Volume 3, Issue 8, August 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Online Banking Security Flaws: A Study

Rajpreet Kaur Jassal
Assistant Professor
BBSBEC Fatehgarh Sahib, India

Ravinder Kumar Sehgal
Principal
JSSIET, Kauli, Patiala, India

Abstract: Online banking has become increasingly important to the profitability of financial institutions as well as adding convenience for their customers. As the number of customers using online banking increases, online banking systems are becoming more desirable targets for criminals to attack. To maintain their customers' trust and confidence in the security of their online bank accounts, financial institutions must identify how attackers compromise accounts and develop methods to protect them. The unique aspect about security in banking industry is that the security posture of a bank does not depend solely on the safeguards and practices implemented by the bank, it is equally dependent on the awareness of the users using the banking channel and the quality of end-user terminals. This makes the task for protecting information confidentiality and integrity a greater challenge for the banking industry. This paper aims to explains about the reason behind the security breaches and the participation of both customers and the banks to enable the hackers or crackers to access others network. The present study aims to find various types of flaws in the security of online banking that results in loss of money of account holders and financial institutions. Security breaches are not only because of banks faults and banks inadequate polices but customers are equally responsible for it, because customers awareness regarding security is equally important .

Keywords: Online Banking Security, Security Flaws, Security Policy, Users Usability, Customer Awareness

I. INTRODUCTION

Internet banking has gained wide acceptance internationally and seems to be fast catching up in India with more and more banks entering the fray. Online banking allows customers or users to conduct financial transactions on a secure website operated by their banks, credit unions or building societies. It can be accessed from anywhere that there is a computer with the Internet, and of course unlike bank branches the net is open 24 hours a day 7 days a week.In spite of the great benefits ,the number of malicious applications security problems (targeting) of online banking transactions has increased dramatically in recent years. This represents a challenge not only to the customers who use such facilities, but also to the institutions who offer them, as evidenced by an ongoing trail in the US[8]. For example, in 2008 ,England suffered online banking fraud losses that amounted to £53 million2, and the U.S. had hundreds of millions of dollars in fraud losses resulting from online attacks in 2009. According to the data compiled by the Reserve Bank of India (RBI), the money lost to such scams has doubled in the past four years. In the year 2009, banks lost Rs.2,289 crore (till December), while the loss was Rs.1,057 crore in 2007-08[ ].

So the safe and secure environment of computer technology is the most important concern for all financial service organizations. The responsibility of secure online banking is not only on the banks but also on the customers, because the customers, to operate the online banking, have to have a certain level of knowledge and technical competence and awareness[12]. This paper aims to explains about the reason behind the security breaches and the participation of both customers and the banks to enable the hackers or crackers to access others network. In spite of all these, the use of online banking is increasing and will be increasing in the future. The present study aims to find various types of flaws in the security of online banking that results in loss of money of my account holders along with leakage of their personal information to unauthorized persons. Security breaches are not only because of banks faults and banks inadequate polices but customers are equally responsible for it, because customers awareness regarding security is equally important .

.

II. ONLINE BANKING

At the basic level, Internet banking can mean the setting up of a web page by a bank to give information about its products and services. At an advanced level, it involves provision of facilities such as accessing accounts, transferring funds, and buying financial products or services online as well as new banking services, such as electronic bill presentment and payment, which allow the customers to pay and receive the bills on a bank's website. This is called "transactional" online banking [1]. Online banking is a series of processes in which a bank client logs on to the Website of the bank through the Web-browser that is installed on client's Personal computer and carries out various transactions such as account transfers, bill submissions, account inquiries etc. Online banking is carried out in four major stages illustrated below in Figure 1.

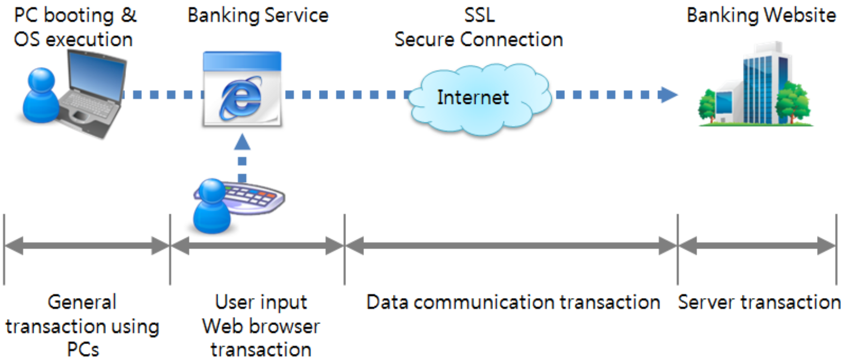
PC booting & OS execution
Banking Service
SSL Secure Connection
Internet
Banking Website
General transaction using PCs
User input Web browser transaction
Data communication transaction
Server transaction

