Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 32 (2012) 260 – 272

Procedia Engineering

www.elsevier.com/locate/procedia

I-SEEC2011

A Comparative Analysis of Internet Banking Security in Thailand: A Customer Perspective

P. Subsorn[a] and S. Limwiriyakul[b*]

[a]Suan Dusit Rajabhat University, Bangkok, 10300, Thailand
[b]SECAU Security Research Centre, Edith Cowan University, Joondalup , 6027, Western Australia

Elsevier use only: Received 30 September 2011; Revised 10 November 2011; Accepted 25 November 2011.

Abstract

Internet technology has influenced everyday life during the past few decades because of its capability to assist and enhance operational and managerial performance in both non-business and business industries. Furthermore, security issues have become more common nowadays in internet technology particularly on internet banking systems due to the harmful impact on confidentiality, integrity and privacy of the bank and its customers. In the previous research, we investigated the internet banking security system of 16 selected Australian banks. The findings from that research revealed that there were deficiencies in internet banking security in all 16 of the selected Australian banks which were likely to affect the confidentiality of the existing and potential customers of the banks. The aim of this paper was to further the scope of the research by investigating internet banking security in another country. It examined 12 Thai commercial banks and compared the results/findings obtained from the previous research paper to generate a feasible guideline for Thai commercial banks. The investigation revealed that there was a distinct lack of internet banking security information provided on all the selected Thai banks' websites as compared to the selected Australian banks which provided better internet banking security information.

Keyword: Customer perspective; Internet banking; Security; Thai commercial banks

1. Introduction

The Internet has become a significant feature in almost every industry [1, 2, 3]. The banking industry is one of the most significant in terms of online presence and online banking services [3, 4]. The Internet is an enabling technology whereby an ordinary industry maybe be modernized to take advantage of

* Corresponding author. *E-mail address*: slimwiri@our.ecu.edu.au.

doi:10.1016/j.proeng.2012.01.1266

electronic commerce (e-commerce) where banking alternatives and convenience are provided to the banks' customers [3, 5]. In providing internet banking systems to their internet banking customers, most of the banks have revised their business strategies, plans and policies to maximize benefits, improve performance and decrease operational costs [3, 6, 7, 8, 9]. Consequently, these improved strategies, plans and policies allow internet banking customers to gain access to their bank accounts and make transactions around the clock and around the world [2, 3, 10]. In 2000, Thai commercial banks were permitted by the Bank of Thailand (BOT) to provide electronic transaction services along with traditional transaction services to their customers [4]. However, information security threats and risks variously classified as low, medium and high have occurred with the introduction of these internet banking systems [3, 11]. The primary concerns for both the internet banking customers and the banking industry are privacy and security of internet banking transactions and personal information confidentiality [3, 6, 12].

The most widespread internet banking security threats and risks are adware, malware, spyware, keyloggers, phishing, Trojans, and viruses [3, 13, 14, 15]. These risks and threats have the capability to manipulate typical banking customers [3, 14, 15, 16] and their information for illegal gain.

Thus, an examination of the security of internet banking systems of Thai commercial banks based on the information provided on the banks' websites was the main objective of this paper. Consequently, existing internet banking customers can gain further knowledge and information in order to assess their own security weaknesses and better secure their internet banking accounts through a checklist. Moreover, potential internet banking customers can be provided with a security background and concept of internet banking security prior to the selection of a bank for the commencement of their online banking.

2. Methodology

A comparative analysis was employed in this paper in two main parts as a qualitative research method. The availability of internet banking security features of the Thai commercial banks was firstly investigated by conducting a descriptive analysis. This was followed by the comparison between selected Thai commercial banks and Australian banks in order to investigate the differences in the internet banking security features between the two countries.

2.1. Sample

Currently, there are 13 financial institution types or 130 financial institutions in Thailand. These are comprised of (i) 14 Thai commercial banks; (ii) 2 retail banks; (iii) 1 subsidiary; (iv) 15 foreign bank branches; (v) 3 finance companies; (vi) 3 credit financiers; (vii) 25 foreign bank representatives; (viii) 21 Assets Management Companies (AMC); (ix) 8 specialized financial institutions; (x) 1 Thai Asset Management Corporation (TAMC); (xi) 1 National Credit Bureau Co., Ltd.; (xii) 11 credit card companies; and (xiii) 25 personal loan companies [17, p. 1].

