ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

The Study of E-Security in Internet Banking

Miss Sarika B. Gaikwad[1], Miss Ashwini A. Yadav[2], Miss Pallavi H.Patil[3]

Asst. Professor, Dept. of Computer Science, Smt.K.R.P. Kanya Mahavidyalaya, Islampur (Maharashtra), India [1,2,3]

Abstract: Today's world is an electronic or digital world. The use of online services is increasing day by day. Most used and growing part of online services is Internet Banking. That provides different banking facilities with internet but banks should provides online services with safety and securely. The present study shows different cyber attacks used by cyber criminals to access bank customer's confidential information in India. This paper tries to explore several of Technologies and Security Standards recommended to banks for safe internet banking.

Keywords: Internet Banking, Security Standards, Security Tools, Threats.

I.INTRODUCTION

Electronic banking system and method in which a personal computer is connected by a network service provider directly to a host computer system of a bank such that customer service requests can be processed automatically without need for intervention by customer service representatives. The system is capable of distinguishing between those customer service requests which are capable of automated fulfillment and those requests which require handling by a customer service representative. The system is integrated with the host computer system of the bank so that the remote banking customer can access other automated services of the bank. The method of the invention includes the steps of inputting a customer banking request from among a menu of banking requests at a remote personnel computer; transmitting the banking requests to a host computer over a network; receiving the request at the host computer; identifying the type of customer banking request received; automatic logging of the service request, comparing the received request to a stored table of request types, each of the request types having an attribute to indicate whether the request.

E-banking type provides different services to the customers as an e-payment like Smart card, Debit or credit card, E-cheque etc.

Electronic banking give advantages for the banking industry as well as the customer, is an area with tremendous growth. This field has also seen a corresponding rise in network security, data thefts, data losses, identity thefts and other commercial fraud resulting in huge losses to the banking industry. When a bank's system is connected to the internet or intranet, an attack could originate anytime, anywhere. Some essential level of security must be established before business on the internet can be reliably conducted. An attack might be in the form of unauthorized access, destruction, corruption or alteration of data or any type of malicious procedure to cause network failure, reboot or hang. Many Industries, institutions and public and private sector organizations are at significant risk. Comparatively some organizations have identified organized cyber criminal networks as its most potential cyber security threat and some are ready to defend such security threats. Network and computer attacks have become common issues in today's world. Any computer connected online is under threat from viruses, worms and attacks from hackers. Thus, the need to fight computer and network challenges in form of cyber attacks is becoming gradually more essential for security professionals.

II.WHAT CAN ONLINE BANKING DO FOR YOU?

- *Enquiry*

Bank provide more better control over your finances. Whether it is account details such as your account type and number as well as your current and available balance, or your credit card information such as credit limit and recent transactions.

- *Funds Transfer*

Why write a cheque when you can transfer funds online? You can transfer funds in 4 ways:

1. Between your Bank personal accounts Via Account to Account Transfers.
2. To third party Bank accounts. Via Account to Account Transfers.
3. To accounts at any other local banks. Via Account with Other Banks.

- *Bill Payments*

You can conveniently pay your bills via Online Banking for the following:

1. Credit Card bill payments.
2. Insurance premiums.
3. Electrical and Water bills.
4. School Fees & College Fees.

- *eStatements*

You can view or download your latest Credit Card, Current and Savings Account statements online to track your transactions.

- *Cheque Book Request*

Request for a cheque book to be collected at any of Banks' branches.

- *Personal Information Management*

You can easily update your personal information with the Bank through Personal Information Management at your own convenience! This too is secured and changes will be reflected within one working day.

DOI 10.17148/IJARCCE.2015.4840

- *Rates*

View Foreign Exchange rates, updated daily, at the touch of a button.

III.WHERE SECURITY IS REQUIRED?

- Account ID and Password (PIN) Protection
- Auto Timeout Screen Blanking
- Sign-off Button
- Failed Log-on Attempts
- Encryption
- Transfer Funds
- Security regarding Backup of Data

IV.WHY SECURITY IS REQUIRED?

- By cryptography (Encryption/Decryption) Data Confidentiality is achieved.
- For Authentication and Identification of the person who uses the digital signatures.
- Access Control like valid IDs and passwords for the person who access the system.
- Unauthorized Data Integrity.
- Non-Repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

V.SECURITY THREATS

- *Pharming:*

1. In Pharming attack fraudster create false website, so that people will visit them by mistake.
2. This attack takes place when user mistype a website or a fraudster can redirect traffic from genuine website to a fake one.
3. The main purpose of pharmer is to obtain victims personal information for further frauds.

- *DOS (Denial of Service)*

There are two types of Denial of service (DOS) attacks: spamming and viruses

1. Spamming
   a. Sending unrequested commercial emails to individuals.
   b. E-mail bombing caused by a hacker targeting one computer or network, and sending thousands of email messages to it.
   c. Surfing involves hackers placing software agents onto a third-party system and setting it off to send requests to an intended target.
   d. Distributed denial of service attacks(DDOS) involves hackers placing software agents onto a number of third-party systems and setting them off to simultaneously send requests to an intended target
2. Virus is a computer program that designed to replicate self 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.
3. Worms: This is a malicious program that replicates or reproduces 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
4. Trojan Horses: Trojan horse is 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.

