BEST: International Journal of Management, Information Technology and Engineering (BEST: IJMITE)
ISSN(Print):2348-0513; ISSN(Online): 2454-471X
Vol. 3, Issue 8, Aug 2015, 1-8
© BEST Journals

AN ANALYSIS OF SECURITY ISSUES IN E-BANKING

PRANJAL KUMAR CHAKRAVARTI

Assistant Professor, Department of Commerce, Scottish Church College, Kolkata, West Bengal, India

ABSTRACT

In the midway of the 1990s, due to proliferation of the internet and other pioneering area of Information Technology have affected the financial system greatly, such as by moving from limited proprietary systems to open networks. E-banking which is one of the most promising areas of e-finance as financial services are information-intensive and often require no physical transition. E-banking has become increasingly gaining popularity globally, because it is easy and convenient for Internet users to deal with their bank accounts from anywhere of the world at any time. Banks have encouraged for this trend for several years, since it saves lots of resources for the banks regarding of staff training, investment for ATMs and branches, and other operations costs. This easy access to financial accounts makes Internet banking a common target for hackers and other online intruders. Present study focuses on the analysis and evaluation security issues in e-banking system.

KEYWORD: Information Technology, E-Banking, Security Issue, Hackers, Phishing

INTRODUCTION

The Internet has played a key role in changing the business today. As a result of the Internet, electronic commerce has emerged, allowing businesses to more efficiently interact with their customers and other business entities inside and outside their industries. One industry that is using this new communication channel to reach its customers is the banking industry. The e-banking system addresses several emerging trends: customers' demand for anytime, anywhere service, product time-to-market imperatives and increasingly complex back-office integration challenges. A secure end-to-end transaction requires a secure protocol to communicate over entrusted public channels and a trusted private channel at both endpoints.

Deployment of secure protocols is necessary because availability of the trusted channels does not exist in most of the environment, especially when banks are dealing with the outside consumers. The solutions to the security issues require the use of software-based systems or hardware-based systems or a hybrid of the two. These software-based solutions involve the use of encryption algorithms, private and public keys, and digital signatures to form software packets known as Secure Electronic Transaction used by Mastercard and Pretty Good Privacy. Hardware-based solutions such as the Smartcard and the MeChip provide better protection for the confidentiality of personal information. Software-based solutions have the advantage over hardware-based solutions in that they are easy to distribute and are generally less expensive. In today's highly technological world, the machine that destroys paper money and converts it into electronic money is not far from reality. In fact the person interacting with his or her banking account late at night is becoming more of a reality. The information superhighway has found its way into many homes, schools, businesses, and institutions. People buy and sell goods on this new media. Consequently, many businesses are reaching out to customers worldwide using the Internet as its communication channel. This new electronic media of interaction has grown to be known as the electronic commerce. “Electronic Commerce integrates communications, data management, and security services, to allow business applications within different organizations to automatically interchange information.” Consequently, electronic commerce is comprised of interconnected communications networks; advanced computer hardware and software tools and services; established business transaction, data exchange, and interoperability standards; accepted security and privacy provisions; and suitable managerial and cultural practices.

Electronic banking is a new industry which allows people to interact with their banking accounts via the Internet from virtually anywhere in the world. The electronic banking system addresses several emerging trends: customer demand for anytime, anywhere service, product time-to-market imperatives and increasingly complex back-office integration challenges. This system allows consumers to access their banking accounts, review most recent transactions, request a current statement, transfer funds, view current bank rates and product information and reorder checks. Some of the banks that are currently offering this service are Bank of America, Centura Bank, Citibank, Nations Bank, ABN AMRO. The e-banking system can be seen as an “extension of existing banks”, catering to a large population of Internet users.

