ISSN No. 0976-5697

Volume 2, No. 1, Jan-Feb 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Security Issues in Banking & Financial Sector

Shailesh Maheshwari
Assistant Professor , Shri Vaishnav Institute of Management,
Indore,India,
Shailesh2901@Gmail.Com

Abstract: Internet banking services have been operational in Malaysia since 2001. Presently, only banking institutions licensed under the Banking and Financial Institution Act 1989 (BAFIA) and Islamic Banking Act 1983 are allowed to offer Internet Banking services here. There are 12 commercial banks (inclusive of Islamic banks) out of a total of 25 in Malaysia currently offering Internet Banking services. According to the 11 Malaysia Internet Survey conducted by AC Nielson, Internet Banking is the one of the most popular services utilized by Malaysian surfers. The survey found out that 51 percent out of the total respondent base of 8000 used the Internet for online banking once a month.

Keywords: Banking and Financial Institution Act 1989(BAFIA), Malaysian Computer Emergency Response Team (MyCERT), Association of Banks Malaysia (ABM), Anti Phishing Working Group (APWG), National Computer Network Emergency Response Technical Team / Coordination Centre of China (CNCERT/CC), Multipurpose Smart Card (MyKAD).

I. INTRODUCTION

Online banking allows customers or users to conduct financial transactions on a secure website operated by their banks, creditunions or building societies. Online banking has grown rapidlyusing today's computer technology thereby providing the option of online payment bypassing the time-consuming, traditional banking in order to manage the finances more quickly and efficiently. As per the survey conducted by the Pew Internet and American Life roject, nearly one-quarter of all adults, and almost half of all Internet users have reported being online banking customers. Banks see online banking as a value-added customer service and are trying their best to facilitate convenience and speed at low cost.

II. THE BEGINNING

The concept of online banking as we know it today started in the early 1980s. In 1995 the Presidential Savings Bank first announced this facility for regular client use. These days, quite a few banks operate solely via the Internet and have no ‘four-walls’ entity at all. This advent of the Internet and the popularity of personal computers offered both an opportunity and a challenge for the banking industry. Millions of daily transactions are updated using powerful computers by financial institutions across the world. With the accessibility of Internet to common people, banks envision similar economic advantages by adapting those same internal electronic processes to home use.

III. ADVANTAGES OF ONLINE BANKING

We all know that Internet banking has made life much easier and banking much faster and more pleasant, for customers as well as bankers. One of the any advantages of Internet banking is that it is cost-effective and thousands of customers can be dealt with at once. The administrative work gets condensed drastically with Internet banking. Expenditures on bank stationery have gone down, which has helped raise the profit margin of the bank by a huge number. Customers reap the benefit of accessible account information round the clock, regardless of their location. They can reorganize their future payments from their bank account while sitting thousands of miles away. By using online payment services, they can electronically transfer money from their bank accounts or receive money in their bank accounts within seconds. Customers can apply for a loan, can buy or sell stocks and can even open new accounts.

IV. SECURITY ISSUES

A. Online Payment Services

We all have to agree that the Internet offers safe and convenient new ways to shop for financial services and conduct banking business at any point of time. However, online banking security issues have become one of the most important concerns of the banks. Online banking frauds are main reason for the people or potential customers tend to avoid online banking, as they perceive it as being too vulnerable to fraud. It is very important to understand that the security measures employed by most of the banks can never be completely safe and secure. Further, online banking becomes less secure if users are careless or computer illiterate. An increasingly popular criminal practice is to gain access to a user's finances is phishing, whereby the user is in some way persuaded to hand over their password(s) to a fraudster.

B. Steps Taken To Address Security Issues

Some banks require more than a single password authentication before completing a transaction. This is far more secure than the single mode of authentication which is prevalent today. Usage of security tokens is also becoming more popular and is far more secure than any other method as it provides a two way authentication facility. Some banks offer enhanced security using digital certificates which digitally authenticate the transaction by linking the user to a physical device like a computer. Most banks usually use one or more of the above combinations to enhance their security features.