Fig. 1 Online Banking Transaction

For any OLT (Online Transcation)the user first turns on the PC and then open web-browser, accesses the online banking website of the bank and enters the ID or Personal Identifying Number (PIN) and the password by using the keyboard or virtual keyboard. SSL (Secure Socket Layer) encrypt the data transmitted between client's PC and bank's server. The bank's server decrypts the transmitted information and processes the user's authentication, account inquiry, account transfer, etc.[9] But during this whole processing prevalence of malicious applications that steal financial account information has increased dramatically over the last few years, often resulting in victims losing hard currency. The attackers tend to target the weakest link whether it is host computer or bank's server or bank's website. Once the attacker has control over a user's computer anyway , he or she can take advantage by Interruption, Interception, Modification Fabrication of information.

So, Security of online banking transactions is one of the most important areas of concerns to the banking sector. Security issues include adoption of internationally accepted state-of- the art minimum technology standards for access control, encryption / decryption (minimum key length etc), firewalls, verification of digital signature, Public Key infrastructure (PKI) etc by banks. Along with it the security policy for the banking industry, security awareness and education are also the security issues that are given same importance.[6]

III. ONLINE BANKING SECURITY FLAWS

Billions of financial data transactions occur online every day and bank cyber crimes take place every day when bank information is compromised by skilled criminal hackers by manipulating a financial institution's online information system. This causes huge financial loses to the banks and customers. The evolution history of attacks began more than 7 years ago initiating what quickly became known as phishing [20]. Its sophistication has increased on par with the new security technologies adopted by the bank industry intended to mitigate the problem. This means there are some flaws in the security of online banking that results in loss of money of many account holders along with leakage of their personal information to unauthorized persons.

A. Flaws in banking websites

According to a recent study by University of Michigan ,in an examination of 214 bank Websites ,more than 75 percent of bank websites have at least one design flaw that could lead to the theft of customer information and flaws are ones that even an expert user would find difficult to detect and unlike bugs, cannot be fixed with a patch. It was recommended to use SSL throughout the entire website and to avoid using links to third-party sites[15].Secure banking websites have become an integral part of our day-to-day life from our personal to our job-related business . A survey conducted by Pew Internet states 42% of all internet users bank online. With 24/7 access from around the world users can view balances, transfer funds and lots more at their convenience using online banking. Due to the sensitive nature of these sites, security is a top priority. Hackers are increasingly launching targeted attacks against weak websites, as opposed to automated attacks against tens of thousands of sites at once .According to whiteHat Report 2011 the Cross-site scripting was the most prevalent threat, accounting for 55 percent of serious vulnerabilities. Cross-site scripting is when an attacker injects into a web page malicious scripts that can bypass a browser's security mechanism to gain access to a visiting user's computer.

Information leakage was the second most prevalent vulnerability. The flaw was found in 53 percent of the sites, down from 64 percent in 2010, when the vulnerability was number one. In general, WhiteHat found that Web application firewalls would have helped mitigate slightly more than 70 percent of custom Web application vulnerabilities. SQL injection vulnerabilities, a favorite hacker target, was the eighth most prevalent flaw. Fully 5 percent of sites had at least one such vulnerability that could be exploited without logging into the site.SQL injection is a popular way to attack databases through a website. SQL statements are entered into a field on a web form in an attempt to get the website to pass the command to the database. A typical request is for the database to deliver its content to the attacker. One such example is HDFC bank website https://leads.hdfcbank.com leaks information about individual Customers. This can be done by changing the Customer Id when opening up a Recurring Deposit Account[14]. It was seen on 4 feb,2010 and fixed on 17 feb,2010.The SQL vulnerability on HDFC Bank's website was discovered on 15-July-2011 and was reported on 17-July-2011.But even after conducting the vulnerability assessment from a third party they were not able to discover this critical flaw that existed in their web portal since a long time, until complete inputs about the vulnerability is sent to their security team.[14] According to a study released earlier this year by WhiteHat Security, the top banking Web site vulnerability in 2010 was information leakage. The term was used as a catch-all description of a vulnerability in which a Web site reveals sensitive data such as technical details of the Web application, environment or user-specific data.[13] WhiteHat revealed that common causes of this vulnerability were site operators' failure to "scrub out" HTML or script comments containing sensitive information, such as database passwords and improper application or server configurations. In its WhiteHat Security Website Statistics Report, released on Wednesday 6/29/2012, the company found that the average Website had 79 serious vulnerabilities in 2011, compared with 230 in 2010 but Banking Websites possessed the fewest number of serious vulnerabilities (17) of any industry.