- *Unauthorized access*

1. Illegal access to systems, applications or data
2. Passive unauthorized access like listening to communications channel for finding secrets, May use content for damaging purposes.
3. Active unauthorized access like modifying system or data & Message stream modification.
4. Changes intent of messages, e.g., to abort or delay a negotiation on a contract
5. Spoofing containing sending a message that appears to be from someone-else,IP levels (changing the source IP address / destination IP address of packets in the network)
6. Software that illegally access data traversing across the network.
7. Software and operating system’s security holes.

- *Fraud & Theft*

1. Fraud occurs when the stolen data is used or modified.
2. Theft of software via illegal copying from company‘s servers.
3. Theft of hardware, specifically laptops, mobiles etc

- *Phishing:*

1. Phishing is a technique that used to hack or obtain the confidential information from customer.
2. Phishing is attempting to acquire information (and sometimes, indirectly, money) such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.

For example: You may receive an email which appears to have come from your bank or financial organization stating that “your bank account is limited due to an unauthorized activity. Please verify your account as soon as possible so as to avoid permanent suspension”. In most cases, you are requested to follow a link (URL) that takes you to spoofed web page (similar to your bank website) and enter your login details over there

VI.SECURITY TOOLS

•*Firewalls*

A Firewall can protect from external attacks. A firewall is program that monitors all incoming outgoing files between your PC & Internet. It restricts unauthorized connections.

DOI 10.17148/IJARCCE.2015.4840

•Encryption

When you sending the confidential data over the internet it may be accessed by unauthorized person. The bank provides security steps to protect our data by using encryption software. For that you have to enter your PIN & other access codes before transmission of the data on banks website, but don’t forget that banking session is not automatically encrypted when it is saved on your PC.Never send personal information over open network unless it is encrypted.

•Public Key infrastructure (PKI)

1. PKI allows users to exchange data securely and privately through the use of a public and private key pair, created by a certificate authority.
2. The certificate authority also creates a digital certificate, which identifies an individual or organization and includes the public key.
3. Whereas the public key is widely available to people, the private key is kept secret and only known and used by the person or company that requested it. It is used to decrypt messages that have been encrypted by someone else with the corresponding public key
4. To send an encrypted message to someone, you "lock it" using his or her freely available public key. The recipient then decrypts or "opens" it with the corresponding private key
5. The private key can also be used to encrypt a digital certificate to authenticate you to a second party. The recipient then uses the corresponding public key to decrypt it.

•Digital certificates

The Digital Certificate is a special file that serves to identify electronically the customer’s identity (through his/her web browser) before the Bank’s Internet Banking System thus increasing with one more level the Customer’s data protection when performing communication between the client and the Bank.

•Digital Signatures

Digital Signatures provides a high level of security for online transactions by ensuring absolute privacy of the information exchanged using a digital certificate. Digital signature works on the principle of Public Key Infrastructure (PKI). It is a cryptography based on a concept of key pairs (private and public key). If the transmission arrives but the digital signature does not match the public key in the digital certificate, then the client knows that the message has been altered.

- *SSL(Secure Sockets Layer)*

SSL is a system for providing security to Internet communications (especially web browsing). SSL uses encryption to provide *confidentiality* (privacy) and *authentication* (authorization).

This ensures the privacy of communication between you (your browser) and your bank’s server. It’s usually used from the stage of authorization until the end of the online banking session. If your bank provides at least 128-bit SSL encryption (the secure page’s URL always starts with “https ://”), you can be sure nobody can decrypt and see what you send to your bank and vice versa.

•Passwords

Avoid using alpha-numeric character combinations that can be easily guessed at as your password. Examples are: your birthday, telephone number, or automobile plate number. Please use the alpha-numeric character combinations (capital or small letter) difficult to be deciphered as password.

Please avoid using the same password to login other internet services, for example, internet access or email etc.Please, change your Internet banking login password regularly.

Please do not write down your username and password on paper. Do not publish your username and password to anyone nor accept suggestions for your username/password combination from other parties.

VII.GUIDELINES FOR SECURE TRANSACTIONS WITH E-BANKING

- *Security Login ID and Password or PIN*

1. Do not disclose Login ID and Password or PIN.
2. Do not store Login ID and Password or PIN on the computer.
3. Regularly change password or PIN and avoid using easy-to-guess passwords such as names or birthdays. Password should be a combination of characters (uppercase and lowercase) and numbers and should be at least 6 digits in length.

