การศึกษาเปรียบเทียบด้านความปลอดภัยของระบบธนาคารผ่านอินเทอร์เน็ตระหว่างประเทศกัมพูชาและประเทศไทย

A Comparative Study on the Safety of Internet Banking Systems between Cambodia and Thailand

รัชนา สุข[1], สมนึก พ่วงพรพิทักษ์ [2]

Rachana Sok[1], Somnuk Puangpronpitag [2]

Received: 14 October 2015; Accepted: 17 February 2016

บทคัดย่อ

เนื่องจากการแพร่ขยายของการเข้าถึงเครือข่ายอินเทอร์เน็ตทั่วโลก ทำให้การใช้งานระบบธนาคารผ่านอินเทอร์เน็ตได้เติบโตไปอย่างรวดเร็ว โดยการใช้งานธนาคารผ่านอินเทอร์เน็ต มีประโยชน์ที่ให้ความสะดวกแก่ลูกค้าได้เป็นอย่างดี แต่อย่างไรก็ตาม ความปลอดภัยของการใช้บริการดังกล่าว ยังเป็นที่กังวลยิ่ง ดังจะเห็นได้จาก มีกรณีการโจมตีธนาคารผ่านระบบอินเทอร์เน็ตถูกรายงานอยู่บ่อยครั้ง ดังนั้นในช่วงไม่กี่ปีที่ผ่านมา จึงมีการศึกษาวิจัยจำนวนมากเพื่อเข้าใจ ถึงประเด็นด้านความปลอดภัยของธนาคารผ่านอินเทอร์เน็ต แต่ยังไม่มีการศึกษาในเชิงเปรียบเทียบ ด้านความปลอดภัยของระบบธนาคารผ่านอินเทอร์เน็ต ระหว่างประเทศไทยและประเทศกัมพูชา ดังนั้นในงานวิจัยนี้ จึงได้เสนอทำการศึกษาเชิงเปรียบเทียบ ด้านความปลอดภัยของระบบธนาคารผ่านอินเทอร์เน็ต ระหว่างธนาคารในประเทศไทยและประเทศกัมพูชา อย่างละสามแห่ง โดยการศึกษาจะทำ โดยการสังเกตการณ์จุดอ่อนจุดแข็งของการให้บริการจริงๆ ของธนาคาร ตั้งแต่สมัครใช้งาน จนถึงทุกรายละเอียดของการใช้งานในแต่ละขั้นตอน โดยใช้เกณฑ์การสังเกตการณ์ ที่เกิดจากการบูรณาการความรู้ที่ได้จาก การวิเคราะห์คดีความด้านธนาคารผ่านอินเทอร์เน็ตในอดีต ร่วมกับแนวทางที่ระบุไว้ในมาตรฐานด้านความปลอดภัย และการวิเคราะห์งานวิจัยที่ศึกษาด้านนี้ในอดีต จากผลการสังเกตการณ์ ได้พบจุดอ่อนและจุดแข็งเชิงเปรียบเทียบระหว่างสองประเทศ และยังได้เสนอแนวทางในการปรับปรุงปัญหาความปลอดภัยดังกล่าว

Abstract

Due to widespread internet access, deployment of internet banking systems has expanded exponentially. Banking on the internet has notable advantages, particularly in terms of convenience however, safety remains a major concern. Several different crimes have been committed against internet banking sites during the last few years, electronic robbery being one of the most common. As a result, several studies have recently been undertaken to better understand the safety issues of internet banking. Yet, to the best of our knowledge, none of the studies compare the safety of internet banking systems between Cambodia and Thailand. Hence, this paper proposes to comparatively study the safety issues of internet banking of three separate banks in Thailand and three banks in Cambodia. The study was done by observing the strength and weakness of the internet banking services by deploying every step of a transaction. The observation criteria were specified by integrating the knowledge from the following: analyzing past internet banking crime cases, following the guideline of the safety standard and analyzing previous literature. From our observations, we found some strengths and weaknesses in both of the countries. This study provides some meaningful guidelines that address the system's comparative strengths and weaknesses.

Keywords: Internet Banking System, Safety, Evaluation, Cambodia, Thailand

---

[1] *นิสิตปริญญาโท, [2]อาจารย์, สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม อำเภอกันทรวิชัย จังหวัดมหาสารคาม 44150 ประเทศไทย*

[1] *Master's degree student, [2]Lecturer, Department of Computer Science, Faculty of Informatics, Mahasarakham University, Kantarawichai District, Maha Sarakham 44150, Thailand.*

* *Corresponding author: Somnuk Puangpronpitag, Lecturer, Department of Computer Science, Faculty of Informatics, Mahasarakham University, Kantarawichai District, Maha Sarakham 44150, Thailand. somnuk.p@msu.ac.th*

Introduction

Recently, internet technology has permeated into every aspect of our lives. Most industries have integrated this modern technology to serve their customers. Also, banks have provided internet banking systems. The internet banking system is the new way for banking services over the internet. It allows the customers to conduct financial transactions, such as balance inquiry, financial transfer, bill payment, transaction review, online top-up and so on. The internet banking system[1] in Thailand was first originated in 1999 by Siam Commercial Bank (SCB). Yet, the internet banking in Cambodia was first introduced in 2013 by Acleda bank. The internet banking systems in Cambodia are still in their infancy compared to Thailand. Several studies have been done on customer perspective analysis and security comparison of the internet banking systems in Thailand with other countries. For example, Subsorn *et al.*[2,3] investigated and compared customer perspectives of internet banking systems between Australian and Thailand, also between Thailand and China. Rangsan *et al.*[4] did studies on three banks in Thailand by focusing on the impact of customer satisfaction. Moreover, most of the previous works[5,6,7] have studied customer perspectives and internet banking security. Also, Putla *et al.*[8] compared the internet banking systems of six banks in Thailand.