There are a certain tips for online security, which every customer should abide with, irrespective of the fact that you have an account with a traditional bank or an online bank that has no physical offices. It is wise to make sure that that all transactions are legitimate and that your deposits are federally insured. To verify a bank's insurance status, look for the familiar FDIC logo or the words "Member FDIC" or "FDIC Insured" on the Web site. Also remember that the FDIC insures not all banks operating on the Internet. It is important to note that the FDIC protects only deposits offered by FDIC-insured institutions. Keep all your personal information private and secure and always keep the information as where to go for more assistance from banking regulators handy.

To reiterate, it is vital that the customers should never share personal information with anyone, including employees of the bank. To safeguard the confidential information it is important that documents that contain PIN or password mailers should not be stored; the passwords should be changed immediately and memorized before destroying the mailers. One should also ensure that the logged in session is properly signed out.Internet banking is wonderful and convenient, only a little precaution is required to avail all the features of online banking and to sort out the security issues.

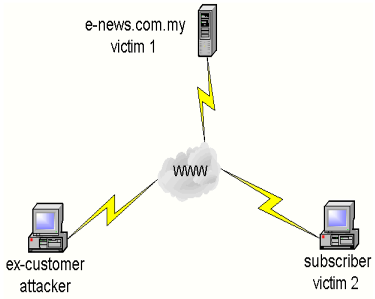
C. Security Incidents

However, 2003 and 2004 saw the emergence of fraudulent activities pertaining to Internet Banking or better known in the industry as "phishing". A total of 92 phishing cases were reported to the Malaysian Computer Emergency Response Team (MyCERT, www.mycert.org.my) in 2004. The modus operandi of this activity is to use spoofing techniques to gain names and passwords of account holders. The victims reported being deceived into going to a fake website where perpetrators stole their usernames and passwords and later use the information for the perpetrators' own advantage. Phishing is an attempt to commit fraud via social engineering. The impact is the breach of information security through the compromise of confidential data. The Association of Banks Malaysia (ABM) has urged both commercial banks and their customers to be extra vigilant following reports of fraudulent email purportedly sent by banks with Internet banking services to online customers. The fraudulent activities mentioned above are not limited to the Malaysian banking industry. It is a worldwide problem particularly in the United States. There, 2560 new unique phishing sites were reported to the Anti Phishing Working Group (APWG) in this year. (see http://antiphishing.org/APWG_Phishing_Activity_Report_Feb05.pdf). It was an increase of 47 percent over the December 2004 figure. APWG is an industry association focused on eliminating identity theft and fraud that result from the growing problem of phishing and email spoofing. This voluntary based organization provides a forum to discuss phishing issues, trials and evaluations of potential technology solutions, and access to a centralized repository of reports on phishing attacks. In China, it was reported that the National Computer Network Emergency Response Technical Team / Coordination Centre of China (CNCERT/CC) received 223 Phishing reports from over 33 worldwide financial and security organization.

a. Attack Techniques Nowadays: the nature of attacks is more active rather than passive. Previously, the threats were all passive such as password guessing, dumpster was diving and shoulder surfing. Here are some of the techniques used by the attackers today:

*b. Trojan Attack:*The attacker installed a Trojan, such as key logger program, on a user's computer. This happens when users visited certain websites and downloaded programs. As they are doing this, key logger program is also installed on their computer without their knowledge. When users log into their bank's website, the information keyed in during that session will be captured and sent to the attacker. Here, the attacker uses the Trojan as an agent to piggyback information from the user's computer to his backyard and make any fraudulent transactions whenever he wants.

c. Man-in-the-Middle Attack: Here, the attacker creates a fake website and catches the attention of users to that website. Normally, the attacker was able to trick the users by disguising their identity to make it appear that the message was coming from a trusted source. Once successful, instead of going to the designated website, users do not realize that they actually go to the fraudster's website. The information keyed in during that session will be captured and the fraudsters can make their own transactions at the same time.