LITERATURE REVIEW

Aderonke and Charles (2010) found that “Banks’ customers who are active users of e-Banking system use it because it is convenient, easy to use, time saving and appropriate for their transaction needs. Also the network security and the security of the system in terms of privacy are the major concerns of the users and constitute hindrance to intending users.” Haq & Khan (2013) analysed the challenges and opportunities in the Indian Banking sector. The study showed that only 28 per cent banking clients were using internet banking after evaluating the population characteristics. It found that there was no significant relationship in between age and use of cyber banking. Srivastava (2007) analysed the customer‟s perception on usage of internet banking. It also focused on what are the drivers that drive consumers, how consumers have accepted internet banking and how to improve the usage rate. The study revealed that education, gender, income plays an important role in the usage of internet banking. Trivedi & Patel (2013) analysed the problems faced by customers while using e-banking facilities in India and observed that most of the customers know about the e-banking services offered by their bank.

OBJECTIVE OF THE STUDY

In this context, the study revolves around the following objectives -

- Identification of the motivations in E-Banking.
- Highlighting the security issues in E-Banking and measures taken from various banks.
- Analysis of the security issue and concluding remarks

PARADIGM SHIFT FROM TRADITIONAL BANKING TO E-BANKING

The Internet is growing at an exponential rate. The number of internet users worldwide will surpass 3 billion in 2015, according to new figures from e-Marketer, increasing 6.2% next year to reach 42.4% of the entire world's population. his year, the internet will reach more than two in five people in the world for the first time as online audience hits 2.89 billion users globally. By 2018, e-Marketer estimates, nearly half the world's population, or 3.6 billion people, will access the internet at least once each month. As the Internet continues to expand, the convenience associated with electronic banking will attract more customers. In today’s market, according to preliminary data from the latest Federal Reserve survey of patterns of consumer spending, almost four-fifths of consumer expenditures are handled by checks, directly or indirectly.. This means that electronic banking has a very large potential for use since many people expect that electronic checks will substitute paper checks. Moreover, for consumers, electronic money (electronic cash and electronic checks) means greater efficiency than using coins, paper bills, and traditional banks. The electronic banking system brings the convenience of 24-hour, seven days a week, banking by offering home PCs tied directly to a bank’s computers. In addition, electronic money also offers greater security than a paper-and-coin system. Users are able to make a backup copy of their funds and if the electronic money is stolen, the users can invalidate the serial number just as they now stop payment on a paper check.

E-banking has been around for some time in the form of automatic teller machines and telephone transactions. More recently, it has been transformed by the Internet, a new delivery channel for banking services that benefits both customers and banks. Access is fast, convenient, and available around the clock, whatever the customer's location (see illustration above). Plus, banks can provide services more efficiently and at substantially lower costs. For example, a typical customer transaction costing about $1 in a traditional "brick and mortar" bank branch or $0.60 through a phone call costs only about $0.02 online.

E-banking also makes it easier for customers to compare banks' services and products, can increase competition among banks, and allows banks to penetrate new markets and thus expand their geographical reach. Some even see electronic banking as an opportunity for countries with underdeveloped financial systems to leapfrog developmental stages. Customers in such countries can access services more easily from banks abroad and through wireless communication systems, which are developing more rapidly than traditional "wired" communication networks.

E-BANKING SCENARIO IN INDIA

The banking industry in India is facing unparalleled competition from non traditional banking institutions, which now offer banking and financial services over the Internet. Indian banks are going for the retail banking in a big way. Throughout the country, the Internet Banking is in the nascent stage of development (only 50 banks are offering varied kind of Internet banking services). In general, these Internet sites offer only the most basic services. 55% are so called 'entry-level' sites, offering little more than company information and basic marketing materials. Only 8% offer 'advanced transactions' such as online funds transfer, transactions & cash management services · Foreign & Private Banks are much advanced in terms of the number of sites & their level of development. Internet Banking is the new generation of banking in India. Most private and MNC banks have already setup an elaborate Internet banking infrastructure. E-banks can be classified as Fully Traditional banks, traditional banks with Internet presence and fully Virtual banks [Agarwal 2002]. The success of traditional banks with Internet presence is prominent not only in India but also anywhere in the world. India has an extensive banking network, consisting of rural and urban banks. Largely speaking the most of the Indian banks are still public sector banks. New age private sector banks like ICICI, HDFC, UTI are fast becoming choice of citizens in urban areas where technology penetration is high. As banks are going to play a key role in IT enabled public services involving electronic money transactions we feel that cooperative banks should consider NET-Banking in a big way. [MIT 2001]. A cost comparison study done by IBM global services consulting group clearly shows the advantage of using Internet as medium for banking services over other traditional mediums (fig 1). As per the recent survey, traditional banks spend 60% of the revenue generated to run a branch. Whereas, the cost of providing same services via Internet comes out to be only

