# Risk Management in E-Banking

K.V.D. Kiran
*Department of Computer Science and Engineering*
*K L University,Vaddeswaram, A.P,India*

Sk.Sharmila
*Department of Computer Science and Engineering*
*K L University,Vaddeswaram, A.P,India*

T.Abhishek
*Department of Computer Science and Engineering*
*K L University,Vaddeswaram, A.P,India*

**Abstract- The wide development of the Internet technology is creating the opportunity for companies to extensively utilize computer systems for the delivery of services. New business models, which rely on electronic payment systems, are emerging and each one is 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. The number of malicious applications targeting online banking transactions has increased dramatically in recent years. This represents a challenge not only to the customers who use such facilities, but also to the institutions who offer them. This paper makes an attempt to explore empirically the details of E-Banking. The study indicates different types of risks, vulnerabilities and mitigation methods 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 concentrate on the development of a methodology for the assessment and analysis of threat and vulnerabilities within the context of a security risk management.**

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

## I. INTRODUCTION

E-banking is a generic term making use of electronic channels through telephone, mobile phones, internet etc. for delivery of banking services and products. The concept and scope of e-banking is still in the transitional stage. E-banking has broken the barriers of branch banking. Today most of the banking happens while you are sipping coffee or taking an important call. ATMs are at your doorstep. Banking services are accessible 24x7. A huge part of this change is due to advent of IT. Banks today operate in a highly globalized, liberalized, privatized and a competitive environment. In order to survive in this environment banks have to use IT. E-banking means any user with a personal computer and a browser can get connected to his bank's website to perform any of the virtual banking positions. Currently there is a clear need for efficient security models by 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.

## II. TYPES OF ATTACKS AND RISKS IN E-BANKING

### *A) TYPES OF ONLINE ATTACKS*

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: local, remote and hybrid attacks. Local attacks happen on the victim's machine, remote attacks don't modify the machine but try to intercept or redirect the traffic of a session and hybrid attacks combine local and remote attacks and are the most powerful.

*B) REMOTE ATTACKS*

Phishing Attacks: An e-mail message from a large online retailer or Internet Bank website announces that your account has been compromised and need to be updated and gives the link to update the same. So you follow a link in the message, if you click on the link it leads to the website that is as similar as original website, it is spoofed login page. If you give the account details that will be redirected to the attacker and it might be misused.

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). The attackers again need to bring the user to the fake site. The redirection is done via e-mail+link. The redirection is done by reconfiguration of some networks settings for that an attacker needs malicious software. In Pharming user sees the correct URL in browser location bar.

Malware attacks: Attackers try to send the malware through attachments , try to trap you by sending false emails with attachments saying to update your account information.

Voice-over-IP: Traditionally the phone service has been a trustworthy source. With caller IDa number could be traced easily to a customer and while phreaking and other attacks were possible, 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. Caller-ID is easily spoofed by an attacker and there can be a much more convoluted trail between a VoIP connection and a real person.

Vishing: Vishing is another word for VoIP Phishing, which involves a party calling you faking a trustworthy organization (e.g. your bank) and requesting confidential and often critical information.

Man-in-the-middle attacks: VoIP is particularly vulnerable to man-in-the-middle attacks, in which the attacker intercepts call-signaling SIP message traffic and masquerades as the calling party to the called party, or vice versa. Once the attacker has gained this position, he can hijack calls via a redirection server.

Automated answering systems: The automated answering and menu systems used by most large companies, including banks, can also be used by an attacker. Combined with VoIP and war-dialing techniques an attacker can automatically try hundreds of numbers and use an automated system which, like banks, solicits details like credit card numbers in the name of ease of use or security.

Keystroke capturing/logging: Anything you type on a computer can be captured and stored. This can be done using a hardware device attached to your computer or by software running almost invisibly on the machine. Keystroke logging is often used by fraudsters to capture personal details including passwords. Some recent viruses are even capable of installing such software without the user's knowledge.

LOCAL ATTACKS

A common mistake made by every user is they believe their online banking session is perfectly safe when they use an SSL 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 little does the user realize 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 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 achieved by injecting the Trojan directly into the web browser's memory space, which also can often bypass desktop firewalls when making outgoing connections. Other local attack methods include running a layered service provider (LSP) monitoring all network traffic, writing its own network driver, or displaying a carefully crafted copy of a website on top of the official website. From the user's viewpoint, 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 assword 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).

HYBRID ATTACKS

Nothing limits an attacker to only one type of attack. 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 theaddress bar of the browser. So the Trojan needs to modify the browser settings to not display the address bar or overlay it with a fake pop-up window. Even though this is feasible, it resides on the same level as basic phishing attacks and can be equally well done by remote attacks. The more sophisticated approach of the attacker would rather 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 attacker the possibility to redirect certain domains to predefined IP addresses. This technique is used by the Trojan.

Some other types of attacks:

1. Sniffers — Also known as network monitors, this is software used to capture keystrokes from a particular PC. This software could capture logon

2. IDs and passwords.

3. Guessing Passwords — using software to test all possible combinations to gain entry into a network.

4. Brute Force — a technique to capture encrypted messages then using software to break the code and gain access to messages, user ID's, and passwords.

5. Random Dialing — this technique is used to dial every number on a known bank telephone exchange. The objective is to find a modem connected to the network. This could then be used as a point of attack.

6. Social Engineering — an attacker calls the bank's help desk impersonating an authorized user to gain information about the system including changing passwords.

7. 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.

8. Hijacking —intercepting transmissions then attempting to deduce information from them. Internet traffic is particularly vulnerable to this threat.

