud.

3. **Pharming:** In Pharming attack fraudster create false website, so that people will visit them by mistake. This attack takes place when user mistype a website or a fraudster can redirect traffic from genuine website to a fake one. The main purpose of pharmer is to obtain victims personal information for further frauds.
4. **Spyware:** Spyware can enter in any system as hidden components of free programs. They can monitor web usage, keystroke logging and virtual snooping on user’s computer activity.
5. **Trojan horse/Trojan:** Trojan horse are the most dangerous type of attack in which attacker can directly gain unauthorized access to victims systems. This virus enters in victim system with the help of different legitimate software. An updated antivirus and firewall can protect any user from this kind of attacks.
6. **Virus:** Virus is a computer program that designed to replicate itself from one computer to another. It can slow down user system or corrupt its memory and files. Email and file-sharing facilities are the main reason for spreading viruses.
7. **Worm:** This is malicious programs that replicates or reproduce itself until all the storage space on a computer drive will be filled. It uses system time, speed, and space when duplicating. It can also interrupt Internet usage.
8. **Social Engineering:** One of the most common attacks does not involve knowledge of any type of computer system. Tricking consumer s into revealing sensitive information by posing as a system administrator or customer service representative is known as social engineering. Social engineers use surveillance and a consumer’s limited knowledge of computer systems to their advantage by collecting information that would allow them to access private accounts.
9. **Port Scanners:** Attackers can use port scanners to ascertain entry points into a system and use various techniques to steal information. This type of software sends signals to a machine or router and records the message the machine responds with to ascertain information and entry points. The main purpose of a port scanner is to gather information related to hardware and software that a system is running so that a plan of attack can be developed.
10. **Packet Sniffers:** The connection between a user’s computer and the web server can be “sniffed” to gather an abundance of data concerning a user including credit card information and passwords. A packet sniffer is used to gather data that is passed through a network. It is very difficult to detect packet sniffers because their function is to capture network traffic as they do not manipulate the data stream. The use of a Secure Socket Layer connection is the best way to ensure that attackers utilizing packet sniffers cannot steal sensitive data.
11. **Password Cracking:** Password cracking can involve different types of vulnerabilities and decrypting techniques; however, the most popular form of password cracking is a brute force attempt. Brute force password attacks are used to crack an individual’s username 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. Brute force cracking takes advantage of systems that do not require strong passwords, thus users will often use common names and activities making it simple for a password cracker to gain access to a system. Other password cracking methods include using hash tables to decrypt password files that may divulge an entire systems user name and password list.
12. **Denial of Service Attacks:** Denial of service attacks are used to overload a server and render it useless. The server is asked repeatedly to perform tasks that require it to use a large amount of resources until it can no longer function properly. The attacker will install virus or Trojan software onto an abundance of user PC’s and instruct them to perform the attack on a specific server. Denial of service attacks can be used by competitors to interrupt the service of another E-Commerce retailer or by attackers who want to bring down a web server for the purpose of disabling some type of security feature. Once the server is down, they may have access to other functions of a server, such as the database or a user’s system. This allows the attacker the means to install software or disable other security features.
13. **Server Bugs:** Server bugs are often found and patched in a timely fashion that does not allow an attacker to utilize the threat against an E-Commerce web site. However, system administrators are often slow to implement the newest updates, thus allowing an attacker sufficient time to generate a threat. With the millions of web servers in use around the world, thousands often go without timely patches, leaving them vulnerable to an onslaught of server bugs and threats.
14. **Super User Exploits:** Super user exploits allow attackers to gain control of a system as if they were

an administrator. They often use scripts to manipulate a database or a buffer overflow attack that cripples a system, much like a Denial of Service attack for the purpose of gaining control of the system. Users can create scripts that manipulate a browser into funneling information from sources, such as databases.