For the purposes of this paper 12 out of 14 Thai commercial banks that provided internet banking services were selected for the comparative analysis and for the formulation of the proposed internet banking security checklist. The other financial institution types were not examined as they were not fully operational bank types and did not offer internet banking services [17]. Nonetheless, Thanachart Bank Public Company Limited and Siam City Bank Public Company Limited (SCIB) were individually analyzed at the time of the analysis as they were using different security features on their internet banking security systems prior to and after merging. The list of the selected Thai commercial banks utilized in the analysis is provided in Table 1.

2.2. Data collection

A secondary data source which was publicly and readily available via the selected banks' websites was employed in this paper to evaluate their internet banking security features.

Additionally, we adopted and adjusted the proposed internet banking security checklist from our previous research paper for the purpose of investigating the security features of the selected banks to generate a more applicable internet banking security checklist for Thai commercial banks. External validity for the other associated sectors or organizations can be obtained through the results and findings from the proposed internet banking security checklist to be utilized as a guideline for enhancing their own operations on internet banking security systems. The internet banking security checklist is displayed in detail in the following section.

2.3. The proposed internet banking security checklist

This checklist consists of six main security feature categories and one additional supported security feature category that banks offer and make available to their internet banking customers. These categories are (1) general online security and privacy information to the internet banking customers; (2) Information technology (IT) assistance, monitoring and support; (3) software and system requirements and settings information; (4) bank site authentication technology; (5) user site authentication technology; (6) internet banking application security features; and (7) languages. Each of these security feature categories were analyzed in detail respectively in Section 3.

3. Analysis of the websites of selected Thai banks

Table 1 presents and summarizes the analysis and results findings with the discussions in the following sub-sections.

	Represents		Represents		Represents
✓	Yes	*	Optional	na	Not applicable
A	AES 256-bit encryption	E	Entrust Authentication Services	K	Akamai Subordinate CA 3
R	RC4 128-bit encryption	V	VeriSign Authentication Services		
e	English	c	Chinese	j	Japanese

Table 1. A summary of the proposed internet banking security checklist

		Thai Commercial banks											
Security feature categories		Bangkok Bank	Bank of Ayudhya (Krungsri)	Kasikorn Bank (KBank)	Krung Thai Bank (KTB)	Thai Military Bank (TMB)	Siam Commercial Bank (SCB)	Siam City Bank (SCIB)	Standard Chartered Bank (Thai)	Thanachart Bank	United Overseas Bank (Thai) (UOBT)	Kiatnakin Bank	CIMB Thai
General online security and privacy information to the internet banking customers													
1.1	Account aggregation or privacy and confidentiality												
1.1.1	Complied with the national privacy principles and privacy law	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1.2	Losses compensation guarantee												
1.2.1	Responsibility with conditions provided by the bank			✓	✓	✓			✓	✓			
1.2.2	No responsibility	✓	✓				✓	✓			✓	✓	✓
1.3	Online/internet banking security information												
1.3.1	Hoax email, scam, phishing and spyware	✓	✓	✓	✓	✓	✓		✓			✓	✓
1.3.2	Trojan and virus		✓	✓					✓		✓		
1.3.3	Keylogger								✓		✓		
1.3.4	General online security guidelines	✓	✓	✓			✓	✓	✓			✓	✓
1.3.5	Security alert/up-to-date issue	✓											
1.3.6	Provides password security tips	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓
1.3.7	Other security information								✓				
1.4	Bank security mechanism system												
1.4.1	Antivirus protection		✓		✓		✓	✓		✓		✓	
1.4.2	Data encryption	✓	✓	✓	✓		✓	✓					
1.4.3	Firewall (s)	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	
1.4.4	Intrusion Detection System (IDS)/alert system	✓			✓		✓	✓		✓			
1.4.5	Other/general information		✓			✓							✓
1.4.6	No information												
IT assistance, monitoring and support													
2.1	Hotline/helpdesk service availability												
2.1.1	24/7 customer contact centre by phone	✓	✓	✓			✓	✓	✓				
2.1.2	Not 24/7 customer contact centre by phone				✓	✓				✓	✓	✓	✓
2.1.3	Via email	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
2.1.4	Secured email												

