Secure E-Banking Environment: A Comparative Analysis of Various Security Aspects

Dr. Tejinder Pal Singh Brar
Associate Professor, Department of Computer Application, CGC-Landran (Mohali)

Abstract
From the last one decade Indian financial sector has witnessed change of trends not only in terms of growing customer base but also due to generation of revenue by them. Considerable percentage of customers has adopted online channels for conducting financial transactions. But at the same time customers are concerned about various online security threats. Due to sensitive nature of customer’s information that is available online financial institutions need to increase security. The main objective of this paper was to investigating E-banking security in Indian banking sector. Data has been collected from websites of 9 commercial banks. The study discovered that there was a lack of appropriate E-banking security measures that were implemented by selected Indian commercial banks.

Keywords: Security, Authentication, OTP, Trust

Introduction
Online technologies have affected every individual’s life during the past few decades. But at the same time security issues have become more common nowadays in internet technology particularly on E-banking systems due to the harmful impact on confidentiality, integrity and privacy of the bank and its customers. With the introduction of enhanced communication technologies number of electronic services for customers’ have evolved and spread widely. Also the need for security has also increased because attackers have developed more complicated methods to compromise authentication mechanisms and gain unauthorized access to customers’ sensitive information. There are number of factors which affect the customers thinking about online banking security. The same factors are also driving the need for enhanced authentication for online banking solutions. These factors include the growing number of phishing attacks, increased usage of pharming and malware and widespread data security breaches.

Now a day’s data breaches are happening all over the world on a regular basis. Phishing attacks or malware can easily steal passwords, and attacker correctly answers the challenge questions on the basis of amount of information about customer that is available online. Many data breaches are linked to compromised usernames, passwords and OTP’s. It raises a question: Why do not we make strong security controls and why we rely on simple user names and passwords? Infect, no single security solution is enough to defend against today's versatile attacks. Various attack tools have been developed and programmed into downloadable kits. Rootkit-based malware secretly installed on a computer system that can monitor a customer’s activities that aid theft and misuse of their login credentials. Such type of malware can break
strong authentication techniques like multi-factor authentication. This article reviews possible attacks according to which authentication mechanisms adopted by banks evaluated.

There were number of incidents reported in the past where hackers hack the bank account and eventually huge financial losses were incurred; we now discuss attack tree which shows types of attacks. There is one node at the root level i.e. user’s bank account compromise that represents the final target of the attacker. An attacker may use one of the leaf nodes as a means for reaching the target. Internet banking attacks can be classified into three categories: User terminal (UT) attacks, Communication channel (CC) attacks, Internet banking server (IBS) attacks.

(i) User terminal (UT) attacks: These attacks primarily target the user equipment like the tokens that may be involved, such as smartcards or other password generators, as well as the actions of the user himself. These attacks include:

- User surveillance
- Theft of token and handwritten note stealing
- Malicious software installation
- Smartcard analyzers
- Smartcard reader manipulator
- PIN calculators
- Social engineering
- Web page obfuscation

(ii) Communication channel (CC) attacks: These attacks focus on communication links. These attacks include:

- Pharming
- Sniffing
- Active man-in-the-middle attacks
- Session hijacking

(iii) Internet banking server (IBS) attacks: These types of attacks are offline attacks against the servers that host the Internet banking application. Examples include:

- Brute-force attacks
- Bank security policy violation
- Web site manipulation

Review of Literature

Security and data confidentiality are major barriers in E-Commerce applications for the banking industry. Customers who wish to trade in the E-commerce world found security and privacy is the most challenging
problems faced by them. Security further affects trust and satisfaction of the customer. Kalakota and Whinston, (1997) defines Perceived security as a threat that creates a circumstance or condition, with the potential to cause economic hardship to data or network resources in the form of destruction, disclosures, and modification of data, denial of service, and/or fraud, waste and abuse. Fitzgerald (2004) argued that lack of awareness of online banking and the security concerns are the major ‘non-adoption’ areas of E-banking. Malhotra and Singh (2009) found that slowly but steadily, the Indian customer is moving towards internet banking. But they are concerned about issues such as security and privacy. Mukti (2000) found that security is main barrier to e-commerce expansion in Malaysia.

According to Aladwani (2001), future challenges for the adoption of E-banking are internet security, consumers’ privacy, bank’s reputation and online banking regulations. Author further found that customers ranked privacy and internet security as the most important future challenges. According to him, security is the most feared problem on the internet. Banks and customers take a very high risk by dealing electronically. The survey conducted by White and Nteli (2004) found that UK consumers ranked the security of bank’s website as the most important attribute of internet banking service quality. This situation is further illustrated by Sathy (1999), investigator the adoption of internet banking found that security concerns and lack of awareness about the internet banking were the two main obstacles for the non-adoption.

