View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia - Social and Behavioral Sciences 65 (2012) 364 – 369

Procedia
Social and Behavioral Sciences

International Congress on Interdisciplinary Business and Social Science 2012

(ICIBSoS 2012)

Biometrics Technologies Implementation in Internet Banking Reduce Security Issues?

Normalini, M.K.[a*], T. Ramayah [b]

[ab]*School of Management, Universiti Sains Malaysia, 11700 Minden, Penang, Malaysia*

Abstract

Information security is a great concern to computer users, which is not only a technical problem, but also related to human factors. One of the main issues in Malaysia related to Internet banking is the weak security in Internet banking application. Therefore this study will investigate further the solution to enhance the security issues in Internet banking implementation. In today's high speed world, millions of transactions occur every minute. For these transactions, data need to be readily available for the genuine people who want to have access, and it must be kept securely from imposters. There are three basic approaches to the verification of an individual's identity: something you have (e.g. Debit card), something you know (e.g. password, PIN) and something you are (e.g. fingerprint), which is unique about yourself and cannot be shared. Moreover, the benefits of investigating biometric authentication systems in online banking will secure the log in process to the system and removes password vulnerabilities; enhanced convenience such as employees quickly log in using their finger; reduced help desk costs by eliminating calls for password resets. Many systems utilize a combination of these methods in order to increase the level of security. Thus, a possible option is to introduce biometric authentication.

© 2012 The Authors. Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
Selection and peer-review under responsibility of JIBES University, Jakarta

Keywords: Security; Biometrics technologies; Authentication; Phishing; Internet banking

1. Introduction

As a continually growing financial service of electronic commerce, Internet banking requires the development and implementation of a sound security procedure. The existing literature highlights

* Corresponding author. Tel.: +6012-4628794
E-mail address: normalini_mk@yahoo.com

1877-0428 © 2012 The Authors. Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
Selection and peer-review under responsibility of JIBES University, Jakarta
doi:10.1016/j.sbspro.2012.11.135

security as the primary factor which determines the adoption of Internet banking technology. The secondary information on Internet banking development in Malaysia shows a very slow growth rate. The number of Internet banking users is growing not just in Malaysia, but throughout the world. The convenience of using Internet banking to perform banking facilities 24x7 gives an edge over the delivery channels offered previously such as phone banking, fax banking, kiosk and online banking through dedicated lines to the bank. Generally, Malaysians are accepting Internet banking with open hands. However, besides the advantages of Internet banking there are issues that need to be dealt with. These issues are big in nature and the awareness about it among the Malaysians and banking customers in specific are growing in nature. The main issue is about trusting the Internet banking (Ooi, 2002) due to security reasons. Tan and Teo (2000) found risk to be a very significant factor, and, Ndubisi, Sinti and Chew (2004) agreed the importance of adequacy of security in order to raise the confidence of public to utilize the system. Poon (2008) examined the factors affecting the adoption of e-banking services in Malaysia in light of the ten determinants namely convenience, accessibility, feature availability, bank management and image, security, privacy, design, content, speed, and fees and charges revealed that security, privacy and convenience are important factors contribute to users acceptance of e-banking.

2. Malaysia Internet Banking Security Implementation

E-banking refers to the use of the Internet as a remote delivery channel for providing services such as opening a deposit account, transferring funds among different accounts and electronic bill presentment and payment (Ahmed, Zairi, & Alwabel, 2006). According to Ahmed et al. (2006), banks in Saudi Arabia are moving slowly and with caution into the e-banking because their concerns for security and reliability. In the UK, a large proportion of the population have access, at work, at home or both, to personal computers and this in turn has seen the increasing acceptance and use of the Internet for information search and purchases via the Internet (Littler & Melanthiou, 2006). However, the rate of adoption has been slower than originally envisaged. According to Littler & Melanthiou (2006), the apparent reluctance to commit partially or exclusively to Internet banking may result from concerns about the security of Internet banking accentuated by some well publicized breakdowns. The Malaysian banking security policy shall comply with the requirements of Bank Negara Malaysia pertaining to the privacy and confidentiality of the information and transactions as well as the need to maintain the security and integrity of the system. Below are security procedures and requirements which designed to ensure the optimal security of the information .