Many banking websites Present Secure Login Options on Insecure Pages which leave users vulnerable to man-in-the-middle attacks. Users don't have any way of knowing if their usernames and passwords are being sent to a hacker site. This makes it impossible for a user to make the correct decision. Some banking Sites forwarded users to new pages that had different domains without notifying the user from a secure page. Generally, if a knowledgeable user visits a secure website of bank, he or she will look for the bank's name in the URL, prefixed by https. Several financial institution websites start with https, but for some transactions, they redirect the customer to a site with different domain and even the signed certificate also bears a different company name. Now it is up to the user to determine if the new site is really affiliated with the financial institution or it happens to be a window that popped up as a result of some other event, or even an attack[2]. Contact Information/Security Advice on Insecure Pages that can be changed by hackers and can be used for their benefit because users rely on that information. So not only the data channel must be secured, but also the context that is used to generate the session keys for the channel must be secured and that security-relevant context is contact information or security advice because users rely on that Information. operations. And it has been also noted that some of the banking sites don't provide contact details where user should report in case of any security breech or suspected fraud. According to DSCI-KPMG Survey-2010 only 63% of Indian bank sites provide contact details on sites to report any breach-63% [10].

Security-Sensitive Information like social security numbers or passwords or account statements provided through email that is insecure channel of communication. Some banks send passwords or user IDs through email if user request that information incase user forget it and most of banks provide account statements monthly through email. But if mail server is insecure, an attacker could be view unencrypted traffic on the network and obtain the sensitive information and accounts of users can be compromised. Some banking sites has IP addresses that match with other lot of ugly sites that can result in easy hacking. And example of it is Jammu and Kashmir Bank's website. A reverse IP check shows this jkbank.net has the IP address: 68.178.156.75 and 53 sites found with the IP 68.178.156.75,a shared host with 53 ugly sites[5].

ICICI bank recently done mistake that the content of the CAPTCHA image was being sent in the Response Header. This happened on the form where you enter your credit card details. It definitely made no sense having the CAPTCHA.[5]

B. Flaws in Banking Policies

The Security Policy is intended to define what is expected from an organization with respect to security of Information Systems. The overall objective is to control or guide human behavior in an attempt to reduce the risk to information assets by accidental or deliberate actions[17]. Protecting customers' privacy and security is important to every bank. So, every bank has some security policies that they publish online in order to help users understand the security measures the bank is taking to make their information secure. It tells how bank is committed to keeping users safe online and uses state of the art fraud prevention and detection technology, monitored around the clock by a dedicated team, to actively protect their finances and confidential information. But along with this users have to play an important role in security. Policy also includes do and don'ts by users and also about hoax emails and security tips for users. So that they can enjoy peace of mind when doing online banking. Security policies should include:

- Security Policy for general users
- Security Policy for banks
- Security Policy for network
- Security Policy for software
- Backup Policy

Security policy for general users should include all the security tips for users i.e what they should do and should not do while doing online banking .

Security policies of bank should clearly indicate that this Privacy Statement does not extend to third party sites linked to this website and advise users to always read the privacy and security statements on these websites. Most of the banking sites has inadequate policies for user IDs and Passwords. Social security numbers and e-mail addresses and date of Births are used for user ids and passwords that can be easily guessed or collected from internet. Banking sites don't have any stated policy regarding user IDs and passwords that can protect account against dictionary attacks. But online banking password 'strength meter' can provide a visible indication of how secure your password is when you are registering or changing your online banking password. The risk assessments indicate that single-factor authentication is the only control mechanism, that is inadequate in the case of high-risk transactions involving access to customer information or the movement of funds to other parties, so banks should try to shift from single factor authentication policy to multifactor authentication like use of One time password(TAN) and security tokens or smart cards and biometrics[11]and most latest PKI. There should be some provision for automatic timeout periods and password lockout so that if user logged in to account, but haven't been using it for a certain period of time, account will automatically logout user so that anyone else cannot access banking details if user leave computer unattended. And password lockout policy helps if someone does try to guess password of user, account will be locked after a set number of unsuccessful attempts.