Yet, none of these studies address the safety of internet banking between Thailand and Cambodia. So, this paper aims to comparatively study the internet banking of three banks in Thailand and three banks in Cambodia. Furthermore, this paper uses different thorough methods to analyze safety issues and compares them with previous literature. We take an in-depth observation on the real deployment of the internet banking services, from applying for the services to the details of every step of usage. The criteria of observation were established by integrating the followings: (1) analyzing internet banking crime cases of the last few years, (2) following guideline of the well-known ISO/IEC 27002 safety standard, and (3) analyzing previous literatures on internet banking safety evaluation.

The rest of this paper is organized as follows: First, we review the relevant literature. Next, we observe and compare the internet banking of three banks in Cambodia and three banks in Thailand. Finally, we summarize our findings and provide future direction.

Literature Review

1. Internet Banking in Cambodia and Thailand

According to (Figure 1)[9,10], the amount of bank customers and cash deposits of Cambodia and Thailand have dramatically grown during the past 6 years. This increase of customers has created more workload for the bank's counter services. So, internet banking becomes very useful for banks to help reduce counter workload. For the customer, the internet banking system also brings a big convenience, such as saving travel expense and time, 24/7 service accessibility, and so on.

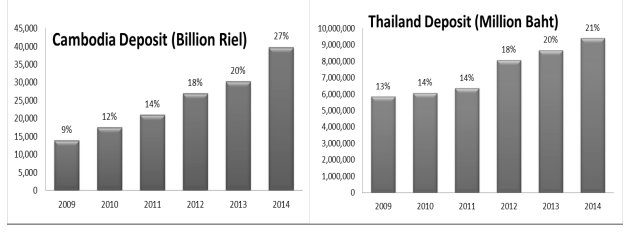


Figure 1 Cambodia and Thailand Deposit Amounts

In Cambodia, the internet banking systems are still in the beginning stages because their banks have only provided typical services since 2013. Now there are 13 banks among 25 commercial banks[9] that have deployed internet banking systems for their customers. In Thailand, internet banking systems have been deployed since 1999 by Siam Commercial Bank (SCB). Recently, all 15 commercial banks in Thailand have deployed internet banking systems for their customer. The Bank of Thailand (BOT) statistics[10] have shown that internet banking users in Thailand have increased from 4 million users (in 2010) to 9 million users (in 2014).

2. Safety vs. Security

In general, safety and security have more or less the same meaning. However, in term of security engineering, these two words mean different things[11]. Safety is related to the management issues like technical defects, accidental deletion, errors, human/ethic, and so on. Yet, security is related to technical issues like

hardware sabotage, hacker intrusion, firewall and so on. Not only the meaning is different, but the translation also different too. Safety is translated to 'សុវត្ថិភាព' (sovat-te-pheap) in Khmer and 'ความปลอดภัย' (kwam-plod-phai) in Thai, while security is translated to 'សន្តិសុខ' (shon-ti-sok) in Khmer and 'ความมั่นคง' (kwam-maun-khong) in Thai.

These two issues are big problems for the internet banking systems around the world. Some previous studies[8,12,13] have mainly focused on security issues. They have proposed several good techniques for security issues without concern for safety issues. For example, Puangpronpitag *et al.*[13] has proposed a protection mechanism again SSL stripping attack that mostly happened on the web of the internet banking systems. Yet, their main focus is on the technical (security) side, not on the safety issues. However, according to the internet banking crime cases (reported during the last few years by the Department of Special Investigation (DSI)[14] Thailand), security is not the only factor that should be of concern. There are also management weaknesses, causing social engineering attacks. Also, user negligence, the bad management of banking services and other safety issues have caused vulnerabilities on the internet banking systems. So, this paper will mainly focus on these safety issues.

3. The Internet Banking Crime Cases

ACIS Research Lab[12] has shown that the internet banking hacking in Thailand has increased exponentially from 2003 to 2012. There are several problems with the safety issues, according to the internet banking crime cases, reported during the last few years. These safety issues could be worried by both banks and their customers. For some cases, the muggers pretend to be an account holder to register internet banking services[15] without the awareness of account holder. Furthermore, some muggers try to steal username and password. Also, some muggers steal One-Time-Password (OTP) by social engineering the mobile operator[16,17] (DTAC, AIS, True). In several cases, the muggers allure the call center's staff to reset username and password. Moreover, the popular technique that most of the hackers used is phishing mail (fraud user's confidential information or username and password by the link sent via emails). So, all of these negligence weakness can give bad effects to the internet banking systems.

In addition, more or less the same internet banking crime cases have happened all around the world. The police have found that some of these crimes were operated by international hackers, moving from one country to another. So, the aforementioned crime cases in Thailand would also concern safety issues of the internet banking systems in Cambodia.

4. Information Safety and Security Standard of the internet banking system

There are several standards, covering information safety and security system of the banks. All these standards provide valuable guidelines and risk management for the internet banking systems. The National Bank of Cambodia and Bank of Thailand have relied on the ISO/IEC 27002:2005[18] standard to measure risk management of the internet banking systems. It serves as a practical guideline (covers with 11 security control clauses, containing a total of 39 main security categories) to protect critical information and build a confidence for commercial organization. So, in this paper, we choose the ISO/IEC 27002:2005 (Code of practice for information security management) standard as a part of our criteria to analyze the internet banking systems between Cambodia and Thailand. Their details can be found in reference no. 18.