15%. This is a huge savings for banks and consumer. Definitely the consumer is the principal beneficiary of the Internet Banking. He will be access the same services with more efficiency at low cost. E banking will have two-fold effect, first, it will reach the remote consumer and second it will create the realization among consumer about benefits of investment in different financial products. Investment in-turns boost the financial markets and economy. A research shows that a large urban population use Internet for gathering information about different financial products like personal loan, credit card, insurance etc., thus reducing cost of printing, promotion and distribution.

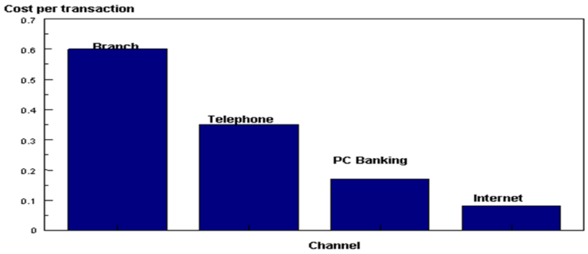

Figure 1: Cost of Internet Banking Over Other Mode of Banking (Source: IBM Globalservices Consulting Group)

SECURITY ISSUE

The trend of growth of E-Banking brings many security issues and increasing cost of implementing higher security system for both e-banking users and the banks. The most critical issue of e-banking security is to protect valuable information that is susceptible to unauthorized access by attackers. Various kinds of security threats and issue are associated for e-banking system, e.g. communication risks, client authentications, and human factors. In fact the attackers can choose to hack the current e- banking systems, e.g. trojan horse, botnets, social phishing and so on. The profit driven attacks activity has risen dramatically at every possible level. The Internet related crimes and the security issues are not only applicable for e-banking but also all server-client Internet applications. Jagtic el at discussed how attackers are using "social phishing" to get uneducated victims financial or personal information.

Banking system intrusion shows the vulnerabilities that exists in financial institution, that have been used by those illegal and unauthorized individuals or groups to intrude an area with secure environment. The violation of system security is all about the money, challenges to intercept data, challenges with acquaintance, data breach, and poor authentication and authorization. Financial industry such as banks plays major role in prepare the people a good service, good system, and the best security systems that can meet customer's expectation and also to attract prospective customers to use trust and using their system to keep their personal data, information and most importantly their money safe. Although there is always vulnerabilities occur around the time, banking system should have a backup plan or other shields in order to handle any malicious behavior, that intend to violate the customer's information. Ways of prevention should be taken care like the one that has being stated in this paperwork. In order to provide effective and secure banking transactions, there are four technology issues needed to be resolved. The key areas are:

- **Security**

The security issue along with the possible attacks may occur due to the insufficient protections. The examples of potential hazards of the electronic banking system are during on-line transactions, transferring funds, and minting electric currency, etc.

- **Privacy**

Generally speaking, the privacy issue is a subset of the security issue. By strengthening the privacy technology, this will ensure the secrecy of sender's personal information and further enhance the security of the transactions. The examples of the private information relating to the banking industry are: the amount of the transaction, the date and time of the transaction, and the name of the merchant where the transaction is taking place.

- **Authentication**

Encryption may help make the transactions more secure, but there is also a need to guarantee that no one alters the data at either end of the transaction. There are two possible ways to verify the integrity of the message. One form of verification is the secure Hash algorithm which is "a check that protects data against most modification." The sender transmits the Hash algorithm generated data. The recipient performs the same calculation and compares the two to make sure everything arrived correctly. If the two results are different, a change has occurred in the message. The other form of verification is through a third party called Certification Authority (CA) with the trust of both the sender and the receiver to verify that the electronic currency or the digital signature that they received is real.