The network must be designed and configured to deliver high performance and reliability to meet the needs of the operations whilst providing a high degree of access controls and range of privilege restrictions. System hardware, operating and application software, the networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorized network intrusion .So there should be strong policies regarding use of Intrusion detection systems, firewall configurations used and virus scanning tools to protect against unauthorized persons and viruses from entering our systems of bank. To make all communication secure from user's computer to bank, data should be encrypted to ensure the confidentiality of all data sent and received, 256-bit SSL encryption technology should be used. A padlock symbol displayed on web browser tells the user that you are viewing a secure web page. Bank should regularly employs independent security consultants to confirm the security of systems by reviews of areas such as architecture, firewall configurations , the security of web server and the security of the different applications on site. So every bank should make policy regarding use of firewall configurations, network device security, web server security and web application security and security audits.

Banks should strongly advise users to keep an OS and browser up-to-date with security patches .Even most of banks in India support, out-dated browser versions such as IE 5.5 and Firefox 1.0. Updating OS, browser, firewall and anti-malware is challenging for many Internet users. Patch management includes collecting all necessary patches, dealing with postpatch conflicts, determining the trustworthiness of a patch source etc. [9], which is a difficult problem even for enterprise IT departments. In addition to usability problems, such updates may even frustrate or fool diligent users. For example, Bellissimo et al. [6] showed that some popular software updates (e.g. McAfee VirusScan) were vulnerable to man-inthe-middle attacks; i.e., a malicious party could install malware exploiting several software update vulnerabilities. [7]. Other problem is that no *Universal Standard* format for a Privacy Policy has been designed and declared for banks in India yet. It will be very helpful for online banking consumers, if there is an authority to monitor and control the proper format and points included in the privacy policy for banks. Some policies are too small whereas some of them are too large and difficult to understand and some banks policy links are inactive[3].Changed policies should be uploaded to the banking sites along with date of change and information regarding this should be given to users either in the form of highlights or new events. According to a survey only 11% sites notify users about change in policy[3]. Even the Reserve Bank of India (RBI) that is the main body, has been issuing various directions and recommendations from time to time to strengthen cyber security of banks operating in India, however, Indian banks are not following the directions of RBI in this regard in toto and a majority of banks in India still do not have a well defined cyber security policy. RBI observed that at present some banks do not have proper security policy and methods to monitor the service level agreements with third parties and have inadequate audit trail, so it has issued warning to banks to comply the directions of RBI by Oct,2012[16].

According to a research report only 43% of the banks have posted their privacy policies on their web sites. It is observed that in some cases, like PNB , privacy policy is exceptionally small and does not include even minimum number of points which are essential to make a privacy policy, i.e it does not include general user policy means what is expected from user's side. These types of privacy policies should be improved.9% websites are having inactive link of privacy policy on their home page which is not fair with the consumer[3].The presence of Privacy Seal in privacy policy makes the users feel more secure for their personal information but it is a finding here that very few websites have privacy seal. According to a research report 37% of Banking websites security policy clearly spells the restriction in disclosure of the information to third party. Only 26% banking sites provide links to the policy on all important user centric data forms. Only 26% banks, policy list the security countermeasures deployed to secure the information and above all only 42% banks display their privacy policy on corporate website of the bank[4].

C. Flaws in Users Usability and Customer Awareness

The unique aspect about information security in banking industry is that the security posture of a bank does not depend solely on the safeguards and practices implemented by the bank, it is equally dependent on the awareness of the users. This makes the task for protecting information confidentiality and integrity a greater challenge for the banking industry. Financial institutions have made, and should continue to make, efforts to educate their customers. Because customer awareness is a key defense against fraud and identity theft, because the biggest threat to online banking is still malicious code executed carelessly on the end-user's computer. The attackers tend to target the weakest link. Once the attacker has control over a user's computer, he or she can modify the information flow to his or her advantage. So financial institutions should evaluate their consumer education efforts to determine if additional steps are necessary. Management should implement a customer awareness program and periodically evaluate its effectiveness. Methods to evaluate a program's effectiveness include tracking the number of customers who report fraudulent attempts to obtain their authentication credentials (e.g., ID/password), the number of clicks on information security links on Web sites, the number of statement stuffers or other direct mail communications, the dollar amount of losses relating to identity theft, etc.[11] Social networking sites such as Facebook, MySpace and LinkedIn are a great way to keep in contact with friends and update professional associates. Unfortunately these also offer cyber criminals another way to gather information about clients. For protection, while using these social networking sites :