5. Related Work

Subsorn *et al.*[2] investigated and compared 16 Australian banks with 12 Thai's Banks. They[3] have also compared 13 mainland Chinese banks with 19 licensed Hong Kong banks by using six main security checklists. The results have pointed out the lack of security of several banks. However, these two studies have mainly focused on the general security issues of the internet banking services. They have not taken concern of safety issues. They have not applied to deploy real internet banking services, and learn from the real cases. Also, they have not included the internet banking crime cases and safety standards to support their checklist

criteria.

Al-Gharbi *et al.*[5] studied the internet banking systems of six banks in Oman. Three main problems have been found, namely cultural factors, language barrier, and the difficulties of developing countries to associate with e-commerce application. The results have pointed out that security and privacy are the main issues for Oman internet banking services. Oman is still lacking in internet banking education, and the computer adoption among Oman people is quite low. Oman has also faced regulation issues. All of these are main barriers in deploying internet banking services. So, user's perception of banking technology is very significant for any developing country. Karim *et al.*[6] investigated the internet banking system towards secure information among users and banks. Totally, 1,500 questionnaires were distributed on the internet (emails and social network websites) and through educational institutes in London, A total 712 feedbacks were received. Among those feedbacks, 643 were completed and used for analysis. The results found that information security policy should be included in order to avoid attacks and risks. Also, their customer's knowledge on some security issues of the internet banking, such as hacking, phishing, identity theft and fraud is still low, and should be of concern. However, none of the banks included this on the survey.

Loke *et al.*[7] investigated customer satisfaction of the internet banking in Malaysia by distributing 500 questionnaires to the respondents. The results of their investigation found that staff support & knowledge and web security & trust were significant for customers towards the internet banking services. While the customer satisfaction is also a main concern of the internet banking services, the security policy is also significant for banking transactions.

Rangsan *et al.*[4] investigated customer satisfaction among top three banks in Thailand by distributing a questionnaire to 450 respondents. The results found that an online registration time is the important factor that has an impact on customer satisfaction.

Putla *et al.*[8] have studies on both safety and security issues of six internet banking services in Thailand. The results showed that protection management of the internet banking in Thailand is capable enough to terminate all kinds of spoofing attacks to be account holder in Thailand.

Most related works studied security issues of the internet banking systems in different aspects, but not many works have focused on the safety issues. The previous studies have also had drawbacks. For example, some of them have not yet included safety and security standards to support their criteria. Most of them have not yet deployed that services to make a real observation on the cases. Some of them have not yet included the lessons learned from the internet banking crime cases as the criteria. Moreover, none of previous related studies have observed and compared the safety issues of the internet banking systems of Cambodia and Thailand.

Materials and Methods

This paper mainly aims to evaluate and compare the internet banking systems of three banks in Cambodia and three banks in Thailand, particularly focusing on the safety issues. For Cambodia, Acleda Bank (the largest bank in the country), Canadia Bank (the government shareholder bank), and Cambodian Public Bank (the top third bank of Cambodia) have been chosen as case studies. For Thailand, Bangkok Bank (the largest bank in the country), Thai Military Bank (the government shareholder bank) and Siam Commercial Bank (the first bank deploying internet banking in Thailand) are chosen as case studies.

We focus on observation and deployment of the internet banking systems, based on the personal banking account of 6 banks. The corporate accounts are not in the scope of this work. We will also propose a suggestion guideline to reinforce safety issues. As shown in (Figure 2), the observation criteria come from previous work analysis, the safety and security standard, and internet banking crime cases. So, our observations to evaluate internet banking are listed as follows:

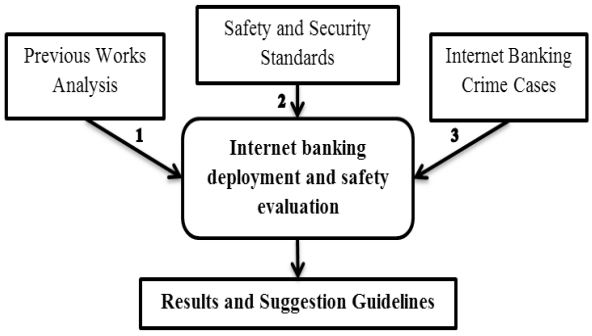
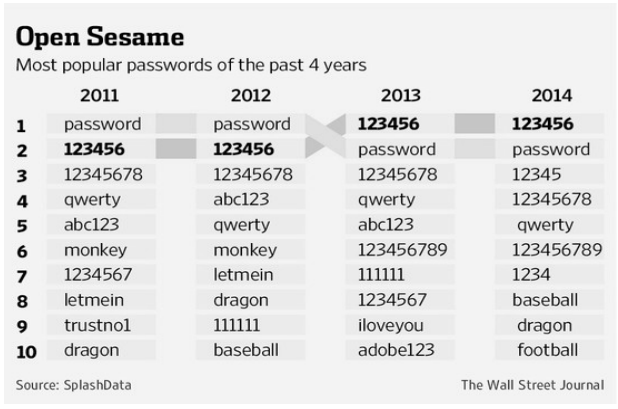


Figure 2 Research Methodology

1) We critically observe the steps of opening a bank account till the closing of the bank account. We also observe the way to register the internet banking service at a bank branch, ATM, call center and online/mobile application. Moreover, the important criteria of this section are authentication documents. Before a customer can open a bank account, and then register for an internet banking system, all banks need to authenticate the customer identity. For example, citizen identity card, passport, passbook, and other supported documents issued by government must be shown to the bank staff.

2) Internet banking username and password policy has also been included to our observation. Username and Password restriction and bank verification system play very important role to secure the internet banking system. Recently, many weak passwords have been revealed as shown in (Figure 4). Some users may set their password too weak. So, the bank password restriction policy, and the implementation of username/ password verification system have been observed.

Moreover, we have also observed on the way to delivery username and password after registration, and the way to reset username and password through bank branch, bank call center, online or ATM.



