Dept of Computer Science, P B SIDDHARTHA COLLEGE OF ARTS & SCIENCE, VIJAYAWADA.
UGC SPONSORED NATIONAL SEMINAR ON "CYBER SECURITY WITH SPECIAL FOCUS ON CYBER CRIMES & CYBER LAWS (NSCS 2014)" on
15th & 16th November 2014-IJDCST SPECIAL ISSUE, PAPER –ID: IJDCST-15
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

E-Security in Banking System

Ms. A. Aphia Sumalatha[1] , Ms. P. Naga Kavitha[2]

[1]Lecturer, Dept. of Computer Science, St. Ann's College for Women, Mehdipatnam, Hyderabad. E-mail: apphia.sumalatha@gmail.com

[2]Lecturer, Dept. of Computer Science, St. Ann's College for Women, Mehdipatnam, Hyderabad. E-mail: archana78reddy@gmail.com

Abstract: The adoption of 'electronic banking' facilities across commercial banks in India was done during the nineties; mainly to gain competitive advantage. The major gain from e-banking includes 'convenience'. The conversion of paper money to electronic money avoids stealing and offers better security. However, e-security in banking system is always a concern for many, security threats being the only substantial inhibition for the customers. Security & authenticity of a transaction are the most important issues in the e-banking system. The risks include tampering of customers' accounts like password cracking, identity theft, and phishing, amongst many others. To manage the risk and gain trust of the customers, the banking institutions are being forced to adopt various innovative processes. Some of the present methods include password authentication (PIN/TAN system via Secure Socket Layer (SSL) connections), virtual keyboards, access codes, server firewalls, personal firewalls, etc. This paper would first talk about the vulnerability issues related to security and privacy; and then the preventive measures.

Keywords: Internet, e-banking, e-commerce, e-security, privacy, and attacks.

Introduction

Internet has become a part and parcel of man's day to day life. This digital revolution is happening rapidly, with millions of users worldwide and over 95% of the data available in the world was generated in the past 2 or 3 years. As Wikipedia states, Information explosion is *the rapid increase in the amount of published information or data and the effects of this abundance* [1]. While information explosion enables to expand new technologies day after day, it also creates new problems in cyber world.

The businesses which deal in e-services, especially banking industry, are more concerned with these new problems. Cyber stalking and hacking are the most prevalent issues in banking industry. The confidential information needs to be protected and the banks are constantly trying to improve e-security for their customers. Ensuring privacy, reliability, and accessibility of electronic information will always remain the main focus to gain the customer's confidence. The banking institutions have adopted various innovative practices to ensure secure financial transactions in the e-banking industry. The security threats include password cracking, identity theft, phishing and pharming, amongst many others. To provide consistency some of the current practices include

password authentication (PIN/TAN system via Secure Socket Layer (SSL) connections), virtual keyboards, access codes, firewalls (both personal & server), etc.

Vulnerability Issues – Threats and Loopholes

General security objectives are privacy, reliability and accessibility. The insecurity is mainly due to phishing, pharming, identity theft and IP spoofing amongst many others. These issues prevent customers from opting e-banking, and the present security approaches appear to be deficient. There is a need to assess and present solutions; as trust is the foundation stone of e-banking.

E-banking Security

To succeed, a bank needs to optimally utilize both web & mobile technology platforms. The financial institutions have to deliver innovative products & services through highly secure channels. The sheer size of 'electronic banking' activities is rapidly witnessing a heavy surge and is demanding infallible security for each and every banking transaction.

Researchers have defined security as a complex concept. Belanger et al. (2002)[2] describe *security as 'the protection against security threats or attacks done either through network and data transaction attacks, or through unauthorized access by means of false or defective authentication.*' Grabner-Krautera & Kaluscha (2003) [3] state - '*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.*

Vulnerability Issues -

Phishing:

a. Fraudulent e-Mails

The fraudulent e-mail is received from an unlawful entity and tries to collect confidential personal and financial data.

b. Phony Websites

These are fraudulent websites made to appear identical to those of a genuine bank or trustworthy websites. Phony websites are also well-known as 'spoofed websites'. These spoofed websites make use of genuine logos of a company to indulge in stealing confidential personal and financial data. And the information is used in e-commerce, or e-banking.

c. Vishing

Vishing is a new form of threat in online frauds. This process combines voice and phishing. Vishing involves voice or telephone services, using VoIP services. The fraudster poses as a bank employee or associate to seek information; and steal the personal data by recording your voice or keyboard strokes.