VIII. SECURITY OF CUSTOMER INFORMATION SENT FROM PC OR MOBILE DEVICE TO WEB SERVER

This includes the availability of secured website information of bank, namely IB section should be always be 128-bit and above secure socket layer (SSL) encrypted in order to remove man-in-the-middle external threats. However, such method is not proven to be completely secure as man-in the-middle attack by hackers may lead to personal information and credentials leak or people can use insecure ways of storing their login credentials on a piece of paper after forgetting passwords, login IDs, secret question – answers (Amtul, 2011; French, 2012). For this reason, if hackers use key logger software to gather information, website should include option of virtual input of data with the help of virtual keyboard. Study of two factor authentications (2FA) of UK banks has also found that some websites do not hide passwords or pass-phrases (Krol, Cristofaro and Sasse, 2014). In addition, from the personal experience of internet banking in South Korea, most of internet banking of Korean banks initially use additional software like anti-virus, anti-key logger, anti-screen capture, antimalware installed obligatory before entering is made into internet banking section. After first installation, the next time you log in, these programs automatically run in the background to secure connection and transfer of any data from user PC to bank web server. This method of installing additional software seem to have proven itself with time, as study of security of IB and financial private information in South Korea indicates that there were few cases of customer hacking fraud was reported (Lee, Lim and Lim, 2013).

IX. SECURITY OF WEB SERVER ENVIRONMENT AND CUSTOMER INFORMATION DATABASE

Real world instances have shown that even banks and financial institutions pay great attention and invest heavily in security issues, all information systems have weaknesses that create opportunities for possible threats to the information housed in these systems (French, 2012). As a result, Lee et al., (2013), suggest using central government regulated encrypted repository of all customer private information with the help of e-pin . This means that after first registration in any bank, customer information is sent to the central repository and after authenticating user a unique password-protected e-pin number is issued. Next registration in bank will not require user to enter personal data again, but to enter the unique e-pin and the data will be retrieved by bank automatically and verified. This method will effectively eliminate perceived information system weaknesses and reduce possibility of external attacks. (Musaev and Yousoof, 2015).

X. SECURITY MEASURES TO PREVENT UNAUTHORIZED ACCESS TO INTERNET BANKING SESSION (IB)

Two-factor authentication (2FA) has proven to be secure method customer verification requiring them to produce additional authentication (Krolet al.,; Dmitrienko, Liebchen, Rossow, and Sadeghi, 2014). Together with their unique login ID and password like one time pass code (OTP) issued by OTP token or received by SMS to mobile device, phone call, card reader or a card with random numbers. Nonetheless, increased security could have negative effect on the IB system use French, (2012), such are too many specific information, predefined security questions and answers that needed to be remembered by customers to verify their entry into IB section lead to decreased perceived usability. Moreover, 2FA schemes have conceptual vulnerabilities and not completely secure because OTPs can be intercepted (Dmitrienko et al., 2014).Among other security measures are: session timeouts or auto-terminal/account logoff, automatic lockouts after a number of unsuccessful login tries, use of strong passwords (French, 2012).

XI. PHISHING ATTACKS ON ONLINE BANKING

The phishing attack has become one of the most common financial crimes in recent years. Phising is defined as "a criminal activity using social engineering techniques that enables phishers to attempt fraudulently acquire sensitive information, such as passwords, credit card details, national identicard information etc., by masquerading as a trustworthy person or business in an electronic communication. Phishers can even breach the security of a bank after they access user's financial information; then, they conduct a wide range of illegal activities. Online banking users are more vulnerable to e-banking frauds, when they conduct any financial activity through the web, such as money transfer. Phishing attackers can breach the security of bank websites by using sophisticated technologies such as the Man-in-the-Middle Attack. The attackers' goal is to get access to bank users' data Junger. They then use this financial data to harvest money or conduct financial frauds for their benefits, such as funds transfer and purchasing goods. Thus, e-banking users are at risk of losing their money. Phishing attacks may include deceptive, malware, and DNS-based attacks. In deceptive attacks, hackers send a deceptive message to the bank users. The deceptive message may have some sense of urgency, such as reporting a fake account problem and a fake issue with account activation. The purpose of the deceptive message is to lure the user to interact immediately. (Emigh, 2005; Musaev et al., 2015).

Deceptive phishing is another type of phishing attack that attempts to gain access to financial accounts of users. The most common method of a deceptive phishing attack is sending false notifications through email Damodaram (2016). In this type of phishing attack, an attacker sends email messages to users, masquerading as one of the bank's representatives. In addition, this deceptive email contains a "call action," which means that the phisher is using a sense of urgency in order to attract recipients into clicking on a fraudulent website link included in the email Emigh (2005). If the user clicks on the provided link, the user will be directed to a fraudulent website which looks like a legitimate bank's website. Thus, the user may feel comfortable entering his or her confidential information, such as username and password. Once the user enters that information, phishing attacker collects the confidential information and can then sign into the user's banking account to conduct fraudulent activities Mishra (2016). An example is provided and illustrated in Fig. 1, how bank users could be deceived by a fraudulent website.