Open Sesame

Most popular passwords of the past 4 years

	2011	2012	2013	2014
1	password	password	**123456**	**123456**
2	**123456**	**123456**	password	password
3	12345678	12345678	12345678	12345
4	qwerty	abc123	qwerty	12345678
5	abc123	qwerty	abc123	qwerty
6	monkey	monkey	123456789	123456789
7	1234567	letmein	111111	1234
8	letmein	dragon	1234567	baseball
9	trustno1	111111	iloveyou	dragon
10	dragon	baseball	adobe123	football

Source: SplashData — The Wall Street Journal

Figure 3 Weak passwords from Wall Street Journal

3) A call center is a convenience service that banks deploy to help their customers, using staff to communicate and discuss with the customers via phone. However, call center can be a risk for bank to provide their services according to the previous crime cases. Some user's information can be compromised to authenticate the hackers as the real customers through this call center. For example, a user's full name, phone number, identity card number, birthdate, pet's name and so on may be easily found from the user's Facebook information. Hence, call center authentication is one of our observation points.

4) Two-factor authentication is a modern secure method that several banks deploy nowadays. Mostly, banks use one time password (OTP) as the second authentication factor to authenticate almost all transactions of the internet banking systems, such as fund transfer, bill payment, top-up, and so on. So, analyzing on OTP is one of our criteria.

5) Alerting system can help users from an incident withdrawal or a fund transfer-out by some muggers. The alert can also warn the users of several activities of their internet banking systems, such as log-in, setting change, fund transfer and so on. So, the details and approaches of implementing alerting systems (eg., via e-mail, via SMS or others) are also observed and analyzed.

6) Transaction limitation can help users from transferring money-out in unpredictable amounts by hacker. This limitation and the method to change it are parts of our observation points.

7) The use of an on-screen keyboard has also included for our analysis since it can protect users from key-loggers.

8) Some banks allow their users to pause the internet banking service through different ways, for example via a bank branch, call center and online. It can help the internet banking's customers from being harassed by some muggers. A customer can also pause or suspend his/her internet banking service immediately in emergency cases.

9) Since several internet banking systems have relied on SMS OTP, the problems of renewing mobile sim cards to take control of the victim's SMS OTP have found in several crime cases. So, how mobile operators manage the renewing process of mobile sim cards can be a big issue in the internet banking safety. In this work, three main operators in Cambodia (Metfone, Smart, Cellcard) and three main operators in Thailand (DTAC, AIS, True) have been observed for this issue. According to the crime cases[7,8], we mainly observe on authentication documents, required to request a new mobile sim-card at the operator branches.

Results

The results of observing on six banks (in Cambodia and Thailand) are presented in this paper as A, B, C, D, E, and F. We omit the real name of the banks to avoid conflicts with the bank. Without providing the real name, it can also help avoid guiding the hackers to the specific vulnerabilities of a specific bank.

According to our observation and deployment of internet banking service at three banks in Cambodia and three banks in Thailand, we have found the following:

1) Opening a bank account and registering for an internet banking account

Three banks in Cambodia allow their customers to open bank accounts and register to the internet banking through bank branch only. Three banks in Thailand allowed their users to open bank account at a bank branch only. Yet, for the internet banking, Thai banks allow the customers to register through both a bank branch and an ATM machine as shown in (Table 1). None of the six banks allows the internet banking registration via their call center.

The major difference between Cambodian banks and Thai banks is that Cambodian banks allow only the registration at the bank branch. This registering process is rather safe (up to the carefulness of bank staffs). Yet, it is inconvenient for the customers, and can increase the workloads at the bank branches.

Table 1 Internet Banking Registration

Register Through	A	B	C	D	E	F
Bank Branch	✓	✓	✓	✓	✓	✓
ATM	×	×	×	✓	✓	✓
Call Center	×	×	×	×	×	×
Mobile Application	×	×	×	×	×	✓

Moreover, the required authentication documents for opening a bank account between these two countries are quite the same. For example, citizen identity card with local residential address, and valid passport with work permit or other related documents, issued by government authorities, organization or university. We have also noticed that all banks process rather strictly on a foreigner to open a bank account and to register for the internet banking. They focus on valid visa and the staying period. If the staying period is less than 30 days, opening the bank account and internet banking account are not allowed.

For the foreigners, VISA, work permit and other documents, issued by local authorities are extra requirements for opening a bank and internet banking accounts. According to our observation on the local citizen, we have found that all five banks require the customer real citizen identity card. The photocopy is not allowed. Yet, there is a bank in Thailand (the bank F), allowing the customer to use his/her army identity card to open the bank account. In Cambodia, some banks have also trained their staffs how to carefully check whether the citizen identity card is real or fake. According to the crime cases in reference no. 15-17, the hackers have used the faked documents of other government authority identity card to open the bank account in the

name of victim; then take the control of the internet banking if the victim has not yet applied for the internet banking. So, in this case, Bank F would be vulnerable to fake army identity cards. Generally, the citizen identity card is very familiar to bank staffs. However, other government authorities' documents (such as army identity card) are not so familiar. So, when it is faked, it can be more difficult to be noticed.

Hence, it would be very important that Bank F should train their staff to validate both citizen identity cards and army identity cards properly. Otherwise, this would be a vulnerability. Furthermore, we have found that not all Thai banks have trained their staffs properly to validate the documents for opening the bank account. The lesson learnt from Cambodia practice in training the staff for this job would be deployed to Thai banks. Furthermore, Thai identity card (Figure 4) is a smartcard with an EV chip while the Cambodia citizen identity (Figure 5) can be a non-smart card.