According to Alnsour and Hyari (2011) trust has a significant and positive effect on ease of use. The more a user trusted the bank and its website, the higher their belief that online banking is easy. Higher levels of security may make online banking more useful. Bala et al. (2011); Viega and McGraw (2001) suggests developers have to incorporate security during the development process itself in order to produce software assurance systems, since the existence of flaws at the design or coding stage of the development process can open web applications to a wide range of attacks. According to the white paper published by Symantec co. malicious applications that steal financial account information have increased dramatically over the last few years, resulting in a direct loss of hard currency as well as loss of trust. Dixit and Dutta (2010) insist that banks needs to increase the level of trust between banks’ website and customers.

According to Lin and Vardharajan (2006), trust is the expectation that a device or system will faithfully behave in a particular manner to fulfill its intended purpose, e.g., a computer is trustworthy if its software and hardware can be depended on to perform as expected such that its services are still available today, unaltered, and behave in exactly the same way as they did previously. Similarly, Krauter and Faullant(2008) confirmed the influence of trust on risk perception and consumer attitudes towards internet banking. Tendency to trust is a determinant not only for interpersonal relationships but also for trust in technological systems. On the same lines Tat et al. (2008) study predictors of intention among users to continue using the E-banking services in Malaysia and conclusion confirmed that among the tested predictors, trust is found to
be the strongest predictor of intention to continue using internet banking, followed by compatibility and ease of use.

Detection of attacks still needs to be enhanced significantly not only in India but also across the globe. Schwartz (2014) describes a security lapse related to credit and debit card transactions in US. On the same lines Karimi (2014) reports that Federal Trade Commission reports identity theft accounted for 18 percent of consumer complaints in 2012 alone and about 85 percent of identity theft incidents involved fraudulent use of credit card information. Finkle and Henry (2013) found that Target Corp (TGT.N) which is one of the biggest retailers in U.S. attacked by hackers in November 2013 which lasts for 19 days. This attack compromised up to 40 million credit cards and debit cards also managed to steal encrypted personal identification numbers (PINs) that makes it the second-largest data breach in U.S. retail history.

Nearly 80% of U.S. banks think that malware on their customers’ PC is a top security risk. Indeed this seems justified because U.S. consumers lost over US$ 2 billion and 1.3 million PCs to malware in 2010, Dinesh (2011). The top spot of weak authentication is taken by password which is the most prevalent and weak form of authentication because it is very easy to steal. According to Kitten (2014) the average annualized cost of cyber-crime for U.S. financial services institutions in 2013 was $23.6 million i.e. nearly 44 percent increase from 2012. Almost all of these major fraud cases in the last couple of years can be linked to authentication infrastructures.

While analyzing Indian scenario of cyber-attacks, Bipindra (2014) in his report highlight the incident when Defense Research and Development Organization’s (DRDO) computers were hacked by Chinese hackers and carted away electronic files relating to Cabinet Committee on Security (CCS) which is the country’s highest decision-making body on security affairs. According to article posted by Information Age (2012), hackers have breached information systems belonging to the Indian Navy, stealing sensitive data and sending it to computers with Chinese IP addresses. Kumar (2014), states that 3,000 internet connections of the Defense Ministry and the Air Force Communication Centre have been compromised and about three hundred thousand modems in Delhi are also vulnerable to Domain Name System (DNS) exploitation attacks.

According to Gurung (2014) there is an increase in the cyber-crime by 51%, the cases related to cyber-crime that was filled in the year 2013 was 4356 and this year it is increased by 51 percent in comparison to previous year. In yet another kind of security related incident Tripathy (2014) reported that Chinese telecom company Huawei Technologies had hacked into telecom carrier Bharat Sanchar Nigam Ltd (BSNL). Similarly in 2012, a US panel urged American companies to stop doing business with Huawei and ZTE Corporation and warns that China could use firms’ equipment to spy on certain communications and threaten vital systems through computerized links.
Methodology

The availability of E-banking security features of the Indian commercial banks was investigated by conducting descriptive analysis of selected banks. 9 banks were selected on the basis of random sampling and other financial institution types were not examined as they were either comes under regional rural banks or cooperative banks. The list of the selected banks utilized in the analysis is provided in Table 1. In order to evaluate the internet banking security features, data mainly collected from selected banks’ websites or from their periodic journals/publications. The proposed internet banking security checklist consists of sixteen main security features that banks offers in order to make internet banking environment safe for conducting financial transactions.