2.1 Data Privacy, Confidentiality and Integrity

In order to ensure the privacy, confidentiality and integrity of the information which are exchanged, disclosed, shared, stored or used on the system and the transactions, the bank engaged the use of a combination of authentication, encryption and auditing mechanisms which serve as powerful barriers against all forms of system penetration and abuse. These mechanisms which are engaged included:

- Secure Sockets Layer (SSL) Channel
- 128-bit Encryption
- Username & Password protection and authentication
- Firewalls and
- Account-locking

All of which have been thoroughly tested in a series to protect and safeguard against known security issues and prevent any form of tampering or theft of information or transactions.

2.2 Authentication

Distinct usernames, PINs, passwords and preferred security question and answer ("access codes") will be used to verify the identity of customers. These access codes will act as a key to access, customer relevant account(s), financial information and the banking facilities, products and services offered via the banking system. To ensure the integrity of these access codes, customers are advised to maintain its confidentiality by not sharing it or making it accessible to any other person.

2.3 Non-Repudiation

Banks also maintain and constantly update the logs of the transactions which record, among others, the transactions entered into by customers and the nature, time, and date, all of which serves to enable and to verify various transactions made and act as evidence should there ever arise.

2.4 Access and System Design

The system is designed and developed with the primary and the utmost intention of safeguarding the security and integrity of all information and transactions at all times. Banks also adopt a variety of monitoring and review measures upon the security and integrity of the system, which include:

- Enhanced data-encryption methods
- Anti-virus detection, prevention and protection procedures
- Firewall barriers and
- 24/7 surveillance and detection

3. Malaysia Internet Banking Threats and Analyzing E-Commerce Security Framework

Computer crimes cover a variety of different illegal activities and have been changing from year to year as the technology changes. It has become more and more complex and sophisticated as the years go by and becomes more and more difficult to overcome. As the computer technology advances progressively, the types of computer crimes committed also evolves with the technology in which more and more sophisticated crimes are committed. The advancement of computer technology has helped criminals in committing more complex and sophisticated crimes which are harder to detect. As the Malaysian society becomes more and more technology-savvy and Internet savvy due to the encouragement by the government and the country's vision to be a world leading country in computer technology with the Multimedia Super Corridor better known as MSC project, the number of computer-related crimes is on the rise (Mohamed & Maskat, 2007). Another type of crime is e-commerce cheating or better known as "phishing". Phishing is derived from fishing. Phishing is a term used for a short of fraud where phishers send out spoof email to random database to fool the recipient into divulging personal information like credit card details, usernames and passwords, that can be used for identity theft. Phishing is one of the most well knows and fastest growing scams on the Internet today (Singh, 2007). Phishing scam is another type of crime that showed and increment in recent years where the targets are customers of Malaysian and foreign banks. There were reports of fake websites of foreign banks hosted in Malaysia and several of these websites were running from a compromised server in Malaysia (Raslan, 2004).

One of the critical success factors of e-commerce is its security. E-commerce will simply not work when customers do not have the confidence in the security of their credit card numbers as well as other sensitive personal information. However, the successful functioning of e-commerce security depends on a complex interrelationship among several components, including the application development platforms, database management systems, systems software and network infrastructure. Weakness in a single

component can jeopardize security. To analyze e-commerce security framework, the initial framework will be the relationship between the security needs of e-commerce and threats to e-commerce security, the relationship between threats to e-commerce security and technologies to counter threats and lastly is the relationship between technologies to counter threats and tools to implement these technologies (Someswar, Sam, & Sridhar, 2002). Various authors (Deitel, Deitel, & Steinbuler, 2001; Stallings, 1999) have examined the needs of e-commerce security and in general it can be classified as access control, privacy/confidentiality, authentication, non-repudiation and availability. Access control is discussed first because, if access control is properly implemented, many other security problems, like the lack of privacy, will either be eliminated or mitigated. Some of the common threats to e-commerce securities are gaining physical access to premises, wiretaps, packet sniffing, impersonating, gaining access to information, integrity, non-repudiation, viruses and denial of service attacks. However, there are technologies available to counter these threats such as access control and intrusion detection technologies, biometrics, firewalls, encryption schemes and technologies and strategies for virus protection. The tools needed to implement these technologies comprise of namely e-commerce development languages or software (e.g. JAVA), database management system (e.g. ORACLE), operating system (e.g. LINUX) and networking equipment (e.g. CISCO). Organizations could analyze e-commerce security framework to either design new security infrastructures or assess the strengths and weaknesses of current security infrastructures to eliminate duplications, conflicts as well as enhance the current security level.