		Thai Commercial banks											
	Security feature categories	Bangkok Bank	Bank of Ayudhya (Krungsri)	Kasikorn Bank (KBank)	Krung Thai Bank (KTB)	Thai Military Bank (TMB)	Siam Commercial Bank (SCB)	Siam City Bank (SCIB)	Standard Chartered Bank (Thai)	Thanachart Bank	United Overseas Bank (Thai) (UOBT)	Kiatnakin Bank	CIMB Thai
2.1.5	Frequent Ask Question (FAQ)/online support form/chat	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2.2	Internet banking transaction monitoring by the banks												
2.2.1	Provides dedicated team and technology		✓					✓					
2.2.2	No information	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓
Software and system requirements and settings information													
3.1	Compatibility "best" with the popular Internet browsers (based on the bank's information provided)												
3.1.1	Chrome	✓		✓	✓								
3.1.2	Firefox	✓		✓	✓								
3.1.3	Internet Explorer	✓	✓	✓	✓				✓	✓	✓		✓
3.1.4	Netscape												✓
3.1.5	Opera			✓									
3.1.6	Safari	✓		✓									
3.1.7	No information					✓	✓	✓				✓	
3.2	Internet banking user device system and browser setting requirement												
3.2.1	Operating system	✓	✓						✓		✓		
3.2.2	Type of browser	✓	✓	✓	✓				✓	✓	✓		✓
3.2.3	Browser setting										✓		
3.2.4	Screen resolution	✓			✓				✓	✓	✓		✓
3.2.5	Browser automatic or manual test feature available	✓											
3.2.6	No information					✓	✓	✓				✓	✓
3.3	Free/paid security software/tool available to the internet banking customers												
3.3.1	Antivirus/anti-spyware	✓		✓	✓								
3.3.2	Internet security suite												
3.3.3	Provides Internet links to security software vendor(s)	✓											
3.3.4	No information		✓			✓	✓	✓	✓	✓	✓	✓	✓
Bank site authentication technology													
4.1	Employed encryption and digital certificate technologies												
4.1.1	Secure Socket Layer (SSL) encryption	A	R	A	R	R	A	A	A	A	R	R	A

		Thai Commercial banks											
	Security feature categories	Bangkok Bank	Bank of Ayudhya (Krungsri)	Kasikorn Bank (KBank)	Krung Thai Bank (KTB)	Thai Military Bank (TMB)	Siam Commercial Bank (SCB)	Siam City Bank (SCIB)	Standard Chartered Bank (Thai)	Thanachart Bank	United Overseas Bank (Thai) (UOBT)	Kiatnakin Bank	CIMB Thai
4.1.2	Extended validation SSL certificates	✓	✓	✓	✓							✓	✓
4.1.3	Signing Certificate Authority (CA)	V	V	V	V	E	E	V	K	E	V	V	V
User site authentication technology													
5.1	Two-factor authentication for logon and/or for transaction verification available												
5.1.1	Token device			✓		✓	✓	✓			✓		
5.1.2	Short Message Service (SMS)	✓	✓	✓		✓			✓	✓			✓
5.1.3	Email		✓			✓				✓			
5.1.4	Not in use				✓							✓	
5.2	Logon requirement												
5.2.1	Bank/credit cards number or bank register/customer ID or email address	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.2.2	Password/personal code or security number	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.2.3	Other e.g. CAPTCHA				✓								
5.2.4	Two-factor authentication					✓							
5.3	Logon failure limitation												
5.3.1	Max. (times)	3	3	3	3								
5.3.2	No information					✓	✓	✓	✓	✓	✓	✓	✓
5.4	Logon user input type												
5.4.1	Keyboard	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.4.2	Keypad							*		*			
5.5	Scramble an on-screen input keypad												
5.5.1	Customer ID	na	na	na	na	na	na	na	na	na	na	na	na
5.5.2	Password	na	na	na	na	na	na	✓	na	✓	na	na	na
5.6	Password restriction/requirement												
5.6.1	Enforce good password practice							na		na			
5.6.2	Password length (characters)						6-8	6		6		8+	8
5.6.3	Combination of numbers and letters							na		na		✓	✓

