Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 1; January-March, 2015 pp. 48-52

http://www.krishisanskriti.org/acsit.html

Risks Involved in E-banking and their Management

Syed Masaid Zaman[1] and Qamar Parvez Rana[2]

[1]Department of Engineering & Technology Shrivenkateshwara University Gajraula, Amroha (UP) India-244236
[2]Course Director CCNA Jamia Hamdard (Hamdard University) New Delhi–110062, India
E-mail: [1]smasaidd@gmail.com, [2]qprana@jamiahamdard.ac.in

Abstract—*The wide development of the Internet technology is creating the opportunity for organizations to extensively utilize computer systems for the delivery of services. The emergence of new business models which rely on electronic payment systems, creating a new threat and vulnerability which leads to risk. This paper deals with the formal classification of attacks and vulnerabilities that affect current internet banking systems. In recent years the number of malicious applications which are used to target online banking transactions has increased dramatically. This represents a challenge not only to the customers who uses electronic payment systems, but also to the organizations which provide these facilities to their customers. This paper makes an attempt to explore empirically the details of E-Banking. In this study different types of risks have been indicated and therefore vulnerabilities and mitigation methods have been suggested to solve those risks in E-Banking. Modern security management methods now acknowledge that most risks cannot be completely eliminated and that they need to be managed in a cost effective manner. This paper will focus on the development of a methodology for the assessment and analysis of threat and vulnerabilities within the context of a security risk management.*

Keywords*: risk management, vulnerabilities, mitigation methods, E-banking.*

1. INTRODUCTION

E-banking or internet banking is the term that signifies and encompasses the entire sphere of technology initiatives that have taken place in the banking industry. As the name suggests E-banking, E stands for electronic and banking is the term which we all know, it means that it involves the electronic technology. The means of technology used in E-banking are electronic channels which includes telephone, mobile phones, internet etc. which are used for delivery of banking services and products. The concept and scope of electronic banking (e-banking) is still in the transitional stage. E-banking has broken all the barriers of branch banking. In this modern world of technology most of the banking happens while you are sipping coffee or taking an important call. Electronic banking services like ATMs are available at your doorsteps. Banking services are accessible round the clock for all the seven days of the week. This tremendous change happens only due to advent of IT. Due to the adoption of IT in banking services, banks today operate in a highly globalized, liberalized, privatized and a competitive environment. E-banking means that any user can get connected to his/her bank's website to perform any of the virtual banking transaction with a personal computer or mobile phone. Currently there is a clear need of efficient security models to banks which offer online access to their banking systems. E-banking services reduce the gap between the difficulties in customer understanding of the banking transactions and their participation in improving the sophistication of these services. E-banking leads to having a competitive advantage in the different levels.

2. TYPES OF ATTACKS AND RISKS IN E-BANKING

There are main four types of attacks in e-banking which are as under:

- Online line attacks
- Local attacks
- Remote attacks
- Hybrid attacks.

Types of online Attacks

Due to the advent of IT all things became easy on one side. On the other side the risk of online attacks also increases. Now Banks and service providers need to provide security against various types of online attacks. The object of an attack may vary. Attackers may try to exploit know Vulnerabilities in particular operating systems. They also may try repeatedly to make an unauthorized entry into a Web site during a short time frame thus denying service to other customers. We can categorize the attacks into three main groups:

3. LOCAL ATTACKS

Every common user always made mistakes by believing that their online banking session is perfectly safe when they use an SSL (Secure Sockets Layer) connection by third-party users. Security experts continually state that everything is safe if there is a yellow padlock symbol in the browser window. This is true, but the user realizes that SSL was designed to secure the channel from the user machine to the bank computer and not the end points themselves. Whatever is done with the data before the start point and after the end point of the SSL