As shown in Fig. 1 and 2, emails that appear to be forwarded from PayPal and Citibank (Eze, Yih, Ling and Gan, 2008; Alsayed and Bilgrami, 2017). In these cases, the phishing attacker is using a sense of urgency to get the attention of the costumer by sounding like a report of a serious problem from a trusted source such as PayPal or Citibank. The user then clicks on the link provided in order to enter the requested financial information. The phisher collects the victim's information, because the phisher has full access to the bogus website to which they linked to the user.

1. Malware-based Phishing

Malware-based phishing refers to software programs that hackers install on customers' computers. This kind of phishing attack can happen when customers or bank employees visit an unauthorized website or download some infected software programs into their computers. The Phishing attackers use many techniques, such as keyloggers to gain credential information of bank users (Chaudhry, Chaudhry and Rittenhouse 2016). Keyloggers are programs that install themselves onto bank users' computers when customers visit any websites with a keylogger or download a piece of software with a keylogger (Arora, Sharma and Chauhan 2016). Hackers install these types of malware-based phishing software on users' computers without their knowledge or permission. Therefore, phishing attackers find this type of malicious software easy to use for fraudulent activities, a since the victims are often unaware that such software even exist on their computers. When the bank user with infected computers visits their bank's website and enters their financial information, such as usernames, passwords, and token numbers. The malware logs the keystrokes that the users entered while typing in their confidential information (Vaciago and Ramalho 2016). Thus, the key logger collects the required information and sends it to the attacker as a file. Phishing attackers borrow the keystroke information from the file to log in as the user and conduct financial fraud.

2. DNS-Based Phishing

DNS-based phishing, or more succinctly known as pharming, is another type of phishing attack in which an online deceptive agent gains control of the bank users' data. During the pharming technique, attackers are tampering with the bank's host files or domain name system (DNS) (Arya and Chandrasekaran, 2016). This form of attack redirects users to a fake website when they attempt to type in the domain name of their bank's web address Emigh (2005). The hackers can perform the phraming attack in two ways. They can install a virus on the user's computer or tamper with the bank's web domain. Regardless of the method, the result is that the users type the correct URLs of their financial institutions on their browsers, but then they are directed to fraudulent but legitimate-looking websites. Therefore, users remain unaware that the websites into which they are typing their credentials are under the hackers' control.

3. Security and Privacy

Nowadays uptake of Electronic Commerce (EC) applications in the banking industry is very slow only because of security and data confidentiality issues have been a major barrier. Security and privacy are one of the most challenging problems faced by customers who wish to trade in the e-commerce world. Security in the form of keeping customer safe from an invasion of their privacy, affects trust and satisfaction. If banks wish to maintain customer trust, they need to keep their promises regarding security and privacy. Since security is closely related to trust, violations of security norms may backfire in terms of losing customers and negative word-of mouth.

Ganesan and Vivekanandan (2009) described a secured hybrid architecture model for the Internet banking using Hyperelliptic curve cryptosystem and MD5 is described. Information about financial institutions, their customers, and their transactions are, by necessity, extremely sensitive; thus, doing business via a public network introduces new challenges for security and trustworthiness. Given the open nature of the Internet. Transaction security is likely to emerge as the biggest concern among the e bank's account holders. The rapid growth in account hijacking and online fraud are on the rise. The negative publicity damages consumer trust in the online service.

Since personal and financial information can be intercepted and used for fraudulent purposes, online investing involves greater security concerns than conventional trading; users need a sense of security when conducting financial transactions, and it is still one of the major barriers to e-commerce growth.