		Thai Commercial banks											
	Security feature categories	Bangkok Bank	Bank of Ayudhya (Krungsri)	Kasikorn Bank (KBank)	Krung Thai Bank (KTB)	Thai Military Bank (TMB)	Siam Commercial Bank (SCB)	Siam City Bank (SCIB)	Standard Chartered Bank (Thai)	Thanachart Bank	United Overseas Bank (Thai) (UOBT)	Kiatnakin Bank	CIMB Thai
5.6.4	Combination of upper and lower cases							na		na			
5.6.5	Special characters							na		na			
5.6.6	Different passwords as compared to any of previous used passwords							na		na			
5.6.7	Automatically check password strength when creating or changing password							na		na			
5.6.8	No information	✓	✓	✓	✓	✓			✓		✓		
5.7	Transaction verification												
5.7.1	Some external transactions required token/SMS/email	✓	✓	✓		✓	✓	✓	✓	✓	✓		✓
5.7.2	Other method e.g. password												
5.7.3	No information				✓							✓	
Internet banking application security features													
6.1	Automatic timeout feature for inactivity												
6.1.1	Max. (mins)	15	15									15	
6.1.2	In use but does not specify timeout length				✓		✓	✓		✓	✓		✓
6.1.3	No information			✓		✓			✓				
6.2	Limited default daily transfer amount to third party account/BPAY/international transactions												
6.2.1	Less or up to Thai ฿ 100,000						✓		✓				
6.2.2	More than Thai ฿ 100,000	✓	✓	✓		✓		✓					
6.2.3	The default maximum daily limit transfer is vary depend on the type of the internet banking customer	✓				✓			✓				
6.2.4	The maximum daily limit transfer may be increased with the approval by the banks	✓							✓				
6.2.5	The maximum daily limit transfer may be changed by the customer	✓				✓							
6.2.6	No information				✓					✓	✓	✓	✓
6.3	Logging information												
6.3.1	Last login	✓							✓				

		Thai Commercial banks											
	Security feature categories	Bangkok Bank	Bank of Ayudhya (Krungsri)	Kasikorn Bank (KBank)	Krung Thai Bank (KTB)	Thai Military Bank (TMB)	Siam Commercial Bank (SCB)	Siam City Bank (SCIB)	Standard Chartered Bank (Thai)	Thanachart Bank	United Overseas Bank (Thai) (UOBT)	Kiatnakin Bank	CIMB Thai
6.3.2	Activity log	✓											
6.3.3	No information		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓
6.4	Notifications and Alerts												
6.4.1	Via email	✓	✓	✓			✓		✓				
6.4.2	No Information				✓	✓		✓		✓	✓	✓	✓
6.5	Session management												
6.5.1	Session or Page tokens												
6.5.2	Clear session cookie information after logoff or shut down the Internet browser				✓	✓	✓		✓				
6.5.3	Cookie not in use							✓	✓				
6.5.4	Cookie uses for other purpose									✓			✓
6.5.5	No information	✓	✓	✓							✓	✓	
Languages													
7.1	Support other language(s)	e	e	e, c, j	e	e	e	e	e	e	e	e	e

3.1. *Encryption and digital certificate*

Almost half of the selected Thai commercial banks (six out of 12) have employed extended validation SSL certificates whereas the other remaining seven banks only used standard validation. Upgrading from standard to extended validation SSL certificates will provide a better alternative of the bank's existing SSL certificate to its customers. This measure will better ensure the confidentiality of banking customers when using the Internet or other online banking services. In addition, the majority of the selected Thai commercial banks have signed with the VeriSign Authentication Service for their CA. More details are provided in Table 1 in Section 4.1.