B) TYPES OF RISKS

Credit Risk: Credit risk is the risk to earning and eventually capital, arising from a borrower's failure to meet the terms of a credit contract with the bank or otherwise to perform as agreed. It is found in all activities where success depends on counterparty, issuer, or borrower performance. It arises any time bank findings are extended, committed, invested, or otherwise exposed through actual or implied contractual agreements, whether on or off the bank's balance sheet.

Strategic risk: This is the current and prospective risk to earnings and capital arising from adverse business decisions or improper implementation of business decisions. Many senior managers do not fully understand the strategic and technical aspects of Internet banking. Spurred by competitive and peer pressures, banks may seek to introduce or expand Internet banking without an adequate cost-benefit analysis. The organization structure and resources may not have the skills to manage Internet banking.

Transaction risk: This is the current and prospective risk to earnings and capital arising from fraud, error, negligence and the inability to maintain expected service levels. A high level of transaction risk may exist with Internet banking products, because of the need to have sophisticated internal controls and constant availability. Most Internet banking platforms are based on new platforms which use complex interfaces to link with legacy systems, thereby increasing

risk of transaction errors. There is also a need to ensure data integrity and non repudiation of transactions. Third-party providers also increase transaction risks, since the organization does not have full control over a third party. Without seamless process and system connections between the bank and the third party, there is a higher risk of transaction errors.

Information security risk: This is the risk to earnings and capital arising out of lax information security processes, thus exposing the institution to malicious hacker or insider attacks, viruses, denial-of-service attacks, data theft, data destruction and fraud. The speed of change of technology and the fact that the Internet channel is accessible universally makes this risk especially critical.

Liquidity risk: This is the risk to earnings or capital arising from a bank's inability to meet its obligations. Internet banking can increase deposit and asset volatility, especially from customers who maintain accounts solely because they are getting a better rate. These customers tend to pull out of the relationship if they get a slightly better rate elsewhere.

Compliance risk: This is the risk to earnings or capital arising from violations of, or nonconformance with, laws, regulations and ethical standards. Compliance risk may lead to diminished reputation, actual monetary losses and reduced business opportunities. Banks need to carefully understand and interpret existing laws as they apply to Internet banking and ensure consistency with other channels such as branch banking. This risk is amplified when the customer, the bank and the transaction are in more than one country. Conflicting laws, tax procedures and reporting requirements across different jurisdictions add to the risk. The need to keep customer data private and seek customers' consent before sharing the data also adds to compliance risk. Customers are very concerned about the privacy of their data and banks need to be seen as reliable guardians of such data. Finally, the need to consummate transactions immediately (straight-through processing) may lead to banks relaxing traditional controls, which aim to reduce compliance risk.

Foreign Exchange Risk: Foreign Exchange risk is present when a loan or portfolio of loans is dominated in a foreign currency or is funded by borrowings in another currency. In some cases, banks will enter into multi-currency credit commitments that permit borrowers to select the currency they prefer to use in each rollover period. Foreign exchange risk can be intensified by political, social or economic development. Appropriate systems should be developed if bank engage in these activities.

Interest rate risk: This is the risk to earnings or capital arising from movements in interest rates (e.g., interest rate differentials between assets and liabilities and how these are impacted by interest rate changes). Internet banking can attract loans and deposits from a larger pool of customers. Also, given that it is easy to compare rates across banks, pressure on interest rates is higher, accentuating the need to react quickly to changing interest rates in the market.

Reputation risk: This is the current and prospective risk to earnings and capital arising from negative public opinion. A bank's reputation can be damaged by Internet banking services that are poorly executed (e.g., limited availability, buggy software, poor response). Customers are less forgiving of any problems and thus there are more stringent performance expectations from the Internet channel. Hypertext links could link a bank's site to other sites and may reflect an implicit endorsement of the other sites.

## III. MITIGATION MEASURES

Mitigation strategies: event monitoring and customer behavioral profiling So, what can banks and financial institutions do to protect their customers from the impact of man-in-the-browser attacks? Customer authentication measures 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

if it fits the established profile of the genuine customer. 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 funds transfers and bill payments

• 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.

Electronic Security Vendors: A rich variety of vendors operate in what is becoming a global industry for electronic security. Many types of companies operate in this industry. In the United States alone, $5.1 billion in security software was sold in the year 2000—a 33 percent increase over the prior year. These companies are involved in every facet of securing the wide area networks over which financial services are provided. The 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. These vendors provide tools to monitor all content entering a network for malicious codes, such as harmful attributes. Trojans, worms, and viruses are methods used to deploy an attack once the perpetrator enters the system. Viruses are programs that infect other programs on the same system by replicating themselves. Virus scanners are critical in mitigating these attacks. Vendors of virus scanners provide software 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: Companies that produce firewalls provide virtual “security guard” at the gate of the customer’s facilities. A firewall is a system that enforces the access-control policy between two networks. Vendors create these virtual guards to protect a network’s integrity.

Penetration Testing Companies: These consulting organizations simulate attacks on networks to test for a system’s inherent weaknesses. They then patch the holes found during the simulated attacks. Typically, 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 uses complex algorithms to shield messages transmitted over public channels. It provides safe passage from point A to point B. When the message reaches its destination, the recipient uses another algorithmic key to open it. It is highly recommended for use by mobile workforces and/or large non centralized corporations or institutions.

## IV.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 for online banking systems currently in use are strongly based on Internet banking user identification and authentication methods, which are also the components where most Internet banking systems' 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 authentication data. This fact indicates that secure internet banking systems should provide security mechanisms as user independent as possible, mitigating the risk of user related information’s leaks and security issues affecting the system and leading to fraud.

## REFERENCES

[1] 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.

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

[3] 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.

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

[5] O. Dandash, P. Dung Le, and B. Srinivasan, Internet banking payment protocol with fraud prevention, 2007 22nd International International Symposium on Computer and Information Sciences, Nov. 2007, pp. 1-6.

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