Cyber Cracy Security System for Improper Indian Banking Websites

Dr. Ashvine Kumar[1], Ms. Priyanka[2]
Research guide, Associate Prof., Hindu Institute of Management in Sonipat[1]
Research Scholar, Mewar University, Chittorgarh, (Rajasthan) [2]

Abstract

Cyber security and infrastructure protection can only be achieved by understanding the behavior and techniques of attackers and building defenses based on this knowledge. Hackers and cyber defenders as terrorists possess the same resources and skills in the cyber arms race can be won. Banking in India originated in the last decade of the 18th century. Since that time the banking sector applying different ways to provide facilities and securities to a common man regarding to money. Particularly on security issues in the banking sector plays a very important role in the implementation of technologies. The banking sector is at the core of who comes to cyber security becomes more important on that front. After the arrival of Internet and World Wide Web communicating banking sector is totally change specially in terms of security because now money is in your hand on a single click. Now users with different kinds of ways is the number of options to manage your money. In this paper an attempt to cyber crime security mechanisms put forward on issues of Indian banks have websites.

Key words:- Cyber defense ,Mechanism, Encryption

Introduction

Cyber cracy mechanisms against unauthorized access or attack a computer or computer system (Internet) on the measures taken to protect. It is related to the security of computer systems and networks and is applied to the computer. In the world of banking, information technology development and more flexible payment methods and more user-friendly a huge impact on the development of banking services. Internet banking, access their bank accounts and banking transactions, including consumer Internet access. At the basic level, Internet banking to provide information about their products and services, a bank may set up a web page. At an advanced level, it involves provision of facilities such as accessing accounts, transferring funds, and buying financial products or services online. This is called “transactional” online banking. In spite of the great benefits of the online banking, it is extremely essential that banks regard the risks associated with it. One significant step that banks must take before going through any transformation is to insure the proper handling of online banking risk. To use the online banking customers and banks to determine the best method but it is very difficult. Crime is a social and economic phenomenon and is as old as human society. Crime is a legal concept and has the sanction of law. Crime or misdemeanor "criminal proceedings which may result in punishment that can be followed by a legal inaccurate". Is a declaration of guilt, it is a violation of criminal law. Per Lord Atkin "the criminal quality of an act is any standard, but can not be discovered by the context: is the act prohibited with penal consequences". Cyber-crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illegal activity. Cyber-crime is the latest and perhaps the most complicated problem in the cyber world. Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber-crime. Cyber-crimes are computer related as well as computer generated crimes which are increasing day by day.

Defending a computer system against malicious attack depends on making many different cracy mechanisms work together. In addition to protecting against intrusions, these mechanisms should provide intrusion detection and response. The semantics of input and output for these mechanisms - what the alert from an intrusion detector means, and the implications of issuing a command in response - can vary greatly from one mechanism to another. In this paper, the authors discuss the abstract interface they have developed for integrating various cracy mechanisms to defend a distributed application. Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by illegally as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. A phishing technique was described in detail in 1987, and the first recorded use of the term "phishing" was made in 1996. The term is a variant of fishing probably influenced by breaking and alludes to "baits" used in hopes that the potential victim will "bite" by clicking a malicious link or opening a malicious attachment, in which case their financial information and passwords may then be stolen. Not all phishing attacks require a fake website. Messages that claim to be from a bank, tell the users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phisher, and provided by a Voice over IP service) was dialed , it prompts the user to enter the account number and PIN. Phishing (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls is from a trusted organization.

Research Objectives

The present study Objective:

1. To determine the issues of effectiveness and secureness for banking.
2. To describe cyber crime cracy mechanism for banking industries.
3. To indentify the status of Indian banks.

