Security Patches Against the Loopholes in Internet Banking

Mrs T. K. George
Research Scholar
Cochin University of Science and Technology

Dr. Paulose Jacob
Professor
Cochin University of Science and Technology

Abstract **- The Banking industry is undergoing a major transition after the Introduction of internet banking services. The products & services are available for the customers, just a click away from them, through the internet and communication technology. In the middle of these sophisticated facilities there a lot of security and privacy concerns to be tackled by the banker in order to have an effective and convenient transaction management system. One of the added advantages of internet banking is remote accessing is possible for almost all types of transactions with a faster result. There is an increase in number of loop holes occurs due to diversification of hardware and software used in internet transaction to avail the product and services in Internet banking. There should be an appropriate strategy to deal with this situation. An appropriate authentication mechanism and a cryptosystem can be the most favored technology for increasing the security and reducing the vulnerabilities in internet banking.**

Keywords: Internet banking, Authentication, Loop holes, Cryptosystem, Security patches

INTRODUCTION:

Security is one of the important concerns in internet banking[1]. The industry is facing lots of challenges, if they are provided with a vulnerable system for accessing the details and storing and communicating the transactions to the concerned people in different locations. Secured encryption / decryption system, standard firewalls and fraudulent authentication strategies of Public Key Infrastructure can be some of the strong area to be considered for patching up the major loopholes in the system. There are different dimensions to tackle the global transactions, which seem to be the problematic issue for the bankers to deal with the security of data and its transmission within the network. The dimensions of the risk are higher over the internet and the prevention or control measures are comparatively fewer[2]. Appropriate technological support is required to transmit the information safely. The security concerns can be addressed at different levels such as security of customer information, Internet banking server with customer database and the malicious attack during the transaction management. Online banking application must support data encryption at the highest level to achieve the security in encryption. Internet banking transactions should have a browser that supports this encryption and patches up any security holes in it.

Infrastructure support for Internet Banking

Most of the bankers are focusing on internet channel for providing banking services, as the cost of banking services in conventional methods are expensive compared to internet banking[2]. The important tasks such as user interaction, online transaction processing based on the business rules, data storage and retrieval can be implemented by using a multi-tier framework. It consists of a presentation layer which deals with session management and interface related issues. There also exists an application layer which is in charge of ensuring the business rules and a data layer which updates, maintains & recovers data. Security infrastructure usually deals with the security of the hardware, software and network by considering authentication, authorization, non-repudiation and Data protection. Appropriate entry of personal identification number and the password is an important aspect of authentication. There is special user code by the bank for each customer to process the transaction. The major part of data protection is carried out by a secure socket layer, which will ensure the confidentiality and integrity of the data transmission with the help of a crypto system. This protocol is supported by all the major servers and browsers and ensures that the encryption and decryptions are done with required strength of verification by the recipient. Strength of data transmission depends on the length of encryption key is being used. Size of the key is having utmost importance in data protection. In the SSL protocol, 40-bit and 128-bit encryption is used[5].

Important rules of Information Security.

Some of the important factors, which are to be considered as the important rules of information security is as follows:

- If the information system is not protected properly it is a business crime.
- Information Security Policy has to be incorporated according to the requirement specification, otherwise it is not acceptable.

- Auditing has to be done frequently to identify and monitoring the security status.
- There should be an appropriate Analysis & Risk management strategy, which will strengthen the security aspects of information system.
- An appropriate malware protection technique has to be implemented.

In any e-commerce, there should be an appropriate plan policy and protection mechanism to protect the information online against the cyber-attacks [6].

Theoretical framework for Consumer adoption of Internet Banking

According to one of the research survey conducted[7],while taking a decision on opting the internet banking ,the customers may select their transaction management system based on the factors such as ,accessibility, self-efficacy, convenience and usability. The survey states that, the bank must have marketing strategies to attract banking customer's attention to the internet banking services and provide the supporting facilities to carry out the transaction. There should be a clear demarcation on the advantages they are going to avail is very high while comparing it with the traditional banking services and the cost and risk involved in the transaction process are very low. The bank should provide sufficient support to increase the confidence level of the consumers by providing them with the knowledge base to handle the transaction in a secure and trust worthy platform. This will contribute significantly to the customers for the adoption of online banking as the transaction management system[7].

Loop holes & security Patches.

PKI plays an important role in supporting the required security services, by way of providing key certificate for the trusted path to support the digital signature to increase the confidentiality of electronic transactions. Security tools scanners, sniffer devices, intrusion detection and other auditing tools can be used for monitoring and controlling users, networks and banking systems[8].

In internet banking, appropriate security of hardware, software and communication technology is essential to preserve the resources against the unauthorized access and preserve the valuable resources from any type of malicious attack or destruction[9]. There should be a proper authentication system to verify the identity of the customer and stop the vulnerable unauthorized entities by using an appropriate crypto system. Malicious users can cause major changes in the system. Discretionary or mandatory access control can be implemented for the effectiveness of the system. An intruder can be the reason for denying the access of a privileged user. In the absence of a properly configured system and lack of security patches, hackers can enter the system through the security holes. With the help of an appropriate encryption & decryption system the confidentiality of the message can be ensured.