Step 1 (attacker sends spoof email)

Diagram On How Information Is Being Compromised

D. Striking A Balance

Presently, Internet banking customers only need a computer with access to the Internet to use Internet banking services. Customers can access their banking accounts from anywhere in the world. Each customers is provided a login ID and a password to access the service. It is indeed easy and convenient for customers. However, the use of password does not provide adequate protection against Internet fraud such as phishing. The problem with password is that when it has been compromised, the fraudsters can easily take full control of online transactions. In such cases, the password is no longer works as an authentication token because we cannot be sure who is behind the keyboard typing that password in. However, easy access and convenience should not be at the expense and mercy of the security of information. This is important in order to ensure the confidentiality of information and that it is not being manipulated or compromised by the fraudsters. There are several methods of ensuring a more secure Internet banking:

a. Minimum Requirement: Two Factor Authentication Based on the above method, the security measures in place are not adequate to prevent fraud. The current method of using only one factor of authentication definitely has its weaknesses. The security aspects of Internet banking need to be strengthened. 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. MyKAD is a good avenue to introduce the second factor.The above security measures will greatly minimize incidents of Internet banking fraud. The smartcard here provides a second layer of authentication.This will stop a perpetrator even if he manages to obtain the user's password. Intercepted passwords cannot be used if fraudsters do not have the Smartcard. Besides addressing fraudulent activities, this can instill customers' confidence in Internet banking.

b. Additional Requirement: Three Factor Authentication However, for a better security, a three factor authentication process should be considered. The third authentication factor is the use of biometric such as iris or thumbprint recognition. This ascertains who one is, biologically. This method of authentication has been introduced by the Employee Provident Fund (EPF) for it members, but is limited to getting the latest statements of a member. With a three-factor authentication a more secure method can be implemented - a password to ascertain what one knows, a token (smartcard) to ascertain what one has, and biometric recognition (for example fingerprint or thumbprint) to ascertain who one biologically is. As such, if passwords have been compromised, fraudsters need to get through another two levels of authentication to access a customer's account. This would be difficult, if not totally impossible.

V. CONCLUSION

The providers of Internet banking services must be more responsive security requirements. While there is no doubt that Internet banking transaction should have layered protection against security threats, the providers should approach security considerations as part of their service offerings.

Currently, there are no formal processes being put in place to determine the level of security provided by these service providers and to what minimum standards they should be. Local financial institutions should consider the above-mentioned recommendations to ensure confidentiality of customer information. However, there is a cost implication to the above recommendation. Part of the costs is already taken care of by MyKAD - a multipurpose digital application card for all citizens over the age of 12. The additional costs are the hardware and software for the card reader and biometric recognition. However, this is indeed a serious matter that needs to be looked into by the relevant authorities in this country. In the long run, the cost involved to implement better security will be worth it and beneficial to the banking industry.

VII. REFERENCES

1. National Security Agency's collection of security recommendation guides (www.nsa.gov)
2. http://antiphishing.org/APWG_Phishing_Activity_Report_Feb05. pdf
3. The importance of file security, control and reliability www.novell.com/products/netware/nw6_w_importance.html
4. Computer Security Technology Planning Guide http://seclab.cs.ucdavis.edu/projects/history/cd
5. Administering Trustworthy Computing www.microsoft.com/technet/treeviewproddocs
6. Center for Internet Security (www.cisecurity.com)
7. International Common Criteria information portal www.commoncriteria.org
8. The Complete Reference Network Security.
9. Smith, Ben and Komar, Brian. Microsoft Windows Security Resource Kit(Microsoft Press, 2003)
10. Strassberg, Gondek, Rollie. The Complete Reference: Firewalls.
11. Stephen, Nortcutt. Inside Network Perimeter Security. Indianapolis: New Riders Publishing, 2003
12. Desman, Mark B. Building an Information Security Awareness Program. Auerbach Publishing 2003.
13. Peltir, Thomas R. Information Security Policies, Procedures and Standards: Guidelines for Effective Information Security Management. CRC Press, 2001.