Review of Literature

Study Related Technology

Raja et al. (2008) evaluated the impact of e-payment system on the business opportunities. They identified that due to the growth of internet users, various electronic payment mechanisms had been developed to cater the diversity of applicants. The researchers classified the e-payments into three main groups, namely, cash like systems, check like systems, and hybrid systems which were further classified into credit cards, debit cards and electronic cheques . They identified three main issues related to e-payment that were security issues, low interest among businessmen, and heavy reliance on traditional payment methods. They also analyzed that there were technical and
cultural problems which hinder the path of e-payments. However, to make e-payments more effective, security threats should be reduced; and people should be realized that traditional payment methods were more time consuming than electronic payment methods. They should also be realized that plastic card payments were more convenient, easier and more secure than cash or cheques.

Sarangapani and Mamtha (2008b) studied the impact of Information Technology on banking sector and its security related aspects. Due to recent developments in banking industry and with introduction of Basel-I and II implementation; customers are more demanding now and it requires innovation in banking services. The researchers found that now the banking industry has been more customer-oriented with unlimited market place, extensive product breadth and e-enabled services provided to the customers. The IT initiatives in banking industry have resulted

into reduction of time. Introduction of negotiated dealing system, screen based trading and RTGS for online settlement of inter-bank transfers of fund had also resulted into safe, secure and quick movements of funds. The authors also studied e-security aspects of banking which pose damage and threat to the existing e-banking system. It includes unauthorized access to computer system or network, stealing information, e-mail bombing, data diddling, denial of service, viruses, etc. The authors concluded that existing legal framework was adequate to meet the challenges of e-banking; and it had become essential to create awareness of e-banking among customers, banks and society. Different attempts have been made by the researchers to give a close look to the concept of electronic banking. The review of literature provided that e-banking services have a negative impact on banks' profitability in the short run because of increased capital costs on account of technical and electronic infrastructure, training their employees and also to create the environment where the banks can electronically operate smoothly. However, these services have a positive impact on the profitability of banks in the long run. Despite the increasing importance of E-banking services, the research pertaining to E-banking in Indian context has been limited. While concluding, it can be said that e-banking services are complementary to the existing branch network and not a substitute to it.

Studies related to banks:-

Ramani (2007) studied the impact of e-payment system on Indian banking sector. E-payment was required for handling large volume of business payment and remittances for hassle free, quicker and faster payment remittances at low cost, and paperless transactions. The researcher highlighted various steps taken by RBI for the e-payment. It includes RTGS, deferred net settlement system such as electronic clearing services debit and credit, electronic fund transfer and NEFT. The researcher studied that these methods had increased the use of core banking solutions, data warehousing and data mining. E-payment had reduced the chances of fraud, improved customer service by cutting the delay in payment obligation.

Suresh (2008) highlighted that recently developed e-banking technology had created unpredicted opportunities for the banks to organize their financial products, profits, service delivery and marketing. The objectives of the study were to evaluate the difference between traditional and e-banking, and to identify the core capabilities for the best use of e-banking. The author analyzed that e-banking will be an innovation if it preserved both business model and technology knowledge, and disruptive if it destroys both the model and knowledge. He also differentiated e-banking from traditional banking in five ways, namely, value proportion, market scope, cost structure, profit potential and value network. However, in order to exploit technical and business capabilities of e-banking, banks should generate more customers inside and outside India so that more revenues could be generated that lead to better future of Indian economy.

Studies Related To E-Banking Security:-

Several researchers using diverse classification techniques have defined security being a complex concept. *Belanger et al. (2002)* define security as the protection against security threats. Along with that, *Grabner-Krautera and Kaluscha (2003)* postulate that, security assures the protection of the two vulnerable points in e-commerce systems, which are the uncertain underlying technological infrastructure and the unreliable users of the system. *Kesh et al. (2002)* gave a broader definition of the term security wherein they argue that security cannot be defined only as technological measures but to include several non-technical mechanisms such as policies, strategies, information listed on websites and so on. *Oscarson (2003)* argue that security is primarily composed of a set of security primitives or objectives that are aimed at protecting the systems and/or users against threats. The primary goals of security are Confidentiality, Integrity, Availability, Authentication Authorization, Non-repudiation and Privacy *(Kesh et al., 2002).* These goals are explained below.