3.2. Languages

All of the selected Thai commercial banks have both Thai and English languages on their websites available to their customers. Furthermore, KBank provides multi-languages which include Chinese as well as Japanese. More details are provided in Table 1 in Section 7.1.

3.3. Logging information

Bangkok and Standard Chartered banks are the only two out of 12 selected Thai commercial banks who have declared that they provide logging information such as last login and activity logs on their websites. The 10 remaining Thai commercial banks have not provided logging information on their websites. The provision of such information can increase the confidentiality in criterion in internet banking security to both existing as well as potential internet banking customers. More details are provided in Section 6.3 in Table 1.

3.4. Logon requirement

All of the 12 selected Thai commercial banks require customer ID or user ID as well as password for logon. Furthermore, KTB required a Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) incorporated with the user ID and password. Thus, this extra input interactive element increased the security of its logon authentication process. In addition, TMB banks has deployed and enforced a two-factor authentication method into their internet banking logon process. Table 1 in Section 5.2 elaborates on this.

3.5. Logon user input type

Two out of the 12 selected Thai commercial banks have deployed a keypad with a scramble method for a password input type. Therefore, the password input screen keypad will change every time the webpage is opened. Nevertheless, this keypad is only an alternative for the internet banking customers of SCIB and Thanachart bank. The imposition of a virtual keyboard for banking customer logons enhances security by reducing the potential risk of keylogger attacks on customers' computers. Table 1 in Section 5.4 summarizes the login user input type of the 12 selected Thai commercial banks.

3.6. Password requirements/restrictions

There was a lack of password requirements and restrictions information on seven out of 12 of the websites of the selected Thai commercial banks. The majority of the remaining five selected Thai commercial banks have provided some password requirements information such as length and character type. Three out of these five selected Thai commercial banks required a minimum password length of six characters. Typically the minimum password length should be any combination of eight alphanumeric characters. However, a longer length is more secure and recommended. See Table 21 in Section 5.6 for more details.

3.7. Session management

Five out of 12 selected Thai commercial banks have not offered any session management information on their websites. KTB, TMB and SCB declare on their websites that they will clear session cookie information after internet banking customer logoff or shutdown of the Internet browser. Both Thanachart and CIMB Thai banks claim that they occasionally use cookie technology for other non-related internet banking purposes such as statistical information. Providing session management information such as cookie, page and session tokens will increase awareness as well as confidentiality to both existing and potential internet banking customers. See Table 1 in Section 6.5 for more information.

3.8. Two-factor authentication

The majority of the 12 selected Thai commercial banks have utilized a two-factor authentication technique for their internet banking transaction verifications. However, both Krung Thai and Kiatnakin banks are the minority who do not use a two-factor authentication technique. SMS is the most widely used two-factor authentication technique followed by token device and email respectively. See Table 1 in Section 5.1 for more information. In addition, only TMB has used a two-factor authentication technique for the logon process. 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. See Section 5.2 for more details.

3.9. Websites information not up-to-date

Six out of 12 selected Thai commercial banks have provided wrong SSL encryption information on their websites. Five of these selected Thai commercial banks have used 256-bit encryption although their websites display that 128-bit encryption is being used. The other remaining six have deployed 128-bit encryption but indicated 256-bit encryption on their websites. See Section 4.1 in Table 1 for more details. In addition, the Thai version website of Standard Chartered Bank claims that they have not employed cookie technology, yet the English version in the data protection and privacy policy section states that “we will occasionally use a "cookie" and/or other similar files or programs”. This misinformation may create uncertainty or mistrust in customers’ minds particularly about the use of cookies.

4. Comparison between the selected Australian banks and the selected Thai commercial banks

4.1. Account aggregation or privacy and confidentiality

All of the 16 selected Australian banks have complied with the Australian privacy principles and privacy laws. Similarly, all of the 12 selected Thai commercial banks have also acted in accordance with the Thai national privacy policies and laws. However, there were variations in the details in each privacy policy depending on the selected Thai commercial bank.