Security Analysis

It is important to analyze number of security measures provided by banks in an online environment because it not only helps in building the bank’s reputation but also it helps in adoption and acceptance of online delivery channels by intended customers as well as potential customers.

Table 1: A Summary of E-banking Security Checklist

<table>
<thead>
<tr>
<th>S.no</th>
<th>Security Features</th>
<th>ICICI</th>
<th>HDFC</th>
<th>YB</th>
<th>SBI</th>
<th>IB</th>
<th>BOB</th>
<th>CB</th>
<th>DB</th>
<th>ADCB</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>General security and privacy information and</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>guidelines</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Losses compensation guarantee</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>3</td>
<td>Hoax email, scam, phishing and spyware</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>4</td>
<td>Security alerts</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>5</td>
<td>Antivirus protection</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>6</td>
<td>Data encryption</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>7</td>
<td>Firewall</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>8</td>
<td>Intrusion Detection System + alert system</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>9</td>
<td>Hotline/helpdesk service availability</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>10</td>
<td>Internet security suite</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>11</td>
<td>Signing Certificate Authority (CA)</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>12</td>
<td>User site authentication technology</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>13</td>
<td>Two-factor authentication for logon</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>14</td>
<td>Token device</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>15</td>
<td>Logon failure limitation</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>16</td>
<td>Transaction Monitoring</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

*Y-YES; N-NO; YB- YES BANK; IB- Indian bank; BOB- Bank of Baroda; CB: Citibank; DB- Deutsche Bank; ADCB: Abu Dhabi Commercial Bank
Almost all of the selected Indian banks have provided information regarding general security and privacy information and guidelines on their banks’ websites. This information is necessary as far as customer’s perspective is concerned. On the other hand no information has been offered by any of the selected Indian bank regarding providing guarantee about loss compensation in case any online theft or account hacking. Majority of banks (ICICI, HDFC, YB, SBI, IB, CB, ADCB) provide information on hoax email/scam/phishing and spyware while no information has been provided by BOB and DB. As far as security alerts is concerned majority of banks sent security alerts to their customers while (YB, IB and ADCB) do not provide any information regarding the same. It has been found that not even a single bank out of selected banks has offered antivirus protection through which customers can scan their systems on regular basis. On the other hand data encryption has been provided by all the banks through 128-bit SSL encryption algorithms. Information regarding implementation of firewall has not been provided by YB, IB, BOB and DB; similarly no information is given on IDS/alert systems. Hotline or helpdesk numbers are provided by all the banks while no information is given by any of selected banks on Internet security suite.

Information about certified authority(CA) is provided by all the banks while no information is provided on technology implemented on user’s site. The majority of the 09 selected commercial banks have utilized a two-factor authentication technique for their internet banking transaction verifications. However, banks that do not use a two-factor authentication technique include YB, IB and DB. It was found that SMS is the most widely used two-factor authentication technique followed by token device and email respectively. The use of a compulsory two-factor authentication for logon purposes offers greater security for online banking customers. This security feature can increase the confidentiality to both the existing and potential internet banking customers. Login failure limitations are provided by all the banks, it is considered as another security feature. Only four out of 9 selected Indian commercial banks have provided information about internet banking transactions monitoring on their websites.

**Conclusions and Recommendations**

Financial institutions in India show upward trends in terms of adoption and usage of electronic banking by retail and corporate sector. But due to fear of financial loss customers’ are losing their trust on E-banking security mechanisms. However, banks are trying their best to provide secure environment in which customers’ can transact with confidence. As the study evaluates, due to ongoing cyber-attacks and vulnerabilities in current security measures, there is a need to further strengthen the level of security. Banks should perform periodic risk assessments prior to implementing new electronic financial services or at least every twelve months and adjust their authentication controls for customers’ in reply to new threats to their online accounts.
It was found that there were several internet banking security issues exists for the selected Indian commercial banks. Most of the selected banks have been deficient in providing internet banking security information to their existing and potential internet banking customers. Moreover, password security should be strengthened. This is due to the fact that longer password lengths offer better security by being harder to crack. In addition, the selected Indian banks should upgrade their 128-bit SSL to 256-bit SSL to provide the finest available encryption alternative to improve the confidentiality of their internet banking customers. In addition, extended validation SSL certificates should also be considered for enhanced customer confidentiality. Proper education and awareness programsshould be held in order to provide security awareness such as potential risks and threats information to all existing and potential internet banking customers. Strong authentication is required at different levels of conducting transaction via electronic means. It is important to not only to evaluate online banking applications and identify existing vulnerabilities but also there is a need to evaluate layered security approaches and the areas where these additional layers of authentication should be added. For online, as well as other financial transactions strong authentication measures should be built into the multifactor approach.

Bibliography