The Cambodian government has just deployed smartcard citizen identity cards since 2013. So, there are still a lot of non-smartcard citizen identity cards, deployed in Cambodia. Since the smartcard is more difficult to be faked, Thai citizen identity cards are therefore safer from spoofing in comparison to the Cambodia one.

Figure 4 Cambodian and Thailand citizen identity cards

To register for an internet banking in Cambodia, all three banks require the customers to register for internet banking only at their bank branch. The required documents are a citizen identity card or a passport, plus a passbook, a phone number, and an e-mail. Driving license or officer identity cards are not allowed as a substitute of the citizen identity card. ATM card is optional. For Thailand's bank, the registration can be done by staffs at the bank branch, by the ATM system. For registering at the bank branch, the required documents are more or less the same as the Cambodian banks. For registering via the ATM system, the customer requires an ATM card of the bank, and a registered mobile phone number for SMS OTP. From this point, we can see that registering at the bank branch (if the bank staffs are careful enough) is obviously safe. Yet, it is inconvenient for the bank customers, and creates more workloads for the bank staffs. So, the ATM option of Thai banks can be a good choice. In terms of safety, it would be rather difficult to compromise the ATM registration because the hackers would need to steal the customer's ATM card, knowing his/her PIN and get his/her mobile phone.

After registration completed, all banks deliver the username/password in different ways as shown in (Table 2). For Cambodian Banks (A, B, C), bank A delivers a temporary username and a temporary password of a customer via a shield letter at the bank branch with an expiration of 30 days. For bank B, it sends a permanent username and a temporary password to the customer registered email with an expiration of 2 days. Furthermore, the username is set by the bank and cannot be changed by the customer. For bank C, a permanent username is manually set by the customer at the bank branch while registering. The bank sends only a temporary password to the customer registered email with an expiration of 7 days. The customer then must reset a new password within the expired date.

For Thai banks in registering at the bank branch, bank D sends a temporary username to the customer registered phone number (SMS), and sends a PIN number through post office with an expiration of 3 days. Bank E gives a temporary username and a temporary password via a shield letter at the bank branch. Bank F sends only an activation code via an SMS to the customer registered mobile with an expiration of 3 hours; and then allows setting a permanent username and a password on the internet banking web page.

Three Thai banks allow registering for the Internet banking via ATM. However, Bank E will not allow the ATM registration if the customer is not Thai. The

foreign customers of Bank E need to register their internet banking at the bank branch only.

For ATM registration, bank D and E requests the customer to setup a PIN for internet banking registration at the ATM machine. They then give a temporary username to the registered customer via an ATM slip with an expiration of 2-3 days. The customer then log-in to the internet banking web page by using the temporary username and the PIN number. The customer then set a new username and a new password for his/her internet banking system. Bank F sends only an activation code via an SMS to the customer registered mobile, and then allows setting the username and password at its internet banking web page.

Table 2 First Time Registration

Provided for First Time Registration	A	B	C	D	E	F
Through Email	✗	A	P	✗	✗	✗
Through Shield Letter	A	✗	✗	✗	A	✗
Through ATM Slip	✗	✗	✗	U	U	✗
Through Post Office	✗	✗	✗	Pi	✗	✗
Through SMS	✗	✗	✗	U	✗	Ac

Note: U: *Username;* ***P:*** *Password;* ***A:*** *Username + Password;* ***Pi:*** *PIN Number;* ***Ac:*** *Activation Code;* ✗*:Not Available*

All these different ways of authenticating the customer in registering for the internet banking seem to us rather safe. They try to use different ways to authenticate the customers, such as the user possession authentication factor (by owning the customer registered mobile phone, the customer ATM card) and the second user knowledge factor (by knowing the password of the customer registered mobile phone). The expiration periods can also help minimize the chance of attacks. The main concern would be the banks need to ensure the validity of the customer's registered e-mail, mobile phone number and postal address. After investigation, we have found that all Thai banks can ensure that by registering the customer's e-mail, mobile phone number and postal address at the bank branch during the customer opening the bank account.

2) Changing the registered e-mail, mobile phone number and postal address

The customer's registered e-mail, mobile phone number and postal address are very significant for the internet banking systems. They are deployed to authenticate the customer on the first registration, and to alert the customer of the internet banking transaction. In particular, the mobile phone number is also used as the second authentication factor in the form of SMS OTP. So, any changes to these three items must be validated properly. All Thai and Cambodian banks in this study allow the customer to change it at the bank branch, using the citizen identity card (or other documents) as an authentication factor. The safety on this case is up to the carefulness of the bank staffs to validate the authentication documents. As aforementioned, Cambodian banks specially train their bank staffs to validate such documents while Thai banks have not yet put this policy seriously.

According to our observation, we have also found that the e-mail and postal address can also be changed by going to the bank branch with citizen identity card/passport and passbook to authenticate for all 6 banks (both Thai and Cambodian). Also, we found that bank E and F allowed their customers to change their e-mail and postal address through the internet banking system. Moreover, all banks use OTPs as the second authentication of username/password to validate the changes. For the mobile number almost six banks do not allow to change through the internet banking system expect bank F as shown in (Table 3). Specially, bank F have allowed their customers can be changed the mobile number through ATM, if the old number is still uses as shown in (Table 3). For changing it via call center is not possible for all six banks in our research.