According to *Suh and Han (2003)*, confidentiality ensures that the communication between the user or customer and the service provider is not accessible to other parties. Along with that, *Knorr and Röhrig (2000)* claim that unauthorized access of information should be prevented. The second security goal is integrity. According to *Grandison and Sloman (2000)*, integrity means that during and after information exchange, the content should remain unchanged and should be tamper free. Further to that, *Ally and Toleman (2005)* indicate that, integrity ensures that content is not created, modified, intercepted or deleted by unauthorized people. The third security goal is availability, which according to *Maijala (2004)* means that the information required by users should be accessible when required by them.

In addition to the above threats, *US-CERT (2006)* identifies pharming and malware as other e-banking security threats. Additionally, *Schneier (2005)* claim that, instead of targeting heavily invested bank's internal systems, the attackers are now targeting the end users' PCs, which are the weakest link in the network, through various ways such as phishing, key-logger and Trojan horse attacks. *Ganesan and Vivekanandan (2009)* cite phishing and pharming as the two well-known examples e-banking threats.

In a study by *BITS (2003)*, it was established that there are three common forms of internet banking fraud namely identity theft, friendly fraud or fraud committed by a trusted relative or friend and internal fraud which is perpetrated by a financial institution employee. Furthermore, *BITS (2003)* notes that, there two major threat types which are application and network-based threats. With application threats, the fraudster appears to be a legitimate user of the online banking application, but is instead conducting illegal activities. Security measures such as firewalls, proxy servers, network filters and similar products cannot protect a bank from application-based threats. On the other hand Network-based threats, such as hacks, site-defacement attacks, denial-of-service attacks, and viruses and worms attack the core network and infrastructure but don’t directly try to carry out transactions. Tools such as firewalls can counter these attacks.

Risks, Effectiveness and Secureness for Banking:

The risks of visiting malicious, criminal or inappropriate websites include:

- Viruses and spyware (collectively known as malware).
- Phishing, designed to obtain your personal and/or financial information and possibly steal your identity.
- Fraud, from fake shopping, banking, charity, dating, social networking, gaming, gambling and other websites.
- Copyright infringement – copying or downloading copyright protected software, videos, music, photos or documents.
- Exposure to unexpected inappropriate content.

When you use the internet, your browser (for example Internet Explorer, Opera, Chrome, Safari or Firefox) keeps a record of which sites you have visted in its 'history'.When you use the internet, the websites you visit are visible to your Internet Service Provider and browser provider, and it is possible that records are kept.

In order to provide effective and secure banking transactions, there are four technology issues needed to be resolved. The key areas are:

1. Defensive:- Security of the transactions is the primary concern of the Internet-based industries. In the absence of security, such as the example illustrated in the first section Citibank may cause serious damage. Next to the issue of security attacks due to inadequate safety will be discussed in the next section. The examples of potential hazards of the electronic banking system are during on-line transactions, transferring funds, and minting electric currency, etc.

2. Privacy:- Privacy issues generally, speaking a subset of the security issue and thus will be discussed in a later section of privacy technology. By strengthening privacy technology, to ensure the privacy of personal information of the sender and will further enhance the security of transactions. Examples of personal information relating to the banking industry: transaction amount, date and time of the transaction, and the transaction is the name of the trader.

3. Certification:- Encryption may help make transactions more secure, but there is a need to guarantee transaction no change on either end of that data. To verify the integrity of the message are two possible ways. Is a form of verification that is secure hash algorithm "that protects data against the amendment an investigation." Senders transmit data generated hash algorithm. 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.

4. Severability: Electronic money exchange similar to real money that can be divided into different units. For example, electronic money and money is needed to account for nickels.

Cyber Crime Cracy Staretgy Mechanism for Banks

Cyber criminals are no different than traditional criminals in that they want to make their money as quickly and easily as possible. Cybercrime prevention can be achieved fairly quickly and in a cost-effective manner. When armed with a little technical advice and common sense, many cybercrime attacks can be avoided. Similar to target hardening for a residence or a business (e.g.,lights, locks, and alarms), the more difficult it is for a cyber criminal to successfully attack a target, the more likely he or she is to leave it alone and move on to an easier target.