4.2. Losses compensation guarantee

Ten out of the 16 selected Australian banks have similar policies to compensate customers for any losses occurred, whereas five out of the 12 selected Thai commercial banks have similar policies to compensate for the losses of customers with the banks’ conditions. Conversely, seven out of 12 selected Thai commercial banks used liability waiver clauses to by stating on the internet banking application forms in the services condition section, that they will accept no responsibilities for any losses occurred by internet banking customers or other illegal or non-authorized users.

4.3. Extended validation SSL certificate

Nine out of the 16 selected Australian banks have employed extended validation SSL certificates, whereas six out of the 12 selected Thai commercial banks have employed extended validation SSL certificate technology.

4.4. Internet banking transaction monitoring by the banks

Only two out of 12 selected Thai commercial banks have provided information about internet banking transaction monitoring on their websites. While 14 out of 16 selected Australian banks have provided this information on their websites.

4.5. Languages

All of the websites of 12 selected Thai commercial banks supported at least two languages which were Thai and English. Only KBank supported two additional languages which were Chinese and Japanese. In comparison, all of the 16 selected Australian banks only supported the English language.

4.6. Logon user input type

The majority of both the selected Australian and Thai banks allow their customers to use keyboard as their input type for logon to the bank website. The minority of the selected banks from both Australian (3) and Thai (2) have deployed keypad technology for logon input type purposes for their internet banking customers. However, two out of three selected Australian banks have made the virtual keypad compulsory. On the other hand, both the selected Thai commercial banks have made their virtual keypad as optional to their internet banking customers.

4.7. Online/internet banking security information

All of the 16 selected Australian banks provide general security information guidelines on their websites, whereas only eight out of 12 selected Thai banks provided such information. There was a lack of internet banking security information about keyloggers on both the selected Australian and Thai banks. Only two banks out of 16 selected Australian as well as two out of 12 selected Thai banks provided keyloggers information on their websites. Furthermore, there was only one selected Thai commercial bank which provided information about internet banking security alerts or up-to-date issues, whereas six of the selected Australian banks have provided such information on their websites.

4.8. Password restriction/requirements

The majority of the selected Australian banks provided more information to their internet banking customers regarding password restriction/requirements as compared to most of the selected Thai commercial banks. Only one out of 16 selected Australian banks has not provided password requirements information on its website. In contrast, seven out of 12 of the selected Thai commercial banks have not provided password requirements information on their websites.

4.9. Two-factor authentication for logon and/or for transaction verification available

Half of the selected Australian banks (eight out of 16) have deployed two-factor authentication for logon and/or for transaction verification whereas, the majority of the selected Thai commercial banks (10 out of 12) have used two-factor authentication. Moreover, three out of the 10 selected Thai commercial banks have email as an alternative two-factor authentication to their internet banking customers. Using email as two-factor authentication method was not used in all of the 16 selected Australian banks.

Table 2 presents the summary comparison information between the 16 selected Australian and the 12 selected Thai banks

Table 2. A summary comparison information between the 16 selected Australian and the 12 selected Thai banks

Security feature information on bank website	**The 16 selected Australian banks**		**The 12 selected Thai banks**	
	Number	Percentage (%)	Number	Percentage (%)
National privacy laws and principles compliance	16	100	12	100
100% loss compensation guarantee	10	62.50	5	41.67
Extended validation SSL certificate protection	9	56.25	6	50.00
Provision of information with respect to monitoring Internet banking transaction	14	87.50	2	16.67
Multi-language support	0	0	12	100
Logon user input mechanism via keyboard	10	62.50	12	100
Logon user input mechanism via virtual keypad	3	18.75	2	16.67
Provision of appropriate general Internet banking security information guideline	16	100	8	66.67
Provision of appropriate Internet banking security information such as security alert issues	6	37.50	1	8.33
Appropriate Internet banking information for security threats such as keyloggers	2	12.50	2	16.67
Logon password minimum requirement information	15	93.75	5	41.67
Two-factor authentication for logon and/or for customer transaction verification	8	50	10	83.33

