Volume-4, Issue-6, June-2015 • ISSN No 2277 - 8160

Research Paper Commerce

Benefits and Security Threats in Electronic Banking

M.Sc. AleksandarLukic

KBM Bank AD, Dept. of International Payments Kragujevac, Serbia

ABSTRACT

Internet banking is changing the banking industry, having the major effects on banking relationships. Banking is now no longer confined to the branches were one has to approach the branch in person, to withdrawcashordeposit a chequeorrequest a statement of accounts. In true Internet banking, anyinquiryortransaction is processedonlinewithoutany reference to the branch at any time. The netbanking, thus, now is more of a normratherthananexception in manydevelopedcountriesdue to the factthatit is the cheapestway of providingbankingservices.

Apart from the many advantages of electronic banking has certain security problems. The challenges that oppose electronic banking are the concerns of security and privacy of information. The current focus of security of information transfer is on the session layer protocols and the flaws in end to endcomputing. A secure of this transaction requires a secure protocol to communicate over un-trusted channels and a trusted code at both endpoints. The solution addresses the use of secure protocols because trusted channels don't really exist in most of the environment, especiallysincewearedealingwithlinking to the averageconsumers.

KEYWORDS : internet banking, Information technology, e-security, security threats, secure transactions

Introduction

Internet 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 functions. In internet banking system the bank has a centralized database that is web enabled. All the services that the bank has permitted on the internet are displayed in menu. Once the branch offices of bank are interconnected through terrestrial or satellite links, there would be no physical identity for any branch. It would be a borderless entity permitting anytime, anywhere and any how banking.

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.

Benefitsandimportance of electronicbanking

Internet banking is the latest in the series of technological wonders of the recent past. Internet banking refers to systems that enable bank customers to get access to their accounts and general information on bank products and services through the use of bank's website, without the intervention or inconvenience of sending letters, faxes, original signatures and telephone confirmations. It is the types of services through which bank customer scan request information and carryout most retail banking services such as balance reporting, inter-account transfers, bill-payment, via telecommunication network without leaving their home or organization. It provides universal connection from any location worldwide and is universally accessible from any internet linked computer. [1]

Information technology developments in the banking sector have speedup communication and transactions for clients. It is vital to extend this banking feature to clients for maximizing the advantages for both clients and service providers. Internet is the cheapest delivery channel for banking products as it allows the entity to reduce their branch networks and downsize the number of service staff. The navigability of the website is a very important part of Internet banking because it can become one of the biggest competitive advantages of a financial entity. Due to increase in technology usage the banking sector's performance increases day by day. Internet banking is becoming the indispensable part of modern day banking services.

It is notoriously difficult to predict the future, but some educated guesses can be made using past and current experiences. In our view, the next developments in e – banking will involve new products and services that were not feasible in traditional banking models. This could involve enabling instant payments using mobile devices, or tools to help people manage their multi-bank financial portfolio, simultaneously. Internet only banking may also become more viable as the functionality of e – banking systems grows, and customers adapt to the new ways of conducting their financial activities. International banking might become a reality for ordinary consumers as banking payments systems are increasingly harmonized across borders. E-banking has the potential to be a very rich and pleasant experience, and may provide more opportunities for banks to develop mutually satisfying, tailor made services to enrich relationship with customers. As technology evolves, the opportunities to extend the relationship beyond what is possible in the physical world continue to grow and will only be limited by a bank's ability to innovate or commitment to e-banking. [2]

Despite numerous advantages of electronic banking is the issue of security. Security is important in setting up and e-banking facility. In building up a secure transactions systems factors that have to be considered are improving customer trust and integrating the current services offered to the customers. Since electronic banking is a new technology that has many capabilities and also many potential problems, users are hesitant to use the system. The number of malicious application stargeting online banking transactions has increased dramatically in recent years.

Securitythreats in electronicbanking

The disclosure of important information that should remain confidential, by unauthorized persons or that exceed their authority can cause significant losses for financial institutions. Alteration of information by entering, modifying or overwriting data into the system without authorization or by exceeding one's authority is a type of attack that could potentially harm greatly the banks and their customers. Security threats can affect a financial institution through numerous vulnerabilities. No single controller security device can adequately protect a system connected to a public network. Many problems concerning the security of transactions are the result of unprotected data being sent between clients and servers.

The problems of the systems today are in he rent within the setup of the communications and also within the computers itself. The current focus of security is on session-layer protocols and the flaws in end-to-endcomputing. A secure end-to-end transaction requires a secure protocol to communicate over untrusted channels, and a trustee code at both end points. It is really important to have a secure protocol because the trusted channels really don't exist in most of the environment. [3]

There are various types of attacks that e-banking can suffer. Theyinclude:

1. Social Engineering - One of the most common attacks does not involve knowledge of any type of computer system.Tricking consumer s into revealing sensitive information by posing as a system administrator orcustomer service representative is known as social engineering. Social engineers use surveillance and a consumer's limited knowledge of computer systems to their advantage by collecting information that would allow them to access private accounts.