- **Divisibility**

E-banking increases security risks, potentially revealing up till now isolated systems to open and risky environments. Security breaches essentially fall into three categories; breaches with serious criminal intent (fraud, theft of commercially sensitive or financial information), breaches by 'casual hackers' i.e., defacement of web site s or 'denial of service' [4] causing web sites to crash, and flaws in systems design and/or set up leading to security breaches (genuine users seeing / being able to transact on other users' accounts). All of these threats have potentially serious financial, legal and reputational implications. Many banks are finding that their systems are being probed for weaknesses hundreds of times a day but damage/losses arising from security breaches have so far tended to be minor. However some banks could develop more sensitive "burglar alarms", so that they are better aware of the nature and frequency of unsuccessful attempts to break into their system.

The most sensitive computer systems, such as those used for high value payments or those storing highly confidential information, tend to be the most comprehensively secured. One could therefore imply that greater the potential loss to a bank the less likely it is to occur, and in general this is the case. However, while banks tend to have reasonable perimeter security, there is sometimes insufficient segregation between internal systems and poor internal security. It may be that someone could breach the lighter security around a low value system. It is easy to over emphasis the security risks in e-banking. It must be remembered that the Internet could remove some errors introduced by manual processing (by increasing the degree of straight through processing from the customer through banks' systems). This reduces risks to the integrity of transaction data (although the risk of customers incorrectly inputting data remains). As e-banking advances, focusing general attention on security risks, there could be large security gains.

E-BANKING SECURITY MEASURE

Some of the banks are already taking necessary steps from various security threats to protect their customers' personal information. Although many banks have their own technology and online banking guarantees, there are several measures that virtually every bank takes to ensure that their customers have a safe, secure online banking experience. Some of the measuring actions are taking by various banks are discussed as follows.

- **Anti-Virus Protection:** By using up-to-date anti-virus protection, banks can help detect viruses and prevent them from spreading.
- **Firewalls:** By helping banks block unauthorized access to individuals or networks, firewalls help create a more secure online banking environment.
- **Secure Socket Layer (SSL) Encryption:** This creates a secure connection with your browser when you log in, fill out an application, register for services and more. And although the technology is sophisticated, it's easy to make sure that SSL encryption is active on the page you're using. Just look for the lock symbol at the lower right-hand side of the page or look for **"https://"** at the beginning of the pages URL
- **Cookies:** By placing a cookie (a piece of text stored on a user's computer by their web browser) on the computer after customer’s initial login, banks can then recognize or authenticate customr’s computer when he login to his account again. If user uses a new computer to login to his account or want to erase cookies he will be required to enter additional information at the time of he next login.

HSBC Bank in India ensures security by Multi-layer logon verification i.e., customr’s financial information is protected by a sophisticated combination of a unique Username and Password, and a one-time Security Code generated by Online Security Device. When customer transfer money or pay bills online, HSBC prompts for the Security Code generated by your Online Security Device. This ensures that only customer can authorize payment and transfer requests.HSBC uses 128 bit Secure Socket Layer (SSL) Encryption for information transmitted during an Internet Banking session, which is accepted as the industry standard for encryption. As a security measure, Internet Banking session will automatically shut-down or time-out, out after a period of not being used.

SECURITY ANALYSIS

- **Cost of Attacks**

Banks must constantly increase security. At the same time, the banks must manage costs to make a profit. In contrast, increasing security is increasing the cost for attackers to break into the system, and increasing the punishment that the attackers may suffer. Hence the Internet criminals/attackers/crackers may lose motivation for hacking a high security Online Banking system. According to Lampson’s concepts, there is no absolute security. From attackers’ point of views, security is actually about cost for attackers to break into a certain environment/system/platform including time, money, and punishment. this attack scenario, the potential punishment that the attackers could face is actually rather low. In terms of risk analysis, this threat is highly dangerous and the possibility of the potential attacks is also high.