- *Keep records of online transactions*

1. Regularly check transaction history details and statements to make sure that there are no unauthorized transactions
2. Check e-mail for contacts by merchants with whom one is doing business. Merchants may send important information about transaction histories
3. Immediately notify the bank if there are unauthorized entries or transactions in the account
4. choose right and secure website for online transactions
5. Before doing any online transactions or sending personal information, make sure that correct websites has been accessed.
6. Check if the website is “secure” by checking the Universal Resource Locators (URLs) which should begin with “https” and a closed padlock icon on the status bar in the browser is displayed. To confirm authenticity of the site, double-click on the lock icon to display a security certificate information of the site
7. Always enter the URL of the website directly into the web browser.
8. If possible, use software that encrypts or scrambles the information when sending sensitive information or performing e-banking transactions online

- *Protect your PC from hackers, viruses and malicious programs*

1. Install a personal firewall and a reputable anti-virus program to protect personal computer from virus attacks or malicious programs
2. Ensure that the anti-virus program is updated and runs at all times
3. Always keep the operating system and the web browser updated with the latest security patches, in order to protect against weaknesses or vulnerabilities
4. Install updated scanner softwares to detect and eliminate malicious programs capable of capturing personal or financial information online

- *Do not leave computer unattended when logged-in*
  1. Log-off from the internet banking site when computer is unattended, even if it is for a short while
  2. Always remember to log-out when e-banking transactions have been completed
  3. Clear cookies and history of your web browser after transaction
  4. Do not store or remember the user name and password to your web browser.

- *Check the site's privacy policy and disclosures*
  1. Read and understand website disclosures specifically on refund, shipping, account debit/credit policies and other bank terms and conditions
  2. Before providing any personal financial information to a website, determine how the information will be used or shared with others
  3. Check the site's statements about the security provided for the sensitive information
  4. Check the FAQ section of website for information.
  5. Other internet security measures
  6. Do not send any personal information particularly password or PIN via ordinary e-mail
  7. Do not open other browser windows while banking online
  8. Avoid using shared or public personal computers in conducting e-banking transactions
  9. Disable the "file and printer sharing" feature on the operating system if conducting banking transactions online
  10. Contact the banking institution to discuss security concerns and remedies to any online e-banking account issues

VIII.CONCLUSION

This study indicates that internet banking allows customer to perform transactions at any time and it does not required to visit bank frequently. But, with this good factor, internet banking customers face some challenges with threats. We found that some threats or security problems affecting on customers sensitive information and these problems also faced by banks that provides internet banking facility. To overcome this security problem bank must implement or use appropriate security tools. So the customer can do the secure transactions on internet. Customer makes some common mistakes that may cause to hack or to theft the personal and confidential information. To avoid this customer can take care while doing online transaction & follow guidelines for secure transactions. Security is provided to maximum banks from secure socket protocol, message authentication, and encryption algorithms. It is clear from our survey that private banks are having 40-50% net banking users, while government banks are having only 20 to 30% net banking users.

REFERENCES

[1] Internet Security. Http://cfn.cs.dal.ca/Education/CGA/netsec.html

[2] Electronic Banking. Http://www.electrobank.com/ebaeb.html

[3] Basic Flaws in Internet Security and Commerce Http://HTTP.CS.Berkeley.EDU/~gauthier/endpoint-security.html.

[4] BankNet Electronic Banking Service. Http://sbi.co.in/bank

[5] Samir Pakojwar,Dr.N.J.Uke " Security in Online Banking Services –A Comparative Study" International Journal of Innovative Research in Science, Engineering and Technology Vol. 3, Issue 10, October 2014

[6] The Security Of Electronic Banking by Yi-Jen Yang

[7] Niranjanamurthy M, Kavyashree N, Mr S.Jagannath ―M-Commerce: Security Challenges Issues And Recommended Secure Payment Method‖-Ijmie Volume 2, Issue 8 Issn: 2249-0558-2012

[8] Analytical Study on Internet Banking System Fadhel.S.AlAbdullah,FahadH.Alshammari,Rami Alnaqeib,Hamid A.Jalab, A.A.Zaidan,B.B.Zaidan Journal of Computing, Volume 2, Issue 6, June 2010, ISSN 2151-9617

[9] Susheel Chandra Bhatt, Durgesh Pant "Study of Indian Banks Websites for Cyber Crime Safety Mechanism".(IJACSA) International Journal of Advanced Computer Science and Applications , Vol. 2, No.10, 2011

BIOGRAPHIES

Miss Sarika Baban Gaikwad holds Post Graduate Degree in Computer Application.Presently she is working as Asst.Professor at Smt.K.R.P. Kanya Mahavidyalaya,Islampur, Maharashtra ,India.She has Four years of teaching experience. Her areas of interest are E-Commerce, Software Engineering and Programming Area.

Miss Ashwini Appasaheb Yadav holds Post Graduate Degree in Computer Application.Presently she is working as Asst.Professor at Smt.K.R.P. Kanya Mahavidyalaya,Islampur, Maharashtra , India.She has Four years of teaching experience. Her areas of interest are E-Commerce, computer network and AI.

Miss Pallavi Hanmantrao Patil holds Post Graduate Degree in Computer Science. Presently she is working as Asst.Professor at Smt.K.R.P. Kanya Mahavidyalaya,Islampur, Maharashtra , India.She has Four years of teaching experience. Her areas of interest are E-Commerce, computer network and PHP.