XII. ATTACK TAXONOMY

Now that two main attack vectors have being identified - credential stealing and channel breaking - we can build attack taxonomy (as depicted in Fig. 2). The first step is to look more closely at what makes Internet banking authentication methods so vulnerable to attack in the first place. Offline credential-stealing attacks are effective only against schemes in which user credentials are valid for a rather long time period (vulnerable to phishing) and stored or entered on a potentially insecure device, such as the user's PC (vulnerable to malicious software). The most prominent example is static passwords that are set once and used repeatedly afterward. Such security is based simply on the assumption that the password is nontrivial and kept secret, which in turn requires a trusted environment in which to use the password. According to Anderson (2005), malicious software attacks such as a virus or a Trojan horse, once installed on a client PC, can easily log all keyboard input and periodically email any data gathered to a predefined address. Phishing attacks are even easier to set up because they require very limited context information (such as the name of the user's bank). After capturing a static password, an attacker can use the password fraudulently for some time without raising the user's suspicion. A better solution is the use of one-time passwords. The bank sends the user an ordered list of randomly chosen passwords (sometimes called a scratch list), each of which is valid for one authentication only.

According to Anderson (2001), stealing a onetime password does not make much sense because it cannot be reused later, but all unused passwords must be kept secret. Unfortunately, some users store their password lists on their PCs for convenience, effectively breaking the underlying security assumption and exposing the passwords to offline credential-stealing attacks. Malicious software can then steal the list at any point in time, not just during authentication. Phishing is also possible, but it's slightly more difficult if the banking server explicitly specifies which one-time password will be used next. Moreover, the legitimate user might eventually notice the fraudulent use of one or more one-time passwords. To cross the offline-credential-stealing attack boundary depicted in Fig. 2, an authentication method must thwart attacks by both malicious software and phishers. The former requires that credentials are never pre-exposed to a potentially insecure device such as the user's PC, and the latter is rendered infeasible by limiting the validity of a once-exposed credential to a short time period, effectively generating short-lived credentials on demand. Both requirements are usually fulfilled via small microprocessor-based hardware tokens with a built-in display and a cryptographic key unique to the token. According to Anderson (2001), the token then uses this key, together with an additional source of entropy (such as the current time from a synchronized clock on the token or a short-lived random challenge from the bank's server entered via a keypad on the token), to generate short-time passwords that are valid for, say, 60 seconds. Because these tokens are standalone devices neither directly nor indirectly exposed to the Internet, the user must manually copy the password from the display and enter it in his or her PC. Challenge-response tokens are considered to be slightly more secure than timer-based ones because the additional source of entropy-the challenge-is short-lived, nondeterministic, and (ideally) bound to a previously communicated account number.

Authentication based on a hardware-token Public-key Infrastructure (PKI) also avoids the risk of offline credential-stealing attacks against insufficiently secured PCs. Specifically, these schemes effectively cross the online-channel- breaking-attack boundary independently of user behavior via a SSL/TLS channel-parameter- dependent challenge. PKI uses asymmetric cryptographic algorithms such as Rivest Shamir Adlemann (RSA) or Elliptic Curve Cryptography (ECC) (Lashenget al., 2009). Initially, the bank fits each user with a pair of matching private and public keys for which some trusted authority issues a matching digital certificate. The certificate attests that the username is associated with the given public key and that the user holds the corresponding private key. The private key and certificate then establish a mutually authenticated SSL/TLS channel between the user's PC and the bank's server, effectively eliminating online channel- breaking attacks. The only critical issue is the protection of the user's private key against malicious software. If the key is stored in a so-called soft token (a password-encrypted file on the user's PC), the password and, consequently, the private key are vulnerable to offline credential-stealing attacks. The private key thus must be stored on a tamper- resistant hardware token such as a microprocessor-based smart card, potentially exposing only private-key-related functionality (Anderson, 2001).

XIII. EXISTING ONLINE BANKING SECURITY MODELS

Internet-based (electronic) banking schemes rely on the existence of an Internet connection over which a customer can access bank services. Customers can use existing “browser” software such as Mozilla Firefox or Microsoft’s Internet Explorer as the client interface to the bank system. In this model, the bank’s server provides HTML forms-based interface through which customers can make requests and conduct transactions. Communication security is provided by the SSL protocol which is built into the browser, or else, Customers can download Java applets from the bank-server’s web site. (Lasheng et al., 2009; Sarjiyus et al., 2018).The downloaded applet provides the interface through which customer transactions can take place. In this case, communication security is provided by the applet in addition to the security provided by SSL. Any Internet banking system must solve the issues of authentication, confidentiality integrity and non-repudiation; to ensure that only qualified people can access Internet banking accounts, that the information viewed remains private and cannot be modified by third unauthorized parties, and that any transactions made are traceable and verifiable.