- **Cost Verse Profit for the Banks**

Security experts differ on specifics but agree on cost for implementing security. Security costs lots of money not only for banks but also for many companies, organizations and government. In this case, the authors only looked at this threat from customers’ point view. They overlooked banks’ point of views. Lampson believed although many companies have leant about inadequate security, they won’t spend much money on security. Lampson said “practical security balances the cost of protection and the risk of loss, which is the cost of recovering from a loss times its probability”. Today, the most important issue associated with the growth of E-Banking is security the protection of the valuable information is susceptible to unauthorized access by hackers. At the same time, banks must manage costs to make a profit. The banks could guess the possible loss for some risks is fairly low, compared with the investment of implementing high security.

- **Trustworthy Environment**

Security experts like Lampson and Claessens use different species but they both agree the trustworthy environment platform is important for a security system. However, based on Lampson's trust of chain model, without a trustworthy environment and secure communication channel, any link between the legitimate clients and the banks are still vulnerable. The trustworthy environment should be resistant to the phishing attacksand also social engineering or man-in-the-middle attacks.

CONCLUSIONS

E-banking allows customers or users to conduct financial transactions on a secure website operated by their banks, credit unions or building societies. While electronic banking can provide a number of benefits for customers and new business opportunities for banks, it exacerbates traditional banking risks. In the new age of the Internet and online payment solution systems, individuals are often concerned with the issue of how to beware of online payment security issues. These issues can be tough to understand as well as absorb in a short amount of time. E- banking security issues have become one of the most important concerns of the banks. Banking frauds are main reason for the people or potential customers tend to avoid online banking, as they perceive it as being too vulnerable to fraud. A simple solution that consumers can look for to assure them that they are not being taken advantage of is to always look for identification that identifies the website that they are on is a safe and secure payment solutions program. These security verification symbols can be readily identified on websites and are often located on the first page of a website to let a consumer know that the site has a safe and secure payment solution. There is still a need to establish greater harmonization and coordination at the international level. Moreover, the ease with which capital can potentially be moved between banks and across borders in an electronic environment creates a greater sensitivity to economic policy management. To understand the impact of e-banking on the conduct of economic policy, policymakers need a solid analytical foundation.

REFERENCES

1. B. Lampson, "Computer Security in the Real World", IEEE Computer 37:6,37-46, June 2004.
2. C. Grier, S. Tang, S. King, “Secure Web Browsing with the OP Web Browser”, in IEEE Symp. on Security and Privacy (SP 2008), pp. 402-416, 2008.
3. David H. Freedman. “How To Hack A Bank.” ,Forbes ASAP, 2000.
4. David Moore, Geoffrey M. Voelker and Stefan Savage, “Inferring Internet Denial-of-Service Activity”, Proc. USENIX Security Symposium, Washington D.C, 2001.
5. D.Harley, , R.Slade, , U.Gattiker, , “Viruses Revealed”, McGraw-Hill, 2001.
6. J. Claessens, V. Dem, D. Cock, B. Preneel, J. Vandewalle, “On the Security of Today's On-line Electronic Banking Systems”, Computers & Security 21(3), pp. 253-26 5, 2002
7. K.J.Hole,; V. Moen, T.Tjostheim, , Case study: Online Banking security, Security & Privacy, IEEE Volume 4, Issue 2, March-April 2006 Page(s):14 - 20

8. Larry Rogers, “What is a Distributed Denial of Service (DDoS) Attack and What Can I Do About It?”, CERT Carnegie Mellon University, 2004.

9. O.Susan, “DDoS Threatens Financial Institutions”, Reymann Group Inc., 2005.

10. P. Gühring, “Concepts against Man-in-the-Browser Attacks”, 15 pp., web manuscript, published circa January 2007.

11. R.A.Grimes, , “Malicious Mobile Code – Virus Protection for Windows”, O'Reilly Media In c., Sebastopol, CA, 2001.

12. S.Mark, K.David, “Credit card breach affect Conn. banks and credit unions”, Waterbury Republican-American (Connecticut), 2009.

13. S.Marsia, , Information Security magazine, 2009.

14. T. Jagatic, N. Johnson, M. Jakobsson, F. Menczer, "Social Phishing", Commun. ACM 50(10), pp. 94-100, October 2007.