4. Authentication Technologies

Security for financial transactions is of vital importance to financial institutions providing or planning to provide service delivery to customers over the public Internet, as well as to suppliers of products, services, and solutions for Internet based e-commerce. According to Gupta, Lee, & Rao (2009), with security incidents such as identity theft and account hijacking undermining customer confidence, slowing adoption rates and threatening profits, it is very evident that requirement to go beyond mere passwords for authentication is real and important. In general, the three factors that might be used in an authentication system are:

- Something a user knows (a password or Personal Identification Number (PIN));
- Something a user has (a device such as a smart card or token);
- Something a user is (biometrics).

Traditionally, passwords and PINs have been used as the most commonly used authentication factor. There are benefits and drawbacks of a number of technologies. However, Biometrics is essentially an automated process of the recognition of individuals through a physiological or behavioral characteristic. As the biometric characteristic is part of the user, it cannot be forgotten, lost or stolen. Therefore this technology is more convenient than devices that a user must carry around and certain types of attack relevant of cards or tokens are eliminated.

Countering the threat of fraud is a continuing process requiring constant vigilance and keeping one step ahead of the fraudsters. Ultimately, the choice of authentication solutions will also be different for each bank, depending on its assets, the risks the organization considers acceptable, and the costs of the (considered) security measures. One helpful consideration is to determine to what extent the technology should be compatible with existing infrastructure and ever more changing regulatory and technological landscapes. No single security technology offers a “silver bullet”. The choice of an authentication system requires trade-offs against customer convenience and acceptability. The need for stronger consumer authentication in e-commerce environments has developed into a necessary means of reaffirming consumer safety, confidence, and acceptance. Username and passwords, used as a common authentication by many institutions are no longer sufficient to guarantee suitable access control to consumers’ accounts. Institutions should be proficient in making stronger user authentication within the online environment to protect their clients and preserve confidence and acceptance (Williamson, 2006).

Biometrics technologies is not something new in Malaysia since government sector has implemented in the National Registration Department or "JPN" which represents the largest user of biometrics. "Mykad" as identity card keeps biometrics data through embedded microchip. Besides that immigration department has implemented auto gate system installed at the entrance of the country and airport as an authentication system by using a thumb print scanner to match with a passport embedded microchip which keeps biometric data. A financial institution such as traditional banking also requires thumb print scan to authenticate each risk transaction.

The security issues can be enhanced by using biometric technologies. This is supported by many researchers (Alhussain & Drew, 2009; Ashbourn, 2004; Uzoka & Ndzinge, 2009) on implementation of biometric technologies in online application. Biometrics industry has been tremendously growing in developed countries like US and Japan. There are many gadgets being introduced in those countries in order to facilitate the current lifestyle. The card-less payment system should be replaced and there must be more easier, reliable, secure, cash free and tension free payment system such biometric payment system in which nobody have to take with them dozens of cards for shopping, travelling, pass to enter the office, university or bank as door lock, internet online shopping and many kinds where card system is installed (Kumar & Ryu, 2009). The research conducted in Sweden by Brobeck and Folkman (2005) shows that companies believe that biometrics is for organizations with a very high security need. Furthermore the result shows that individuals are positive towards biometrics. Finger-scan is the most known of, trusted and preferred technology. Most likely because it is a mature identification technique that have been around for a long time. Fahad, Rami, and Mumtaz (2008), stated that the majority of Saudis would have a preference to use fingerprint identification methods. The study by Fahad, Rami, and Mumtaz (2010b) has confirm the acceptance of biometrics authentication system using fingerprint are practically and culturally accepted by the Saudis. Another research conducted by Fahad, Rami, and Mumtaz (2010a), on the acceptance to use the biometric authentication system in the online banking environment can be predicted by using Technology acceptance model.

Past literature above shows the acceptance and biometric technology implementation and it has been implemented in certain government departments, the issues that it is new and impossible to implement in other areas should not arise and this technology should grow to enhance the security level of the authentication system.

5. Conclusion

In Malaysia, as we are moving towards a developed country by the year 2020, it is believed that biometrics could be a key driver of growth in Malaysia. From the perspective of the significance of biometric technologies and global needs and national needs which are in alignment, Malaysia can contribute and even lead the biometric technologies as to accomplish the mission to be a developed country. As the Malaysian government emphasize on security and privacy protection in the financial, economics, and politics, it is undeniable that biometric technology could contribute in achieving that mission. Therefore, this study will look into the biometrics technology implementation solution in an Internet banking environment.