- Make sure your profile pages are only accessible to people you trust and not to the general public by customizing the security settings
- Never publish personal or sensitive information such as your birthday, drivers license number, tax file number or bank account details
- Use a different email address if you want to publish this online
- Don't publish contact details such as your home address or phone number
- Don't use same security questions as used in banking accounts like your pet name etc.

Most of the Privacy policies contain the information that our web sites may contain links to non-Group web sites and links are provided for client's convenience.Banks say "we try to link only to websites that also have high standards and respect for privacy but we are not responsible for their security and privacy practices or their content. We recommend that you always read the privacy and security statements on these websites".So users should review their bank's information about its online privacy policies and practices**.** By law, banks are required to send a copy of their privacy policies and practices annually to clients; clients may also request a copy of this information. Bank web sites should also have this information. As clients read this information, pay particular attention to any mention of the methods used for encrypting transactions and authenticating user information.

Online banking involves certain risks. For clients it is important to educate them self about these risks, how unauthorized access to their financial information occurs, and the steps they can take to protect their financial information. Learning about their rights and responsibilities as an online banking consumer can make a difference to their financial well-being by changing the age-old saying "A penny saved is a penny earned" to "A penny saved is a penny kept."[6]. Banks also publish on website, security tips along with their security policy for online banking, so users should always use those tips before going for any transaction.

To ensure that bank security measures can't be undetermined by manipulation, it is essential that customers ,too take steps to protect the system they use. The ordinary PC environment is exposed to many types of threats because of unsafe web surfing , all types of games and installation and/or use of a variety of unverified programs. If a user carries out an online banking transaction in an environment exposed to various threats, there is no way to guarantee safety for that online banking transaction, because Anti-virus and Anti-Malware programs are installed in the PC to protect against these threats, are unable to counter the exponentially increasing new breed of malicious code. because the Anti-Malware technology is signature base which only detects known threats. For example, the hacking tool for online banking called, Zeus, contains a technology that detects and avoids the Anti- Malware software, and is constantly spreading new breeds or variants of Zeus mostly through famous Web sites, fake Web sites, phishing sites, e-mail, etc. So they should be security conscious when using internet and check their bank statements regularly. 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. In short, having no proper protective measures, a considerable number of PCs may be using the Internet banking even now, completely unaware that they are infected with a variety of hacking tools or malicious codes.[9]. Banks also advise their customers to keep an OS and browser up-to-date with security patches. Beyond the web browser, generally there are many more applications commonly used by millions of users like Microsoft Office products such as Word and Excel, Media players such as Windows Media Player, Realplayer also pose security threats if unpatched and thereby being targeted by attackers. In fact, users must keep all applications up-to-date to avoid known attacks , especially in a Windows environment, though its difficult. Other operating systems, e.g., Ubuntu Linux and Mac OS X provide an update mechanism to keep all installed (native)software packages updated – but these are used by less than 5% of the population[7].While online, user should never surf internet in administrator mode, only surf with minimal user rights, because this makes manipulations and unauthorized accesses more difficult.

The banking sites generally present many security guidelines on their websites. According to DSCI-KPMG Survey-2010 report 100% India's banking sites publish do and don'ts on their websites and 53% Providing demo for secure usage of banking services [10].Banks display following security tips on their sites for clients for security of their funds and information.

1. Banks strongly recommend users to Access your bank website only by typing the URL in the address bar of your browser and also ensure the address on the address bar of your internet browser begins with https.
2. Do not enter login or other sensitive information in any pop up window and prefer to use virtual keyboard for entering login information.
3. Verify the security certificate by clicking on the padlock icon of your internet browser.
4. Use newer version of Operating System with latest security patches.
5. Use latest version of Browsers
6. Ensure that Firewall is enabled and Antivirus signatures applied
7. Scan your computer regularly with Antivirus to ensure that the system is Virus/Trojan free.
8. Change your Internet Banking password at periodical intervals.
9. Always check the last log-in date and time in the post login page.
10. Avoid accessing Internet banking accounts from cyber cafes or shared PCs.
11. Use SMS alert services of bank.