Table 3 Change Mobile Number

Changed Through	A	B	C	D	E	F
IBS	✗	✗	✗	✗	✗	✓
Bank Branch	✓	✓	✓	✓	✓	✓
Call Center	✗	✗	✗	✗	✗	✗
ATM	✗	✗	✗	✗	✗	✓

Note: ✓***: Allowed;*** ✗***:Not Allowed***

3) Username and password restriction

The bank staffs of all six banks have recommended the customers to set a good password, containing with special characters, uppercase, lowercase, and numeric. We found that all banks have set the password restriction contain a minimum of 1 alphabet (1 upper/lowercase and 1 special character), and 1 numeric. Also, we have found that bank A has set password restriction from 8 to 12 characters, bank B (6 to 16), bank C (10 to 14), bank D (8 to 32), and bank E and F (8 to 20). Moreover, bank C accepts only three special characters (@, #, and $). For bank E accepts only five special characters such as (‘), (“), (,), (&), and (spaces). Specially, bank F set it not more than 2 characters repeated on the password restriction. We have also found that bank A forces their customers to change password within 90 days, bank B (30 days) and bank C, D, E and F (60 days).

For safety reasona, long passwords are always harder to crack or guess than the short ones. At least, the best length of password should be 8 to 32 characters. It can be an average affected of user-friendliness and safety. We can see that most of six banks set it at least 8 characters except bank B (at least 6 characters). Furthermore, all of six banks have a strict password policy to avoid dictionary attack, username as the password, less or more than length, worst password announced and all numbers that have set by their customers. For example: “password1234” is a medium password but it can be guess easily. It has used to test with password restriction policy. Two banks among six banks accepted this password. It means that bank D and F still have some gaps on password restriction.

For the username, Bank A and E set it restriction from 6 to 12 characters, bank B has set by bank, bank C (according to customers), bank D (6 to 32), and bank F (8 to 20). Bank A, D, E and F have also set username restriction contain a minimum 1 alphabet and 1 numeric. Specially, bank A has set it differently like first and second character must be alphabetical but no special characters. However, bank F accepted only two special characters are (.), and (_) and also not repeating more than 3 characters like “aaa123”.

The lockout policy is a way to pause the username from log-in even the user has passed the right password. Generally, this lockout will happen, when the user has continuously passed wrong passwords for several times. All of six banks in our studies set the number of continuous wrong passwords at 3 times before locking out the username. In a way, this lockout policy is a good thing in term of safety, since it helps stop the hacker from guessing the password. However, it also creates the other safety problem since a targeted username can be easily DoS-attacked by any hackers, who want to annoy the bank customer. Furthermore, this DoS may happen by accident. From our observation on the six banks, Bank C (from Cambodia), Bank D and E (from Thailand) allow the customer to set his/her username as his/her full name. We found that this policy can create such the DoS. For example, “somnuk” is a very common first name in Thailand. There are so many people, named “somnuk” in Thailand. If the first customer (named “somnuk”) has set their username as “somnuk”, the other customer (who is also named “somnuk”) will have to set their username to something else (for example, somnukp, somnukt, and so on). Unfortunately, these “somnuk”s may forget their usernames and attempt to login as “somnuk”, unintentionally. So, they finally make the real username “somnuk” locked out due to the wrong passwords. So, we would suggest the bank to do not allow the first name as the username.

According to (Table 4), we have also found that all banks allowed their users to reset username and password differently. Mostly, all of six banks allowed their customers to reset their username and password through bank branch by holding the authentication document like citizen identity card/passport, passbook and so on.

For bank A and C, the customers can be reset only password through call center (one times only) with some authentication question. Bank D, E and F can reset both username and password through call center. To reset through online, bank A, D, E and F can reset only password through online but bank C can reset both username and password. Specially, bank F allowed their

customers to reset through mobile application. To reset through ATM machine, only two banks accepted (bank D and F). Banks D allowed both username and password but bank F allowed only password.

To confirm changing of username and password, OTP has used to authenticate with real customers by sending it through mobile SMS or token devices. Bank E has used OTP before changing, Bank F has used OTP after changing but bank D do not used any OTP.

Table 4 Username and Password Recovery

Reset Through	A	B	C	D	E	F
Through Call Center	P	✗	P	A	A	A
Through Online	✗	P	A	P	P	P*
Through ATM	✗	✗	✗	A	✗	P
Through Bank Branch	A	A	A	A	A	A

***Note: U:** Username; **P:** Password; **A:** Username + Password; **P*:** Password Through Mobile Application*

4) Call center authentication

The results of call center authentication have shown that some questions to authenticate the users can be compromised easily like full name, phone number, birth date, identity card number, current address and so on. These kinds of questions are popularly asked to authenticate with users. Moreover, some muggers are smart enough to gather all of that information easily when the user is the targeted. We have also found that the top 10 questions that most of the bank always asked to authenticate with users are: 1) Full name or username, 2) Account number or Phone number, 3) Birthdate or day of birth, 4) Email address, 5) Identity card number or passport number, 6) Last transaction activity, 7) Current Address, 8) ATM Expiration Date or PIN number, 9) Branch of open bank account, and 10) Memorable question and answer.

5) Two factor authentication and the OTPs

From our observation results, we have found that all banks deployed SMS OTP and some deployed Token OTP for their users to enhance the internet banking financial transaction and other activities. Furthermore, SMS OTP is free of charge but Token OTP is annually charge, especially for the high class customers only. In addition, bank C deployed it to general customers to used token OTP and mobile OTP (15$ and 10$ per year respectively). Moreover, we also found all of six banks in this studies set OTP with a maximum length of six digits (except bank D is eight digits) and the maximum expiration is five minutes (except bank C is 1 minute cause of token device and mobile application).

We also found that three banks in Thailand used SMS OTP to confirm with customers transactions (Table 5). For example, first time registration at log-in webpage, fund transfer, payment, add new account (except bank B not used), daily transaction limitation and changing password (except bank D not used). Especially, only one bank (bank B) in Cambodia used OTP on the log-in webpage after passing the username and password. Bank A, E and F used it on changing username and also bank A and F used it on changing phone number.