References

Ahmed, A. M., Zairi, M., & Alwabel, S. A. (2006). Global benchmarking for internet and e-commerce applications. *Benchmarking:An International Journal, 13*(1/2), 68-80.

Alhussain, T., & Drew, S. (2009). Towards User Acceptance of Biometric Technology in E-Government: A Survey Study in the Kingdom of Saudi Arabia. *International Federation for Information Processing*, 26-38.

Ashbourn, J. (2004). *Practical Biometrics: From Aspiration to Implementation.*: SpringerVerlag.

Brobeck, S., & Folkman, T. (2005). *Biometrics- Attitudes and factors influencing a breakthrough in Sweden.* Master thesis, Jonkoping University.

Deitel, H., Deitel, P. J., & Steinbuler, K. (2001). *E-businesses and E-commerce for Managers.* Englewood Cliffs, NJ: Prentice-Hall.

Fahad, A. H., Rami, Q., & Mumtaz, K. (2008). *The feasibility of biometrics authentication in e-commerce: User acceptance.* Paper presented at the IADIS International Conference WWW/Internet., Freiburg, Germany.

Fahad, A. H., Rami, Q., & Mumtaz, K. (2010a). Towards an Understanding of User Acceptance to Use Biometrics Authentication Systems in E-Commerce: Using an Extension of the Technology Acceptance Model. *International Journal of E-Business Research, 6*(3), 34-55.

Fahad, A. H., Rami, Q., & Mumtaz, K. (2010b). Users' acceptance of secure biometrics authentication system: Reliability and validate of an extended UTAUT model. *Communications in Computer and Information Science, 87*(2), 254-258.

Gupta, M., Lee, J., & Rao, H. R. (2009). Implications of FFIEC Guidance on Authentication in Electronic Banking. *IGI Global*. Retrieved from http://books.google.com.my/books?hl=en&lr=&id=rE9yaepbeLIC&oi=fnd&pg=PT294&dq=implications+of+FFIEC&ots=b2SDHvWQmt&sig=SbVfoM5PZiLpk2WJKm-BCmADDqQ&redir_esc=y#v=onepage&q=implications%20of%20FFIEC&f=false

Kumar, D., & Ryu, Y. (2009). A brief introduction of biometrics and fingerprint payment technology. *International Journal of Advanced Science and Technology, 4*, 25-38.

Littler, D., & Melanthiou, D. (2006). Consumer perceptions of risk and uncertainty and the implications for behaviour towards innovative retail services: The case of Internet Banking. *Journal of Retailing and Consumer Services, 13*, 431-443.

Mohamed, N. A., & Maskat, R. (2007). *Computer Crime: The Malaysian Approach.* Paper presented at the Proceedings of the International Conference on Electrical Engineering and Informatics, Indonesia.

Ndubisi, N., Sinti, Q., & Chew, T. M. (2004). *Evaluating Internet banking adoption in Malaysia using the decomposed theory of planned behavior.* Paper presented at the International Logistics Congress Proceeding, Izmir.

Ooi, J. (2002, April 16). E-Banking is here to stay, *News Strait Times*.

Poon, W. C. (2008). Users' adoption of e-banking services: the Malaysian perspective. *Journal of Business & Industrial Marketing, 23*(1), 59-69.

Raslan, S. (2004, April 21). Vandals giving government websites grief., *The Star*.

Singh, N. P. (2007). Online frauds in Banks with phishing. *Journal of Internet Banking and Commerce, 12*(2), 1-27.

Someswar, K., Sam, R., & Sridhar, N. (2002). A framework for analyzing e-commerce security. *Information Management and Computer Security, 10*(4), 149-158.

Stallings, W. (1999). *Cryptography and Network Security Principles and Practise.* Englewood Cliffs, NJ: Prentice-Hall.

Tan, M., & Teo, T. S. H. (2000). Factor influencing the adoption of Internet banking. *Journal of the Association for Information Systems, 1*(5), 1-44.

Uzoka, F. M. E., & Ndzinge, T. (2009). Empirical analysis of biometric technology adoption and acceptance in Botswana. *The Journal of Systems and Software, 82*, 1550-1564.

Williamson, G. D. (2006). Enhanced Authentication In Online Banking. *Journal of Economic Crime Management, 4*(2).