channel is completely out of the SSL encryption context. The Trojan drops a dynamic link library (DLL) and registers its CLSID as a browser helper object in the registry. Thus the Trojan is able to intercept any information that is entered into a web page before it is encrypted by SSL and sent out. This functionality can also be performed by injecting the Trojan directly into the web browser's memory space, which can often bypass desktop firewalls while making outgoing connections. Other local attack methods include monitoring all network traffic, running a layered service provider (LSP), writing its own network driver, or displaying a carefully developed duplicate copy of a website on top of the official website. The user believes that the opened Web site is the real bank site. The URL in the address bar is not spoofed and even the yellow SSL padlock reveals the correct certificate details, if any user should ever take the time to verify it. Only the overlaid fake password prompt is not part of the original web site and of malicious intent. For better security use of non-static user credentials a user name and a static password are simply no longer enough to protect online banking sessions. Some companies are already responded to these threats by introducing dynamic passwords including RSA secured ID tokens or one-time passwords on paper lists called transaction umbers (TAN).

4. REMOTE ATTACKS

Phishing
An e-mail is sent to the user by attacker. Usually, these e-mails claim to come from a legitimate organization such as a bank or online retailer. The e-mail requests the user to update or to verify his/her personal and financial information which includes date of birth, credit card numbers, login information, account details and PINs etc. The e-mail which is sent to the user contains a link that takes him/her to a spoof (duplicate) website that looks identical (or very similar) to the organization's genuine site. The attacker can then capture personal data such as passwords and other financial details. By clicking on the link provided by the attacker may also download malware onto your computer. By the malware your future use of the internet may be recorded and forward to the attacker. The attackers will then use this information to attack bank accounts, credit cards etc. of the users.

Pharming
After phishing started a "ph-fashion" another slightly advanced technique appears that is pharming. It is same as by phishing (stealing PINs, Passwords, Credit card numbers etc). Attacker creates false websites in the hope that people will visit them by mistake. Users can sometimes do this by mistyping a website address – or sometimes a attacker can redirect traffic from a genuine website to their own. The 'pharmer' or attacker will then try to obtain your personal details when you enter them into the false website.

Malware attacks
Short form of 'malicious software', this is designed to access your computer system without your consent. The term covers a variety of interfering software/programs which includes viruses, worms, Trojan horses and spyware. Attackers try to send the malware through attachments and try to trap you by sending false emails with attachments suggesting you to update your account information.

Voice-over-IP
VoIP (voice over IP) is an IP telephony term for a set of facilities used to manage the delivery of voice information over the Internet. Voice over IP involves Sending voice information in digital form in discrete packets rather than by using the traditional circuit-committed protocols of the public switched telephone network. Major advantage of VoIP and Internet telephony is that, it avoids the tolls charged by ordinary telephone service.

Traditionally the phone service has been a trustworthy source. With caller ID the number can be traced easily. Phreaking and other attacks were possible but they were quite difficult and specialized. With the advent of voice-over-IP and gateways from IP telephony to the public switched telephone network associating a number with a real person has become a whole lot harder. There can be a much more convoluted trail between a VoIP connection and a real person and caller ID is easily spoofed by an attacker.

Vishing
It is another word for VoIP Phishing which involves a party calling you faking a trustworthy organization (e.g. your bank). It is an attempt by attackers to take confidential details from you Details like user id, login & transaction password, Unique registration number(URN), One time password (OTP), Card PIN, Grid card values, CVV or any personal parameters such as date of birth, mother's maiden name etc. over a phone call.

Man-in-the-middle attacks
This type of attacks was before the computers. This type of attack happens when an attackers inserting themselves in between two parties communicating with each other. These attacks are essentially eavesdropping attacks. VoIP is particularly vulnerable to man-in-the-middle attacks. In these attacks the attacker intercepts call-signaling, Session Initiation Protocol (SIP) message traffic and masquerades as the called party to the calling party, or vice versa. Once the attacker has acquired this position, he/she can hijack calls via a redirection server.