Table 5 One Time Password Deployment

OTP Deployment	A	B	C	D	E	F
1. Transaction Activity						
First Time Log-in	✗	✗	✗	✓	✓	✓
Log-in webpage	✗	✗	✓	✗	✗	✗
Fund Transfer	✓	✓	✓	✓	✓	✓
Payments	✓	✓	✓	✓	✓	✓
Add new A/C	✓	✗	✓	✓	✓	✓
2. Change settings						
Username	✓	✗	✗	✗	✓	✓
Password	✓	✓	✓	✗	✓	✓
Phone Number	✓	✗	✗	✗	✗	✓
Daily Limitation	✓	✓	✓	✓	✓	✓

Comparatively between Thailand and Cambodia, we have found that all banks in Thailand do not provide Token OTP for the personal bank account while one of three banks in Cambodia provides both token OTP and SMS OTP for personal bank accounts. The customer can

choose SMS or token one as a choice. The other two banks in Cambodia provide also token OTP but for some special personal account (called VIP account) with more deposit in the account. We suggest that Thailand should learn from Cambodia by providing a better security choice (token OTP) if the customers are willing to afford it.

Table 6 Implementation of CAPTCHA

CAPTCHA	A	B	C	D	E	F
First Time Log-in	✗	✗	✗	✓	✗	✓
Log-in Webpage	✗	✓	✗	✗	✗	✓

Particularly, we also observed on the implementation of CAPTCHA in the internet banking transactions as show in Table 6. It showed that only three in our research implement CAPTCHA. Bank B used it (called as secure code) on the log-in webpage. Bank D and F used it on the first time registration and also bank F used it on the log-in webpage after two times failure log-in.

6) Alerting system

Alerting system for the internet banking has set differently according to the internet banking transaction. Yet, it can be changed by users when needed, and it has also changed for alerting through SMS. We found that most of the bank in Thailand alert users via email (free) and mobile SMS (charge 10 to 20 baht per months). Also, all banks in Thailand deployed it in all transactions especially on log-in activity (alerted through via email). According to (Table 7), we found that three banks in Cambodia give the alert for financial transaction (such as transfer, payment, and top-up) only.

Table 7 Transaction Alerting Activities

Alerting Activities	A	B	C	D	E	F
Log-in	✗	✗	✗	✓	✓	✓
Log-out	✗	✗	✓	✓	✓	✓
Transactions	✓	✓	✓	✓	✓	✓
Change Settings	✗	✓	✓	✓	✓	✓

7) The limitation and restriction of usage

According to our observation, we have found that transaction limitation can be changed according to users in settings of the internet banking log-in webpage. The minimum and maximum amount of fund transfer, payment and top-up in Cambodia between $1,000 and $10,000, except bank C set the limitation unlimited. We also defined that all banks in Thailand automatically set daily transaction between 300,000 baht to 700,000 baht. This limitation can help assuage the situation if the account has been hacked. However, if the hackers can have both password and OTP, they will be able to get rid of this limitation easily. This is a problem for both countries.

8) The support for on-screen keyboard

Moreover, we found that only two banks (bank B and E) in our research used on-screen keyboard for the internet banking webpage. Also, Bank B used on-screen keyboard on the log-in webpage for password textbox and bank E used it for OTP and PIN number insertion box as the results show in (Table 8). We can conclude that both Thailand and Cambodia still do not take screen keyboard seriously. Only one bank from each country supports the screen keyboard option. One big problem found in the usage of a screen keyboard in the only Thai bank, applied this technique. The Bank F has applied the screen keyboard to OTP, which is useless and unreasonable. Since OTP is planned for one time usage, it is not a matter if the OTP is sniffed by any sniffers or logged by any key-loggers at all. So, it is clearly non-sense to apply on-screen keyboard in such the way.

Table 8 On-Screen Keyboard

On-Screen Keyboard	A	B	C	D	E	F
Password	✗	✓	✗	✗	✗	✗
OTP and PIN	✗	✗	✗	✗	✓	✗

9) Pausing the internet banking account

Particularly, all banks in our research allowed their users to pause the internet banking service by going through the bank branch. Only two banks in Cambodia

(bank A and C) do not allow pause the internet banking systems through call center. This can be very serious when the customer wants to report the hacking case and pauses their internet banking.

10) The observation on the mobile operators

We carefully observed six mobile centers, three operators in Cambodia and three operators in Thailand. Most of the operator branch offices in these two countries required strict authentication documents from users to request the sim-card with the same number. Mobile operators in Thailand need all customers to register the sim-card through branch office only. Small operators have rights to sale sim-card only. However, we have found that all operators in Cambodia even branch or small office have rights to request a new sim-card with showing of authentication documents. It can be a risk for Cambodia's internet banking users, if a crime happened similar to Thailand on requesting a new sim-card of the victim to get the victim SMS OTP. However, to renew the sim card with the reason of changing sim types (such as from micro-sim to nano-sim), we have found a weakness for some Thai operators. In one case, we pretend to be the owner of one mobile number and request the mobile Operator staffs to change the change the micro-sim to nano-sim. The operator let us write our phone number into a paper and give them the old sim. We did that but gave them the wrong sim (the sim of other phone number). We found that they did not check anything and give us the nano-sim of the phone number that we want. So, the previous sim of that phone number has been cut-out, and our pretend hacker can get the victim SMS OTP. This lesson guides to any bank customers that if their mobile phone, deployed as SMS OTP receiver, happens to have no signal without reason, they should try to ring their own number. If they found that it can be rung somewhere else, they should immediately contact their bank to pause the internet banking service. The previous crime case has also confirmed this weak-point. We would suggest all mobile operators to authenticate the customer more seriously (maybe, by checking the identity card) before issuing the new sim. In particular, the operators should also let the customers return the old sim and check if the old sim is the real one.