General view on the Support of Security Policies within the Bank

Design & utilization of security policies are important criteria to formulate the information security measures and to protect the system from the vulnerabilities[10]. Some of the general views regarding the security policies are:

- Assign the appropriate priorities for information systems that have to be protected.
- Responsibilities of the management team and their support have to be clearly indicated.
- Cyber security involvement and counter measures to protect the system should be indicated.
- Prior to the implementation of the system risk analysis, an auditing has to be done.
- There should be an appropriate format or procedure and a periodic review for updating the current requirements & security measures.
- Employee's role & responsibilities have to be indicated with due importance to take care of the system.
- Training and awareness programs have to be conducted.

Recommendations and views on security measures of Internet banking.

Strong hardware and software based system keep the communication channel strong by controlling the traffic within the channel. A through testing of the malware has to be done to stop the vulnerabilities in Operating system and browser and other programs. It is important to ensure that the system is running on the most secured security patches against the loop holes.

The most favored supporting technology for internet banking is the Public Key Infrastructure (PKI), which is not easily available. Some of the research report indicates that usually the governments recommend this technology because of its usage of 128-bit SSL for server authentication and the verification of the credentials [11] .The application server should provide only the required services and should be isolated. There should be a provision of appropriate Audit Trail and the security log should be handled carefully. The responsible security officer should conduct penetration test to take care of password-cracking Denial of services, Security holes in the software. Some of these tests can be performed with the help of an 'Ethical hacker'. But appropriate care should be taken for physical access to protect the system from internal and external threats. Back up of data & its recovery after the failure, should be taken care, by providing the required infrastructure and testing it periodically. Security scanning and monitoring system can be placed to take care of the intrusion detection. Training

should be provided in a continuous basis for those who handle the technical aspect of the banks, and any changes in security policies have to be informed on priority basis. Only certified products or solutions should be used by the agents to give security patches or to protect the system to have a better control.

CONCLUSION

The importance of secure transactions should be addressed from every angle within the frame work of the internet banking application. Better authentication levels of user data can be carried out by deploying SSL security protocol on the web server, and the proper choice of browser software along with the multitier framework will create yet another firewall to carry out the specific functions on the dedicated network[12]. Keeping a check on the attempts of intruders and taking the customers into confidence by reaching the resources to the most valued customers within a strong internet security frame work, will achieve profit in new generation banking Business.

Customers' perception can be changed by awareness programs. Easy and convenient access, required level of security, decrease in transaction costs and timely response to the queries are clear indicators of better adoption of internet banking among the future users of the banking services. Online banking is an aspect of banking that nobody can resist because it is one of the most convenient ways of banking transactions with faster result.

REFERENCES:

[1].Mukherjee A and Nath P (2003), "A model of trust in online relationship banking", International Journal of Bank Marketing, Vol. 21, No.1, pp.5-15.

[2].Nath R, Paul S and Monica P (2001), "Bankers' Perspectives on Internet Banking" e-Service Journal, Vol. 1, No.1, pp.21-36.

[3].Dhillon, G. and Torkzadeh, G. (2006) Values-focused assessment of information system security in organizations. Information Systems Journal 16 (3): 293–314.

[4].Singhal, D and V. Padhmanabhan (2008). A Study on Customer Perception Towards internet Banking: Identifying major contributing factors. The Journal of Nepalese Business Studies. V (1), 101 – 111.

[5]. Parker, Donn B., (2004) Toward a new framework for information security, in Computer Security Handbook, 4th edition, Bosworth, Seymour and Kabay, M. E. (eds.), John Wiley and Sons.

[6]. H.R. 4061—111 th Congress: Cybersecurity Enhancement Act of 2010. (2009). InGovTrack.us (database of federal legislation). Retrieved June 7, 2010, from http://www.govtrack.us/congress/bill.xpd?bill=h111 -4061.

[7].Gartner, "Online Banking Goes Mainstream in US", Nua Internet Surveys, Scope Communications Group, 2003b.

[8].N. K. Malhotra, S. S. Kim, J. Agarwal (2004), "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model" Information Systems Research, vol. 15, no. 4, pp. 336-355.

[9].Giannakoudi, S. (1999) 'Internet banking: the digital voyage of banking and money in cyberspace', *Information and Communications Technology Law*, Vol. 8, No. 3, pp.205–243.

[10].Mishra A K (2005), "Internet Banking in India Part-I",

[11].Beer, Stan (2006). Customers Preference on Internet Banking, Survey (Retrieved from http://www.itwire.com/content/view/4570/53 on March 20, 2009).

[12]. http://www.tech2date-com/the-history-of-internet-banking.html