For confidentiality and integrity, SSL/TLS is the de facto Internet banking standard, whereas for authentication and non-repudiation, no single scheme has become predominant yet . For that reason, the diversity of Internet banking models which exist today (using SSL as the trusted tunnel) depends on authentication methods available, and security level of a model depends on authentication mechanism used to counter attacks. The secure sockets Layer (SSL) is a commonly used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet’s Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by Netscape, SSL is also supported by Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security. The “Sockets” part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network. SSL uses the public-and –private key encryption system from RSA, which also includes the use of a digital certificate (Viega, 2002). Most programming languages provides APIs that give programmers access to SSL functionality. Java Secured Sockets Extension (JSSE) provides support for SSL and TLS protocols by making them programmatically available. Basically, SSL encrypts the data transmitted between the client and server ensuring confidentiality of the username, password and other client’s credential. Another important aspect of the SSL protocol is authentication. This means that during an initial attempt to communicate with a web server over a secure connection that server will present the web browsers with a set of credentials in the form of a “certificate” as a proof that site is who and what it claims to be.

XIV. WEAKNESSES OF SECURITY MODELS BASED ON SSL/TLS PROTOCOL

SSL/TLS protocol being used as the dc-facto Internet security standard; provides authentication, confidentiality, integrity and non-repudiation of messages transmitted over Internet between the web browser and the web server only (Anderson, 2001).However, this protocol operates below the Application layer in TCP/IP networks and does not provide way to ensure whether a user is, in fact, who he or she claims to be by asking for direct or indirect proof of the knowledge about some sort of secrecy or credential. It is a common mistake for some users to believe that their online banking sessions are perfectly safe when they use an SSL connection. Security experts continually state that everything is safe if there is a yellow padlock symbol in the browser window or the URL start with “https” rather than “http” (Thawte, 2009). The following facts explain why SSL does not guarantee the safety and security of transaction over the Internet:

i. SSL is designed as a secure tunnel from the end user computer’s browser to the server’s web server of the bank, does not protect the end points such as user’s computer. A Trojan exploits this security hole. In addition to that, SSL is beyond providing end-user authentication services (Wueest, 2006; Martino & Perramon, 2008).

ii. The security offered by SSL is based on the use of digital certificates of financial entities’ web servers for which many Internet users are not able to discern the validity of a certificate, and may not even pay attention to it (Martino & Perramon, 2008).

iii. Different browsers versions will offer different levels of security as some are restricted to the use of strong cryptography. For example, some older versions of Netscape and Internet Explorer will even be restricted to offering only weak encryption, unless they are connecting to servers using Server-Gated Cryptography enabled SSL certificate. So, depending on the browser’s vender and version some will only be capable of encrypting at 40 or 56-bit encryption, while more recent browser versions are capable of 128 and even 256-bit encryption key (Thawte, 2009).

iv. Not all Certification Authorities may be validated by all browsers. Some are recognized by a number of browsers, and there are even increasing number of fake CAs which may be recognized by some browsers (Thawte, 2009). These limit the service portability as some banks are enforcing security by restricting customers to use a particular browser (for instance: Bank of China restrict customers to use Internet Explorer, which implies that the customers wanting Internet banking services are requested to use only Microsoft operating systems).The above mentioned facts prove that SSL is not enough to provide trust and security required for Internet banking. Therefore, it is imperative to add other security protocols below and above it in order to provide a trusted environment for customers and banks to process their transactions safely.

XV. BUILDING AN IMPROVED SECURITY FRAMEWORK FOR ONLINE BANKING

Trust and security are key enablers of the Information Society; specifically, they are the first and foremost requirements need to be addressed by Internet banking systems. For customers to use and feel comfortable with Internet Banking services they must have confidence that their online services are trustworthy and secure.