Automated answering systems
Most of the companies including banks are using the automated answering and menu system. On the other hand these types of machines are also used by the attackers to crack the customer's accounts. Combined with VoIP and war-

dialing techniques an attacker can automatically try hundreds of numbers and use an automated system exactly the systems which are using banks, solicits details like credit card numbers in the name of ease of use or security. If any candidate victim has responded to the automated system only once, attackers need to involve a human to interact with the customer. This type of attack is both scalable and affordable.

Keystroke capturing/logging

Anything you type on a computer can be captured and stored. This can be done by using a hardware device attached to your computer or by software running almost invisibly on the machine. Keystroke logging is often used by attackers to capture personal details including passwords. Some viruses are even capable of installing such software without the user's knowledge. The risk of encountering keystroke logging is greater on computers shared by a number of users. An updated antivirus software program and firewall can help you to remove the harmful software before it can be used.

5. HYBRID ATTACKS

Attacks on online banking are increasingly complex; hybrid and cross channel attacks are the newest ways of committing fraud. For the attacker the most successful methods are hybrid attacks that combine strategies from both local and remote attacks. A trivial attack would be if a Trojan executed on the infected machine checked all saved bookmarks for known valuable online services and replaced the URL with a fake one, similar to phishing emails. The obvious flaw in this plan is that the user can see the modified URL if they check the address bar of the browser. So the browser setting needs to be modified y Trojan to not display the address bar or overlay it with a fake pop-up window. Even though this is feasible, because it resides on the same level as basic phishing attacks and can be equally done by remote attacks. The more sophisticated approach of the attacker would be to use all the power they have on the infected machine and altering the hosts file is an obvious place to start. The hosts file gives the possibility to the attacker to redirect certain domains to predefined IP addresses. This technique is used by the Trojan.

Some other types of attacks are:

- **Sniffers**: Also known as network monitors, this is software used to capture keystrokes from a particular PC. This software could capture login ID's and passwords.
- **Guessing Passwords:** Using software to test all possible combinations to gain entry into a network.
- **Brute force** (also known as **brute force** cracking): It is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using **brute force**) rather than employing intellectual strategies.
- **Random Dialing:** This technique is used to dial every number of a known bank telephone exchange. The objective of dialing all the numbers is to find a modem connected to the network and can be used as a point of attack.
- **Social Engineering**: An attacker calls the bank's help desk impersonating an authorized user to gain information about the system including changing passwords.
- **Trojan horse:** A programmer can embed code into a system that will allow the programmer or another person unauthorized entrance into the system or network.
- **Hijacking:** Intercepting transmissions then attempting to deduce information from them. Internet traffic is particularly vulnerable to this threat.

6. TYPES OF RISKS

Credit risk

This is the risk to earnings or capital from a customer's failure to meet his financial obligations. Electronic banking enables customers to apply for credit from anywhere in the world. If banks will intend to offer credit through the internet, it is extremely difficult for them to verify the identity of the customer. Verifying collateral and perfect security agreements are also difficult.

Strategic risk

The strategic risk is defined as a risk related to the possibility of negative financial consequences caused by erroneous decisions, decisions made on the basis of an inappropriate assessment or failure to make correct decisions relating to the direction of the Bank's strategic development. Many senior managers may not fully understand the strategic and technical aspects of Internet banking. With the advent of the technology the competition increases at rapid rate, now need to introduce or expand Internet banking without an adequate cost benefit analysis. The resources and structure of organization may not be able to manage Internet banking.

Transaction risk

Transaction risk or Operational risk is the risk of direct or indirect loss resulting from inadequate or failed internal processes by people and systems or from external events. The main factors of transaction risk involve Inadequate Information Systems, Breaches in internal controls, Fraud, Processing Errors, Unforeseen catastrophes. A high level of transaction risk may occur with Internet banking products if they are not adequately planned, implemented, and monitored by the banks. Banks offering financial products and services through the Internet must be able to meet their customer's expectations. Customers who conduct business over the Internet are likely to have little tolerance for errors or omissions from financial institutions that do not have sophisticated internal controls to manage their Internet banking business.