2. Port Scanners - Attackers can use port scanners to ascertain entry points into a system and use various techniquesto steal information. This type of software sends signals to a machine or router and records themessage the machine responds with to ascertain information and entry points (Cobb, 2007). Themain purpose of a port scanner is to gather information related to hardware and software that asystem is running so that a plan of attack can be developed.

3. Packet Sniffers - The connection between a user's computer and the web server can be "sniffed" to gather anabundance of data concerning a user including credit card information and passwords. A packetsniffer is used to gather data that is passed through a network. It is very difficultto detect packet sniffers because their function is to capture network traffic as they do notmanipulate the data stream. The use of a Secure Socket Layer connection is the best way toensure that attackers utilizing packet sniffers cannot steal sensitive data.

4. Password Cracking - Password cracking can involve different types of vulnerabilities and decrypting techniques;however, the most popular form of password cracking is a brute force attempt. Brute forcepassword attacks are used to crack an individual's username and password for a specific websiteby scanning thousands of common terms, words, activities, and names until a combination ofthem is granted access to a server. Brute force cracking takes advantage of systems that do notrequire strong passwords, thus users will often use common names and activities making itsimple for a password cracker to gain access to a system. Other password cracking methodsinclude using hash tables to decrypt password files that may divulge an entire systems user nameand password list.

5. Trojans - Trojan software is considered to be the most harmful in terms of electronic banking security due to itsability to secretly connect and send confidential information. These programs are developed forthe specific purpose of communicating without the chance of detection. Trojans can be used tofilter data from many different clients, servers, and database systems. Trojans can be installed tomonitor emails, instant messages, database communications, and a multitude of other services.

6. Denial of Service Attacks - Denial of service attacks are used to overload a server and render it useless. The server is askedrepeatedly to perform tasks that require it to use a large amount of resources until it can nolonger function properly. The attacker will install virus or Trojan software onto an abundance ofuser PC's and instruct them to perform the attack on a specific server. Denial of service attackscan be used by competitors to interrupt the service of another E-Commerce retailer or byattackers who want to bring down a web server for the purpose of disabling some type ofsecurity feature. Once the server is down, they may have access to other functions of a server,such as the database or a user's system. This allows the attacker the means to install software ordisable other security features.

7. Server Bugs - Server bugs are often found and patched in a timely fashion that does not allow an attacker toutilize the threat against an e - banking web site. However, system administrators are oftenslow to implement the newest updates, thus allowing an attacker sufficient time to generate athreat. With the millions of web servers in use around the world, thousands often go withouttimely patches, leaving them vulnerable to an onslaught of server bugs and threats.

8. Super User Exploits - Super user exploits allow attackers to gain control of a system as if they were an administrator.They often use scripts to manipulate a database or a buffer overflow attack that cripples asystem, much like a Denial of Service attack for the purpose of gaining control of the system.Users can create scripts that manipulate a browser into funneling information from sources, suchas databases. [4]

In the modern banking the best way for protect against these attacks are: education, personal firewalls, secure socket layer and server firewalls.

A multi-layered security architecture comprising firewalls, filtering routers, encryption and digital certification can ensure that customer account information is protected from unauthorized access. At minimum, a two-factor authentication should be implemented in order to verify the authenticity of the information pertaining to Internet banking services. The first authentication factor can be the use of passwords and the second authentication factor can be the use of tokens such as a smartcard. However, for a better security, a three factor authentication process should be considered. The third authentication factor is the use of biometric.

Conclusion

As a result of the growth of the internet,electronic commerce has immerged and offers tremendous market potential for today's business. One industry that has benefited from this new communication channel is the banking industry.Electronic banking is offering its customers with a wide range of services.Customers are now able to interact with their banking accounts as well as make financialtransactions from virtually anywhere without time restrictions. E-banking is offered by manybanking institutions due to pressure from competitions. Today, it is believed that people makethe difference to information technology and security development and that training on theethical, legal and security aspects of information technology usage should be ongoing at alllevels within organizations

The future of electronic banking will be a system where users are able to interact with theirbanks "worry-free" and banks are operated under one common standard. Most research studieshave indicated that the common problem affecting information security and privacy of customersis e-services provider's lack of security control which allows damaging privacy losses. Apartfrom that, another problem is the subsequent misuse of consumers' confidential information, asin identity theft. These may affect customer's confidence toward online business transaction in avariety of privacy risk assessments by consumers. Current technology allows for secure sitedesign. It is up to the development team to be both proactive and reactive in handling securitythreats, and up to the consumer to be vigilant when doing business online.

REFERENCES

1) Amtul, F., E-Banking Security Issues – Is There A Solution in Biometrics, Journal of Internet Banking and Commerce, Vol. 16, Issue. 2, 2011. | 2) Shah, M. and Clarke, S., E-Banking Management:Issues, Solutions,and Strategies, Hershey - New York, 2009. | 3) Vyas, S., Impact of E-Banking on Traditional Banking Services, International Journal of Computer Science & Communication Networks, Vol. 2, Issue 3, 2012. | 4) Zachary, O., Masese, E. and Wanyembi, G., Security and privacy of electronic banking, International Journal of Computer Science Issues, Vol. 9, Issue 4, 2012. |