The following ten tips are basic ways that cybercrime can be prevented.

- *Keep the computer system up to date-* Cyber criminals will use software flaws to attack computer systems frequently and anonymously. Most Windows based systems can be configured to download software patches and updates automatically. By doing this, cyber criminals who exploit flaws in software packages may be thwarted. This will also deter a number of automated and simple attacks criminals use to break into your system.

- *Secure configuration of the system*- It is important that computers are configured to the security level that is appropriate and comfortable for the user. Too much security can have the adverse effect of frustrating the user and possibly preventing them from accessing certain web content. Using the “help” feature of the operating system can often address many of the questions in this area.
- *Choose a strong password and protect it*- Usernames, passwords, and personal identification numbers (PIN) are used for almost every online transaction today. A strong password should be at least eight characters in length with a mixture of letters and numbers. Using the same password for various sites or systems increases the risk of discovery and possible exploitation. It is never a good practice to write a password down and leave it near the system it is intended to be used on. Changing a password every 90 days is a good practice to limit the amount of time it can be used to access sensitive information.
- *Keep your firewall turned on*- A firewall helps to protect your computer from hackers who might try to gain access to crash it, delete information, or steal passwords and other sensitive information. Software firewalls are widely recommended for single computers. The software is prepackaged on some operating systems or can be purchased for individual computers. For multiple networked computers, hardware routers typically provide firewall protection. (www.fbi.gov/scams-safety/, How to Protect Your Computer, www.fbi.gov/ scams-safety/computer_protect)
- *Review bank and credit card statements regularly*- The impact of identity theft and online crimes can be greatly reduced if you can catch it shortly after your data is stolen or when the first use of your information is attempted. One of the easiest ways to get the tip-off that something has gone wrong is by reviewing the monthly statements provided by your bank and credit card companies for anything out of the ordinary. Additionally, many banks and services use fraud prevention systems that call out unusual purchasing behavior (e.g., if you live in Texas and all of a sudden start buying refrigerators in Budapest). In order to confirm these out of the ordinary purchases, they might call you and ask you to confirm them. Don't take these calls lightly--this is your hint that something bad may have happened and you should take action. Follow the steps outlined in "What to Do If You're a Victim."

Status of Indian Banks Websites

In this paper we take five Indian banks and try to find out the security features using by the bank for online transactions. The data is collected by various reports from web, newspaper and media. For every security feature we provide 5 points. The banks are-

- State Bank of India (SBI)
- Punjab National Bank [PNB]
- Central Bank of India [CBI]
- Bank of Baroda [BOB]
- Allahabad Bank
- Canara Bank

TABLE 1. POINT TABLE

Bank	PE*	VK*	SSL*	UAP*	SMS*	TOTAL
SBI	4	4	3	0	3	15
PNB	4	4	4	0	4	15
CBI	3	4	2	0	2	12
BOB	4	4	4	0	4	15
ALLAHABAD	3	4	3	0	3	14
CANARA	4	4	2	0	2	12

*PE- Password Encryption, *VK- Virtual Keyboard, *SSL Secure Socket Layer, *SMS- Short message service alerts, *UAP- User Awareness Program

(Sources:- (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.10, 2011)

The study for all of us, being implemented as equal banks found their websites. Encryption virtual keyboard with the password. The banks are safe use SMS Alerts and socket layer information in respect of facilities to provide customers money transaction . We provide 5 marks for each feature but no bank got full 5 mark for any feature and the aggregate total of every bank is vary 12 to 15 out of 25.

Reasons for Cracking and Responsibilities:-

The reason behind this is that they all have little bit loop wholes on all the security features but the biggest reason are:-

1. User awareness feature.

2. Lack of knowledge
3. Improper languages to teach
4. Complexity of codes
5. Accessibility of viruses
6. Negligence

Responsibilities of Banks for Customers:-

- What is the meaning of using virtual keyboard
- What is the meaning of strong password
- What is the meaning of SMS alerts
- Don’t access net banking account from cyber café or public computer.
- Use a single computer as far as possible.
- Login net banking site by directly typing site name. Don’t click any link, if that link takes you to login page, close the page, and start over.
- Bank or its representative never asks for password and username over telephone.
- Viruses come with some time SMS alerts, SMS alerts when either secured or not the bank's responsibility to check.
- Change the password after 6 months.
- Remember the id and password, don’t write it anywhere.
- Don’t give any of the personal information to any web site that does not use encryption or other secure methods to protect it.
- Don’t share any information to any one regarding to account
- Install good antivirus programme on the system and regularly update the programme.
- Maintain the equilibrium between usability, productivity and security.