Pharming:

According to Wikipedia, the term "pharming" is a mix of words "farming" and "phishing". Pharming is a method where online hackers control the users by redirecting them to a fake website. The website – www.techterms.com[4] states that 'pharming' process involves e-mail virus that pollutes local DNS cache and modifies the DNS entries or host files. Thereby, the hacker manipulates the user of the cache and redirects them to a fake website.

IP Spoofing:

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Spoofing is used in acquiring unauthorised access to a network or a computer system. The process engages in active interception and involves packet sniffing to acquire information. IP header can easily be controlled by masking a source address. And sequence prediction, specific to Transmission Control Protocol – TCP, leads to session hijacking or host impersonating. [5]

Identity Theft:

Identity theft is an offense in which an impostor acquires personal information with the intention of impersonating the victim. The data obtained is used to raise loans, buying goods and services.

Trojan horse:

A malware and a destructive program intended to connect to a system and gain information in a stealth mode. The installed Trojan program, when executed, gives the fraudster remote access to the computer and allows a crime. According to BitDefender [6], "Trojan malware accounted for 83% of the malware detected in the world."

Preventive Measures

Secured Login:

Data transferred across the bank account, the internet, and the personal computer can be secured through 128-bit Encryption.

Virtual Keypad Login:

'Online Virtual keyboard Login' removes the vulnerabilities associated with hacking of keyboard strokes. This login process is done completely by using a mouse. In a virtual keypad the position of characters keeps changing in random fashion, and avoids malware or spyware attacks in e-banking transactions.

Enhanced Security at Login:

General login into an online bank account requires a PIN – a password. Further, enhanced login necessitates TAN - a time-bound or onetime secret password. This One Time Password adds an additional security layer in executing financial transactions and acts as a multifactor authentication. It is a unique, secure, and a single use password; and can be received by a registered mobile number only. Secure banking transactions are executed using PIN/ TAN via Secure Socket Layer (SSL) connections.

Automatic Session Timeouts & Lock Out:

If a customer stays inactive for a certain time, the session will automatically expire and logs him off from the website. This ensures unauthorised access to account information. And if a user enters incorrect password for about three consecutive times, the account will get locked out, ensuring protection from password cracking by fraudsters.

Digital Certificates:

Digital Certificates facilitate identification of unauthorized websites. The Certification Authority provides the server's authenticity and makes sure online transactions to be secure.

Extended Validation SSL Certificates:

Extended Validation SSL is an e-security credential that certifies authenticity of a website. This e-security feature makes the address bar change to green colour, in case of genuine websites.

Firewalls:

The bank websites employ several firewalls to shield the computer servers and avoid unauthorised access to a network. Server Firewalls engage intrusion detection software to identify e-security threats, by setting up a demilitarised zone. Additionally, Honey pot firewall, a fake server, is used to trap a hacker or an intruder. These firewalls have to be updated consistently to prevent security violations. Personal firewall is also essential while transacting over a web connection.

Anti-Virus and Anti-Spyware:

Anti-virus software on a personal computer ensures e-security. To provide protection from e-security threats, complete scanning of computer periodically and also, configuring the anti-virus software to scan each email both received and sent is necessary. However, to avoid Trojan attacks or spying, anti-spyware software needs to be installed that prevent any spyware attacks.

Conclusion

This paper delves on e-security in banking system as a whole and discussed the threats in brief. The counter actions that were referred to are the measures employed currently by all major banks in India. E-Security in banking system is a very crucial aspect and the counter measures that thwart off threats need to stay updated with current technology trends. Innovative systems or techniques, such as Video branch, eye recognition or other biometrics, must be employed by all the banks to defuse vulnerabilities in e-banking system. Apart from addressing e-security concerns of the customers, the banks should also educate them on e-banking etiquette and warn them of new potential threats. As pointed out earlier, privacy, reliability, and accessibility of electronic information will always remain the main focus to gain the customer's confidence. And this can be achieved only through relentless perusal and implementation of innovative e-security measures in the e-banking system.

References:

1. Wikipedia
2. France Belanger, Janine S. Hiller, Wanda J. Smith (2002) – "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes"
3. Ewald A. Kaluscha & Sonja Grabner-Kräuter (2003) – "Patterns for Consumer Trust in Electronic Commerce"
4. www.techterms.com – an online dictionary for technical terms
5. 'Spoofing: An Introduction' by Matthew Tanase (SecurityFocus.com) 2010
6. BitDefender.com - an e-security website conducted a survey for the period Jan-Jun'09.
7. Generic sources on the web and published articles.
8. Processes employed by various commercial banks in India