Similarly, for Banks to provide Internet banking services they need confidence in the security of online transactions. Trust and security are very closely connected. Trust depends on the actual architecture of the security management system, but the bottom line to gain users' trust, the security management system must ensure users that the system is secured and well-protected (Sanayei & Noroozi, 2009). In traditional banking trust and security are built-up by many reasons; but, the most important being: First, every bank must be authorized and certified by the controlling government to issue banking services; and then, customers are also certified by the government; banks process services which they offer in a secure environment (which is a secure office); next, customers requesting services need to authenticate themselves to the bank, similarly, banks are authenticated customers before starting their transactions; finally, each party verifies, validates and signs transaction documents, and keeps copy of the signed document. "Authentication + Encryption + Certification Authority = Trust" (Thawte, 2009).

Authentication, Encryption, and Certification Authority are well known security mechanisms for processing Internet-based services for a very long time, and they are currently in use by the existing Internet banking models. However, they are not able to provide the required level of trust and security (for online banking) depending on the way they are used. In this research explanation on how to adapt the traditional banking approach to increase the level of trust and security (over the existing one-tier SSL-based security model) using three-tier model for Internet banking.

XVI. CONCLUSION

The existing environment (SSL trusted tunnel) has proved to have some weaknesses, and the level of security depends on the authentication mechanism used (Lasheng et al., 2009).Therefore, we need, first, to examine why high security provided by SSL is being weakened, and then try to build a secure environment by taking into account those weaknesses. A Trojan exploits this fact. For instance: a Trojan which drops a Dynamic Link Library (DLL) and registers its Class ID (CLSID) as a browser helper object in the registry, is able to intercept any information that is entered into a web page before it is encrypted by SSL and sent out. (This is an example of a credential stealing attack). Another example: a Trojan running on an infected computer can alter the local host's file to redirect any request to an IP address controlled by the attacker. The Trojan can also install a self-signed root certificate on the infected computer (using free tools like Open SSL to create these certificates), this enables attacker to generate official-looking SSL connections from the infected computer to the malicious web server hosting the spoofed Internet banking application. Once the user has been trapped on such a spoofed (fake) Internet banking application, the attacker can act as man-in- the-middle and relay any challenge-response protocol that might be implemented by the original Internet banking application system. This in an example of a channel-breaking attack using malicious software (a Trojan). Thus, SSL by itself is neither able to pass the offline-credential stealing attacks boundary nor able to cross the channel-breaking boundary.

REFERENCES

[1] Abdulwahed, M. S. K., &Yaquob, S. Y. A. (2006). Factors influencing the adoption of Internet banking in oman, A Descriptive Case Study Analysis, *International Journal of Financial Services Management*, 1 (2/3), 155 – 172.

[2] Adesuyi, F., Adepoju, S., & David, R. (2013), A Survey of ATM Security Implementation within the

Nigerian Banking Environment, *Journal of Internet Banking and Commerce*, 18(1), 01-16.

[3] Alnsour, M.S., & Al-Hyari, K. (2011), "Internet banking and Jordanian corporate customers: Issues of security and trust", *Journal of Internet Banking and Commerce*, 16(1), 1.

[4] Alsayed, A. O. &Balgrami, A. (2017), E-banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities, *International Journal of Emerging Technology and Advanced Engineering*, 1(7), 109-112.

[5] Alshehri, S., Radziszowski, S., & Raj, R. K. (2011), "Designing a Secure Cloud-Based EHR System using Ciphertext-Policy Attribute-Based Encryption, *ACM Digital Library, IJCS.*

[6] Amtul, F. (2011), "E-Banking security issues - is there a solution in biometrics?", *Journal of Internet Banking and Commerce*, 16(2), 1.

[7] Anderson, R. J. &Schneier, B. (2005), Economics of information security, *IEEE Security and Privacy*, 3(1), 12-13.

[8] Anderson, R. J. (2001), Security Engineering: A Guide to Building Dependable Distributed Systems. (2nd Ed), *Wiley: New York*.

[9] Arachchilage NAG, Love, S., Beznosov, K., (2016), Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, 60, 185-197.

[10] Arora, M., Sharma, K. K., & Chauhan, S. (2016), Cyber Crime Combating Using Key Log Detector tool.

[11] Arya, B., & Chandrasekaran, K. (2016), A client-side anti-pharming (CSAP) approach. *In Circuit, Power and Computing Technologies (ICCPCT), 2016 International Conference on IEEE*, 1-6.