Conclusions

Summarily, we have observed the safety of internet banking comparatively between three banks in Thailand and three banks in Cambodia. We have found that Cambodia is more conservative than Thailand. So, in several cases, Cambodia's internet banking can be more secure. However, on several points, three Thai banks seem to manage the internet banking in a more convenient way. We suggest Thai banks: (1) train their staffs to be aware of safety issues on the registration process, (2) apply on-screen keyboard in the right part of e-banking system, (3) deploy the token OTPs for personal-account customer. For Cambodia, they should improve on: (1) allowing IBS registration through ATM, (2) applying CAPTCHA and the right standard of authentication documents by learning from the other side as aforementioned.

Acknowledgement

This research was supported by the Her Majesty Princess Maha Chakri Sirindhorn Scholarship. We are also grateful to Department of Special Investigation (DSI), Ministry of Justice, Thailand of providing some information on the internet banking crime cases. We would like to show our gratitude to Campu Bank staffs for their opinions and fruitful discussion on this research.

References

1. Jantori P. Security of Internet Banking - A Comparative study of security risks and legal Protection in Internet Banking in Thailand and Germany. Thailand Journal of Law and Policy (Spring) 2010;13(1):1-4.
2. Subsorn P, Limwiriyakul S. A Comparative Analysis of Internet Banking Security in Thailand: A Customer Perspective. Proceedings of 3rd International Social Science, Engineering and Energy Conference (I-SEEC); 23 March 2011; Nakhon Pathom, Thailand. pp. 260-272.
3. Subsorn P, Limwiriyakul S. A Case Study of Internet Banking Security of Mainland Chinese Banks: A

Customer Perspective. Proceedings of the 4th International Conference on Computational Intelligence, Communication Systems and Networks; 24-26 July 2012; Phuket, Thailand. pp. 189-195.

4. Rangsan N, Titida N. The Impact of Internet Banking Service on Customer Satisfaction in Thailand: A Case Study in Bangkok. Proceedings of the International Journal on Humanities and Management Sciences (IJHMS); 2013; pp. 101-105.
5. AL-Gharbi KN, Khalfan AM, Al-Kindi AM. Problems of Electronic Commerce Applications in a Developing Country: A Descriptive Case Study of the Banking Industry of Oman. Proceedings of 5th International Conference on Computing and Informatics (ICOCI); 6-8 June 2006; Kuala Lumpur, Malaysia. pp. 1-6.
6. Karim Z, Rezaul KM, Hossain A. Towards Secure Information Systems in Online Banking. Proceedings of the International Conference on Internet Technology and Secured Transactions (ICITST); 9-12 November 2009; London, UK. pp. 1-6.
7. Loke SP, Noor NM, Khalid K. Customer Satisfaction Towards Internet Banking Services: Case Analysis on a Malaysian Bank. Proceedings of IEEE International Conference Colloquium on Humanities, Science and Engineering Research (CHUSER); 3-4 December 2012; Kota Kinabalu, Sabah, Malaysia. pp. 159-163.
8. Puangpronpitag S, Putla P. An Analysis of Safety and Security for Internet Banking in Thailand. Proceedings of the 11th National Conference on Computing and Information Technology (NCCIT) 2015; 2-3 July 2015; Bangkok, Thailand. pp. 99-105.
9. National Bank of Cambodia. [serial online]. Available from: http://www.nbc.org.kh. Accessed November 1, 2015.
10. Bank of Thailand. [serial online]. Avialable from: http://www.bot.or.th. Accessed November 1, 2015.
11. Schmeh K. Cryptography and Public Key Infrastructure on the Internet. The Atrium, Southearn Gate, Chichester: Jonh Wiley & Sons Ltd.; 2003.
12. ACIS Research Lab. Information Security Research on Thailand's Internet Banking/ Mobile Banking. ACIS Article; 15 June 2014; Thailand.
13. Puangpronpitag S, Sriwiboon N. Simple and Lightweight HTTPS Enforcement to Protect Against SSL Stripping Attack. Proceeding of the 4th International Conference on Computational Intelligence, Communication Systems and Networks; 24-27 June 2012; Phuket, Thailand. pp. 229-234.
14. Department of Special Investigation (DSI), Ministry of Justice– กรมสอบสวนคดีพิเศษ. [serial online]. Available from: http://www.dsi.go.th. Accessed November 1, 2015.
15. it24hrs.com. อีกแล้ว!! เตือนภัย ลูกค้าธนาคาร แม้ไม่ได้เปิด e-Banking ก็โดนขโมยเงินได้!. [serial online] 16 August 2013;. Avialable from: http://www.it24hrs.com/2013/ stealing- money- criminal- subrogate bank/. Accessed August 16, 2015.
16. it24hrs.com. เตือนภัย Internet Banking รูปแบบใหม่!! ปลอมเป็นคุณ ด้วยหลักฐานปลอม สวมรอยโอนเงินออก สูญหลายแสน!. [serial online] 04 August 2013;. Available from: http://www.it24hrs. com/2013/hack-otpbankingchange-new-sim-card/. Accessed August 16, 2015.
17. it24hrs.com. อีกแล้ว! คนร้ายสวมรอยเป็นเจ้าของบัญชี Internet Banking โอนเงินออก สูญหลายแสน!. [serial online] 06 February 2014; Avialable from http://www.it24hrs.com/2014/hack-otp-banking-change-new-sim-card-2/. Accessed August 16, 2015.
18. Standard ISO/IEC 27002:2005. [serial online]. 01 July 2007;. Available from: http://www.slinfo.una.a c.cr/documentos/EIF402/ISO27001.pdf. Accessed September 12, 2015.