5. Conclusions and recommendations

There were several similar internet banking security issues for the selected Thai commercial banks. Most of the selected Thai commercial banks have been deficient in providing internet banking security information to their existing and potential internet banking customers. Moreover, information on password requirements should be mandatory and the password security strengthened to have at least a minimum of 8 characters. This is due to the fact that longer password lengths offer better security by being harder to crack. In addition, the selected Thai commercial 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. Furthermore, the Thai government authority should take formal steps in the form of regulations or legislation to ensure that all of the operating banking institutes provide appropriate internet banking security information on their websites. Finally, education awareness programs between banks and universities as well as government sectors should be developed and implemented in order to provide security awareness such as potential risks and threats information to all existing and potential internet banking customers.

References

[1] Gunasekaran A, Love P. Current and future directions of multimedia technology in business. *International Journal of Information Management* 1999; **19(2)**: 105-120.

[2] Karim Z, Rezaul KM, Hossain A. Towards secure information systems in online banking. in: *International Conference for Internet Technology and Secured Transactions(ICITST 2009)*, London, 2009.

[3] Subsorn P, Limwiriyakul S. A Comparative analysis of the security of Internet banking in Australia: A customer perspective. in: *2nd International Cyber Resilience Conference (ICR2011)*, Perth, Western Australia, 2011.

[4] Hamid MRA, Amin H, Lada S, Ahmad N. A comparative analysis of Internet banking in Malaysia and Thailand. *Journal of Internet Business* 2007; **4**: 1-19.

[5] Steinfield C. Understanding click and mortar e-commerce approaches: A conceptual framework and research agenda. Journal of Interactive Advertising 2002; **2(2)**: 1-10.

[6] Hutchinson D, Warren M. Security for Internet banking: A framework. *Logistics Information Management* 2003; **16(1)**: 64 -73.

[7] the National Office for the Information Economy (NOIE), the Australian Bankers Association (ABA), the Australian Information Industry Association (AIIA). Banking on the Internet: A Guide to Personal Internet Banking Services [cited 2011 April]; Available from: http://www.archive.dcita.gov.au/1999/08/banking; 1999.

[8] Boonruang S. Electronic commerce: Waiting for the laws to pass, Bangkok: The Post Publishing plc; 2000.

[9] Chudasri D. A cosy club no longer. in Bangkok Post; 2002.

[10] Gurau C. Online banking in transition economies: The implementation and development of online banking systems. *International Journal of Bank Marketing* 2002; **20(6)**: 285-296.

[11] Usonlinebiz. Types of Internet banking and security threats [cited 2011 April]; Available from: http://www.usonlinebiz.com/article/Types-of-Internet-Banking-and-Security-Threats.php; 2008.

[12] Hutchinson D, Warren M. A framework of security authentication for internet banking. in: *International We-B Conference (2nd)*, Perth, Western Australia, 2001.

[13] BankMuscat. Internet banking security threats [cited 2011 April]; Available from: http://www.bankmuscat.com/en-us/ConsumerBanking/bankingchannels/internetbanking/Pages/InternetBankingSecurityThreats.aspx; 2009.

[14] Ekberg P, Li S, Morina G. Online banking access system : Principles behind choices and further development, seen from a managerial perspective [cited 2011 April]; Available from: http://www.essays.se/essay/6974685cb6/; 2007.

[15] RSA. RSA 2010 global online consumer security survey [cited 2011 April]; Available from: www.rsa.com/.../consumer/.../10665_CSV_WP_1209_Global.pdf; 2010.

[16] Georg L, Frefel C, Hämmerli B, Liebenau J, Kärrberg P, Posch R. The value of information security to European banking [cited 2011 April]; Available from: www.personal.lse.ac.uk/LIEBENAU/BankingSecurityDETECOM.doc; 2009.

[17] Bank of Thailand (BOT). Lists of financial institutions [cited 2011 July]; Available from: http://www.bot.or.th/Thai/FinancialInstitutions/WebsiteFI/Pages/instList.aspx; 2011.