Conclusion

This paper describes about the different Cyber cracy mechanism being used by the nationalized banks for online transaction and examine where the problem is in the system. It is found that most of the Indian banks use the latest technology for the online security feature but still they have small loop whole in their features. In order to reduce the potential vulnerabilities regarding to the security, many vendors have developed various solutions in both software-based and hardware-based systems. Generally speaking, software-based solutions are more common because they are easier to distribute and are less expensive. In order for electronic banking to continue to grow, the security and the privacy aspects need to be improved. With the security and privacy issues resolved, the future of electronic banking can be very prosperous. The future of electronic banking will be a system where users are able to interact with their banks “worry-free” and banks are operated under one common standard. The biggest threat to the online security is the lack of awareness level in the users about the security challenges and banks also don’t have any user awareness program to spread information. Further, most of the users do not use online facilities because they don’t have proper information and the reason behind all this is the same, which is the lack of awareness. It is also correct to say that the user also have to increase their awareness level because this is not only the responsibility of the banks but also it is for the benefit of the user. In future these technologies will increase rapidly and user will have to use these facilities so it is the requirement of the time that the user as well as the bank should make this system more secure.

References

1. Emerging electronic methods for making retail payments. June 1996.
2. Pfleeger, Charles P. Security in Computing. Prentice Hall, 1997.
3. Duggal Pawan- Cyber Crime.
4. "Phishing, n. OED Online, March 2006, Oxford University Press.". Oxford English Dictionary Online.
5. About Encryption. Http://www.tropsoft.com:80/tropsoft/aboutenc.htm
6. Bank Net Electronic Banking Service. Http://mkn.co.uk/bank
7. Basic Flaws in Internet Security and Commerce.
8. Http://HTTP.CS.Berkeley.EDU/~gauthier/endpoint-security.html
9. Basic Reflections On Security. Http://www.esd.de/eng/secu/secu.htm#10
10. Belgian Banks Put Their Money On a Security Solution From Utimaco.
11. Http://www.mergent.com/html/electronic_banking.html
12. Big Blue Goes E-Banking. Http://iw.com/1996/12/news.html#bigblue
13. Electronic Banking. Http://www.electrobank.com/ebaeb.htm
14. ElectronicBanking Resource Center-www2.cob.ohiostate.edu/%7Erichards/bankpay.html
15. Internet Security. Http://cfn.cs.dal.ca/Education/CGA/netsec.html

16. 2010 Internet Crime Report, Internet Crime Complaint Center, 2011 www.ic3.gov/media/annual report/2010_IC3Report.pdf
17. Cyber Investigations, Federal Bureau of Investigation, 2010 WWW. Fbi . gov /cyber invest /cyber home.html
18. Gordon M. Snow, Assistant Director, Cyber Division, Federal Bureau of Investigation Statement before the Senate Judiciary Committee,
19. Subcommittee on Crime and Terrorism, Washington, DC, April 12, 2011 www.fbi.gov/news/ testimony/cybersecurityresponding-to-the-threat-of-cybercrime-and-terrorism
20. EP 0554492 Hans E. Korth: "Method and device for optical input of commands or data" filing date 07.02.1992
21. T. Dierks, E. Rescorla (August 2008). "The Transport Layer Security (TLS) Protocol, Version 1.2"
22. GSM Doc 28/85 "Services and Facilities to be provided in the GSM System" rev2, June 1985
23. A Times: Why text messages are limited to 160 characters SM 03.40 Technical realization of the Short Message Service (SMS)