[12] Beranek, L. Jiri, K.(2013), The Use of Contextual Information to Detection of Fraud on Online Auctions, *Journal of Internet Banking and Commerce*, 18(3), 1-17.

[13] Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016), Phishing Attacks and Defenses, *International Journal of Security and Its Applications*, 10, 247-256.

[14] Cheng, T. C. E., Lam, D. Y. C., & Yeung, A. C. L. (2006), Adoption of Internet banking: An empirical study in Hong Kong, *Journal of Decision Support Systems*. 42(3), 1558-1572.

[15] Chiu, C.L., Chiu, J.L., & Mansumitrchai, S. (2016), Privacy, security, infrastructure and cost issues in internet banking in the Philippines: initial trust formation, *International Journal of Financial Services Management*, 8, 240-271.

[16] Dalton, G., Mills, R., Colombi, J., & Raines, R. (2006), "Analyzing Attack Trees using Generalized Stochastic Petri Nets," 2006 *IEEE Information Assurance Workshop*, 2006, 116-123.

[17] Damodaram, R. (2016), Study on phishing attacks and antiphishing tools, *International Research Journal of Engineering and Technology*, 3.

[18] Devadiga, D., Jain H., Kothari, H., &Sankhe, S. (2017), E-Banking Security Using Cryptography, Steganography and Data Mining, *International Journal of Computer Applications*, 164(9), 26-28.

[19] Dmitrienko, A., Liebchen, C., Rossow, C., &Sadeghi, A.-R. (2014), "Security analysis of mobile two-factor authentication schemes", *Intel® Technology Journal*, 18(24), 138-161.

[20] Emigh, A. (2005), Online identity theft: phishing technology, chokepoints and counter measures, *ITTC Report on Online Identity Theft Technology and Counter measures*, 1-58.

[21] Eze, C. U., Yih, C.G., Ling, N. T., Gan, G. G. G. (2008), Phishing: a growing challenge for Internet banking providers in Malaysia, *Communications of the IBIMA*, 5, 133-142.

[22] French, A. (2012), "A case study on E-Banking security – When security becomes too sophisticated for the user to access their information", *Journal of Internet Banking and Commerce*, 17(2), 1-14.

[23] Gonzalez, M. E. (2008), An alternative approach in service Quality: An e-banking case study, *Quality Management*, 15, 41-48.

[24] Gupta, P. K. (2008), Internet banking in India: Consumer concern and bank strategies, *Global Journal of Business Research*, 2(1), 43-51.

[25] Jolly, V. (2016), The Influence of Internet Banking on the Efficiency and Cost Savings for Banks' Customers, *International Journal of Social Sciences and Management*, 3, 163-170.

[26] Kasemsan, M. L., & Hunngam, N. (2011), Internet banking security guideline model for banking in Thailand. *Communications of the IBIMA*, 23(6), 1-13.

[27] Kim, C., Mirusmonov. M., & Lee, I. (2010), "An empirical examination of factors influencing the intention to use mobile payment", *Computers in Human Behavior*, 26(3), 310-322.

[28] Krol, K., Cristofaro, E. D., &Sasse, A.(2014), "They brought in the horrible key ring thing!" Analyzing the usability of two-factor authentification in UK online banking", *Cornell University Library, arXiv:1501.04434, unpublished*.

[29] Kuppuswamy, P. (2011), "Enrichment of security through cryptographic public key algorithm based on block cipher", *ISSN : 0976-5166*, (2)3.

[30] Lasheng, Y., & Placide, M. (2009), Three-tier security model for e-business, *Proceedings of the Second Symposium International Computer Science and Computational Technology (ISCSCT)*, 114-119.

[31] Lee, J.H., Lim, W.G., & Lim, J. I.(2013), "A study of the security of Internet banking and financial private information in South Korea", *Mathematical and Computer Modeling*, 58(1-2), 117-131.

[32] Lee, M., (2009), "Factors influencing the adoption of Internet banking: An integration of TAM and TPB with perceived risk and perceived benefit", *Electronic Commerce Research and Applications*, 8(3), 130-141.

[33] Leukfeldt, E. R., Kleemans, E. R., &Stol W. P. (2016), Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks, *British Journal of Criminology*, 9.