12. Keep your mobile phone and other information updated with bank for OTP and SMS alerts.

Some banks like ICCI bank, State Bank of Patiala also provide demo for how to use online banking that helps the customers a lot but the thing is that customer should have the awareness about what the bank is providing for the security and what the customers should do to make transactions completely secure.

According to DSCI-KPMG Survey-2010 measures such as SMS alert, separate transaction password, virtual keyboard seem to be more popular, adoption of the strongly advocated measures such as One-Time-Password (dynamic token), identity grid and risk based authentication are still at a nascent stage[10].But One of the most significant information security challenges highlighted by the banks in the survey is lack of customer awareness on information security and the threat from insecure customer end points.

IV. Conclusion

So online banking facilities give users the flexibility to undertake their banking at a time that best suits them and also saves time but it also presents various security threats.Banks deploy protocols such as SSL and many of them hire security experts to conduct vulnerability assessments and find design flaws in their websites that prevent secure usage. Even then most of the bank sites has design flaws that cause security breaches. Along with this the security polices of the banks have no standard format and policies are inadequate that leads to many security risks. The Security posture of a bank does not depend solely on the safeguards and practices implemented by the bank, it is equally dependent on the awareness of the users using the banking channel and the quality of end-user terminals because the hackers always choose the easiest way to attack.Generally the easiest seems to be attacking the user or his/her PC, so awareness and usability of users is also equally important to make online banking 100% secure. So 100% security guarantee that is given by banks for users transactions is possible if both banks and users together give flawless security posture to online banking by removing all the given security flaws.

References

[1] *Sathye, M. (1999).Adoption of Internet banking by Australian consumers: an empirical investigation. International Journal of Bank Marketing, Vol. 17, No. 7, pp: 324-334.*

[1] White paper on“*Threats to Online Banking- Symantec Security Response”, Dublin*

[2] *W. Lampson Butler ," Computer Security in the Real World “,Annual Computer Security Applications Conference, 2000.*

[3] *Dr. Abha Chandra,Mrs. Vinita Sharma “Analytical Resarch on Indian Online Banking and Users’Privacy”,in Global Journal of Enterprise Information System jan-june2010 vol-2 issue1*

[4] *White Paper,”Best Security Practices in online Banking”, easySolutions 2009.*

[5] *“Internet Banking Flaws in India Banking ” webDEViL ,20th Oct,2008*

[6] ” *Banking Securely Online* **“,***US-CERT, a government organization. 2006, Updated 2008.*

[7] *Mohammad Mannan, P.C. van Oorschot,*“ *Security and Usability:The Gap in Real-World Online Banking”, New Security Paradigms Workshop (NSPW) 2007 New Hampshire, USA.*

[8] *Neha Dixit ,”Acceptance of E-banking among Adult Customers:An Empirical Investigation in India “ , Journal of Internet Banking and Commerce, August 2010, vol. 15, no.2*

[9] *“Online Banking: threats and Countermeasures Revised Version: 1.3”, AhnLab, Inc., June, 2010.*

[10] ”State of Data Security and Privacy in Indian banking Industry- *DSCI-KPMG Survey-2010”, Data Security Council of India, published in feb,2011,*

[11] *Authentication in an Internet Banking Environment by Federal Financial Institutions Examination Council,June 29,2011 [online] Available : http://www.fdic.gov/news/news/financial/2010/index.html*

[12] *Zakaria Karim1, Karim Mohammed* Rezaul2, Aliar Hossain1, **“***Towards Secure Information Systems in Online Banking”, International Conference on 2qInternet Technology and Secured Transactions, ICITST 2009.*

[13] *http://www.zsecure.net/blog/vulnerabilities/hdfc-bank-sql-injection-vulnerability.html*

[14] *http://www.zdnet.com/hackers-gunning-for-banks-web-servers-sites-2062301212/*

[15] *Sue Marquette Poremba”Study: Security flaws threaten online banking”, July 28, 2008 [online] Avaialable:http://www.scmagazine.com/study-security-flaws-threaten-online-banking/article/113010/*

[16] *http://ptlbindia.blogspot.com.au/2012/03/rbi-warned-indian-banks-for-inadequate.html*