Information security risk

This is the risk to earnings and capital arising out of slack (lax) information security processes by which institutions are exposed to malicious hacker or insider attacks, denial-of-service attacks, viruses, data theft, data destruction and fraud. The rapid change of technology and the fact that the Internet channel is accessible universally makes this risk especially critical.

Liquidity risk

The uncertainty arising from a bank's inability to meet its obligations when they are due, without incurring unacceptable losses is known as liquidity risk. It also includes the inability to manage unplanned changes in market conditions affecting the ability of the bank to liquidate assets quickly and with minimal loss in value. Electronic banking or Internet banking increases deposit volatility from customers who maintain accounts solely on the basis of rates or terms. The management must therefore be prepared for immediate changes and consequently immediate solutions.

Compliance risk

Compliance risk is the current and prospective risk to earnings or capital arising by violation of laws, prescribed practices, rules, regulations, internal policies, and procedures or ethical standards. This risk also arises in situations where the laws or rules governing certain bank products or activities of the Bank's clients may be uncertain or untested. This risk may lead the institution to fine, civil money penalties, payment of damages and the voiding of contracts. Compliance risk can expose to diminished reputation, reduced franchise value, reduced expansion potential, inability to enforce contracts and limited business opportunities. Banks need to understand and interpret existing laws as they apply to Internet banking and ensure consistency with other channels such as branch banking.

Foreign exchange risk

Foreign exchange risk is the risk of negative effects on the financial result and capital of the bank caused by changes in exchange rates. This arises when assets in one currency are funded by liabilities in another. Internet banking or electronic banking may encourage residents of other countries to transact in their domestic currencies. Internet banking may also lead customers to take speculative positions in various currencies with the ease and lower cost of transacting. Foreign exchange risk increases in higher holdings and transactions in nondomestic currencies.

Interest rate risk

This risk is arising from movements in interest rates (e.g. interest rate differentials between assets and liabilities and how these are impacted by interest rate changes) to earnings or capital. By internet banking a large pool of customers can be attracted towards loans and deposits. Also, given that it is easy to compare rates across banks. Pressure of interest rates is higher, so the banks need to react quickly to the changing interest rates in the market.

This risk is arising from negative public opinion and it is current and prospective risk to earnings and capital. The reputation of banks may be damaged by poor internet banking services (e.g., limited availability, software with bugs, poor response). Customers are less forgiving of any problem and thus there are more stringent performance expectations from the Internet channel. Hypertext links can make a link between bank's sites to other sites and may reflect an implicit endorsement of the other sites.

7. MITIGATION MEASURES

Payments effected through alternate payment products/channels are becoming popular among the customers with more and more banks providing such facilities to their customers. While the move of providing the e-banking facilities to the customers the banks indeed promotes and encourages the usage of electronic payments, it is important that the banks ensure that transactions made through such channels are safe and secure and not easily amenable to fraudulent usage. Cyber-attacks are becoming more unpredictable and electronic payment systems becoming vulnerable to new types of misuse. So, what can banks and financial institutions do to protect their customers from the impact of man-in-the-browser attacks? The authentication measures of the customers fall short in this scenario, so instead financial institutions can mitigate their risk by gaining a better understanding of the activity occurring within the online banking session to determine. A layered approach to online banking fraud monitoring – one that analyzes the login event, the outgoing transaction and risky sequences of events – best positions a financial institution to minimize online banking fraud. All customer interactions can be categorized into event classes that incorporate both monetary and non-monetary actions. These are as follows:

- Payment events—Financial transactions such as bill payment and funds transfers
- Login events—IP address and session ID profiling.
- Password events—Changes in logon passwords.
- Profile events—Changes to customer demographic information (e.g., addresses).
- Payee events—Changes to external payee account details.
- Navigation events—Changes to how a customer navigates an online internet portal.

In isolation, one of these events may not indicate fraudulent activity. When combined, however, they predict strong patterns of criminal intent.