[34] Maholtra, P., & Singh, B. (2007), Determinants of Internet banking adoption by banks in India, *Journal of Emerald Internet Research*, 17(3), 323-339.

[35] Martino, A. S., & Perramon, X. (2008), Defending e-Banking Services: An Antiphishing Approach Services, *IEEE Congress on Services*, 1, 251-254.

[36] McGuinness, R. (2010), Hackers' cash raid on 3,000 accounts. *Metro*.

[37] Mishra, R. (2016), Review: Phishing Attack Types & Preventive Measures, *Imperial Journal of Interdisciplinary Research*, 2.

[38] Mohammed, S. K., Siba, S. M., &Sreek, U. (2009), Service quality evaluation in Internet banking: An empirical study in India, *International Journal of Indian Culture and Business Management*, 2(1), 27-31.

*[39]*Musaev, E. &Yousoof, M. (2015), A Review on Internet Banking Security and Privacy Issues in Oman. *ICII 7th International Conference on Information Technology*.

[40] Peotta, Holtz, B., & David, D. (2011), A formal classification of internet banking attacks and vulnerabilities. *International Journal of Computer Science & Information Technology*, 3(1), 186-197.

[41] Peotta, L. & Holtz, M. D. (2011), "A formal classification of Internet banking attacks and vulnerabilities", *International Journal of Computer Science & Information Technology (IJCSIT)*, (3)1.

[42] Razak, L.T. (2016), The Effect of Security and Privacy Perceptions on Customers' Trust to Accept Internet Banking Services: An Extension of TAM" Mohammed A. Al-Sharaf,"Ruzaini A. Arsha," Emad Abu-Shanab and "Nabil Elayah" Faculty of Computer Systems and Software Engineering, *UMP. Journal of Engineering and Applied Sciences*, 100, 545-552.

[43] Safeena, R. (2010), Customer perspectives on E-business value: case study on Internet banking, *Journal of Internet Banking and Commerce*, 15, 1-17.

[44] Saleh, Z. (2011), "Improving security of online banking using RFID", *Academy of Banking Studies Journal*, 10(2), 1-8.

[45] Sanayei, A., & Noroozi, A. (2009), Security of Internet banking services and its linkage with users trust: A case study of percian of Iran and CIMB Bank of Malaysia, *International Conference on Computer and Electrical Engineering (ICIME).*

[46] Sarjiyus, O. & Asua, W. (2018), Security and Trust for Online Banking Services in Real World, *International Journal of Engineering Research and Allied Science*, 3(6), 1-4.

[47] Sharma, S. (2016), A detail comparative study on e-banking VS traditional banking, *International Journal of Advanced Research*, 2, 302-307.

[48] Srivastava, S. S., & Gupta, N. (2011), "A Novel Approach to Security using Extended Playfair Cipher", *International Journal of Computer Applications*, (0975 – 8887), (20)6.

[49] Thawte, The value of authentication. Retrieved on September, http://www.thawte.com, 2009.

[50] Tripathi, A. K., & Tripathi, M. (2012), "A framework of distributed database management systems in the modern enterprise and the uncertainties removal", (2) 4, *ISSN: 2277*.

[51] Une, M., & Kanda, M. (2011), "Issues on Cryptographic Algorithms".

[52] Vaciago, G., & Ramalho, D. S. (2016), Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings, *Digital Evidence & Elec. Signature L. Rev.*, 13, 88.

[53] Viega, J., Mcgraw, G. (2002), Building Secure Software. *Addison Wesley, New York*, NY 74-75.

[54] Wada F., Olumide, L., & Paul, D. (2012), Action Speaks louder than words – understanding Cyber Criminal behavior using criminological theories, *Journal of Internet Banking and Commerce*, 17(1), 01-12.

[55] Wueest, C. (2006), Threats to Online Banking, *Symantec Security Response Dublin*.

[56] Yoon, H. S., & Occena, L.(2014), "Impats of customers' perceptions on internet banking use with a smart phone", *Journal of Computer Information Systems*, 54(3),1-9.

Citation of this article:

Dr. Oye. N. D., Sarjiyus. O., “Online Security Framework for e-Banking Services: A Review”, Published in *International Research Journal of Innovations in Engineering and Technology (IRJIET)*, Volume 3, Issue 2, pp 6-21, February 2019.

****