A new industry with a rich variety of vendors came into existence and became a global industry for electronic security. Many types of companies operate in this industry. These companies are involved in every facet of securing the wide

area networks over which financial services are provided. Following is a brief description of the major categories of vendors. Companies involved with active content monitoring and filtering produce tools that examine for potentially destructive content material entering a network. The tools provided by the vendors are used to monitor all content entering a network for malicious codes, such as harmful attributes. The methods like Trojans, worms and viruses are used to deploy an attack once the perpetrator enters the system. Viruses are set of instructions or programs that infect other programs on the same system by replicating themselves. Virus scanners which are also known as utility software's are critical in mitigating these attacks. Vendors of virus scanners provide those utility software's that scans and cleans networks and is periodically updated.

Intrusion Detection Systems Vendors

Companies that produce network intrusion detection systems provide products to monitor network traffic and alert the systems administrator with an alarm when someone is attempting to gain unauthorized access.

Firewall Vendors

A firewall is a network security system that controls incoming and outgoing network traffic based on a set of rules. Firewall is a virtual "security guard" provided by the vendors at the entrance of the customer's facilities. A firewall is a system that implements the access-control policy between two networks. These virtual security guards are created by the vendors to protect a network's integrity.

Penetration Testing Companies

Pentest a short form of penetration test is an attack on a computer system with the intention of finding security weaknesses, potentially gaining access to it. Penetration testing companies simulate attacks on networks to test for a system's inherent weaknesses. They then provide the security to attacks found during the simulation. Vulnerability-based scanning tools provide a current snapshot of a system's vulnerabilities.

Cryptographic Communications Vendors

Vendors who supply this product enable the client company to protect its communications with an encryption envelope. Encryption is a technique which uses complex algorithms to shield messages transmitted over public channels. It provides safe passage to data from source to destination. At the destination the message is decrypted using another algorithm. It is highly recommended for use by mobile workforces and/or large non centralized corporations or institutions.

8. CONCLUSION

The knowledge of the real role of IS in banks would help IS managers in managing information systems by judging the business needs of the IS projects, associated risks, importance and ranking of IS managers in organizational hierarchy, need for innovation and flexibility in IS planning approach, etc. The security models currently used in internet banking systems are strongly based on user identification and authentication methods which are also the components where most Internet banking system vulnerabilities are found. Most of the attacks directed at online banking systems target the user focusing on obtaining authentication and identification information through the use of social engineering and compromising the user's Internet banking access device in order to install malware which automatically performs banking transactions, apart from obtaining authenticated data. By this fact it is indicated that banks should provide security mechanism which should be as user independent as possible. Mitigating the risk of user related information's leaks and security issues affecting the system and leads to fraud.

REFERENCES

[1] Lucas, H C (1994). Information Systems Concepts for Management,San Francisco: McGraw-Hill.

[2] Kulkarni, P G (1997). "Trends and Effectiveness of IT in Banking Sector," in Kanungo, Shivraj (ed.), Information Technology at Work—A Collection of Managerial Experiences, New Delhi: Hindustan Publishing Corporation

[3] HALLER, N. A One-Time Password System (RFC 2289). Internet Engineering Task Force. [S.l.].1998

[4] CAVUSOGLU, Hasan e Cavusoglu, Huseyin. Emerging Issues in Responsible Vulnerability Disclosure. Workshop on Information Technology and Systems (WITS 2004). Barcelona, Spain, 2004.

[5] Threats to online Banking published by virus bulletin, July 2005

[6] O. Dandash, P. Dung Le, and B. Srinivasan, Internet banking payment protocol with fraud prevention, 2007

[7] www.researchmanuscripts.com/isociety2012/6

[8] Abha Singh "E-banking" Edition 2012

[9] 22nd International Symposium on Computer and Information Sciences, Nov. 2013.

[10] www.ijaiem.org/volume2Issue3/IJAIEM-2013-03-15