

**SECURITY AND SAFETY EVALUATION AND ENHANCEMENT
OF INTERNET BANKING SYSTEM: A CASE STUDY OF
CAMBODIAN PUBLIC BANK PLC.**

SOK RACHANA

**A thesis submitted in partial fulfillment of the requirements for
the degree of Master in Computer Sciences
at Mahasarakham University**





The examining committee has unanimously approved this thesis, submitted by Mr. Sok Rachana, as a partial fulfillment of the requirements for the Master of Science degree in Computer Sciences at Maharakham University.

Examining Committee

..... (Asst. Prof. Chatklaw Jareonpon, Ph.D.)	Chairman (Faculty graduate committee)
..... (Somnuk Puangpronpitag, Ph.D.)	Committee (Advisor)
..... (Phatthanaphong Chomphuwiset, Ph.D.)	Committee (Faculty graduate committee)
..... (Khamroun Sunat, Ph.D.)	Committee (External expert)

Maharakham University has granted approval to accept this thesis as a partial fulfillment of the requirements for the Master of Science degree in Computer Science

.....
(Asst. Prof. Sujin Butdisuwan, Ph.D.)
Dean of the Faculty of Informatics

.....
(Prof. Pradit Terdtoon, Ph.D.)
Dean of Graduate School
March 21, 2016



ACKNOWLEDGEMENTS

This thesis was granted by Her Majesty Princess Maha Chakri Sirindhorn Scholarship and Mahasarakham University Funding for Cambodian Student.

The thesis would not have been accomplished if without the help from several people. First of all, I would like to thank my advisor Professor, Dr. Somnuk Puangpronpitag for giving me a good opportunity and experience to work with his team. He has been a constant source of guidance and support during every stage of my research work. His constant feedback on technical aspects skills helped me in honing my knowledge. I express my profound gratitude to Associate Dean, Dr. Chatklaw Jareonpon, Assistant to The President in Information Technology, Dr. Phatthanaphon Chomphuwiset, Professor, Dr. Panida Songram for the courses they taught helped me to develop my skills and their recommendation to improve this research.

I was very fortunate to have many friends both within and outside the Faculty of Informatics during my Master Degree life. I thank them all for their being very supportive.

I would also like to thank Cambodian Public Bank staffs for their opinions and fruitful discussion on this thesis.

I sincerely thank the members of ISAN Lab for being helpful and supportive to me during this thesis.

I am deeply indebted to my parents and my families who have been with me throughout my life and whose love and sacrifices brought me where I am today.

Sok Rachana

TITLE Security and Safety Evaluation and Enhancement of Internet Banking System: A Case Study of Cambodian Public Bank Plc.

AUTHOR Mr. Sok Rachana

DEGREE Master Degree of Science **MAJOR** Computer Science

ADVISORS Somnuk Puangpronpitag, Ph.D.

UNIVERSITY Mahasarakham University **YEAR** 2016

ABSTRACT

Due to the widespread of internet access around the world, the deployment of internet banking systems have been growing up rapidly. The internet banking has its advantages, particularly in term of convenience of the bank's customers. Internet banking safety focuses on management and processes issues of the internet banking systems, while security concerns on technical issues of the internet banking systems. However, security issues still exists on the internet banking web log-in uniform resource locator (URL) beginning with https. Safety issues of the internet banking also still causes a big concern and problematic. There are several crime cases on robbing the internet banking, reported during the last few years. So, several studies have done to understand on security issues of the internet banking in Thailand and all around the world. Yet, to the best of our knowledge, there is one particular approach that nobody else tried to compare on both security and safety issues of internet banking systems between Cambodia and Thailand. Hence, this thesis proposes to comparatively study on both security and safety issues of three banks in Cambodia and three banks in Thailand and focusing on one case study of Cambodian Public (Campu) Bank in Cambodia. This study done by observing the strength and weakness of the real internet banking service from apply to deploying of each step and testing on testbed of Campu bank's log-in webpage. The observation criteria are specified by integrating the knowledge from analyzing the past internet banking crime cases, following the guideline of the safety and security standard and analyzing the know-how of previous literature review. From our observation and experiment will be discuss with two well-versed Campu bank's staff to share our finding with their opinions in term of security and safety of the internet banking between two countries, and provide some suggestion guidelines to improve on it.

Key words: Cambodian Public Bank, Internet Banking System, Safety, Security, Evaluation, Enhancement



CONTENTS

	Page
Acknowledgement	i
Abstract	ii
List of Tables	vii
List of Figures	ix
CHAPTER 1 INTRODUCTION	1
1.1 Rationale of the research	1
1.2 Objective of the research	3
1.3 Significance of the research	3
1.4 Scope of the research	3
1.5 Glossary	4
CHAPTER 2 LITERATURE REVIEW	6
2.1 Safety vs. Security	6
2.2 Internet Banking Systems	7
2.2.1 Benefit of Internet Banking	8
2.2.2 Problems on Internet Banking	9
2.3 Crime Cases on the Internet Banking Systems and Risks	9
2.3.1 Counterfeit Official Documents of Victims	9
2.3.2 Skim An ATM Card	13
2.3.3 The Internet Banking Risks	13
2.3.4 Crime Cases Analysis	15
2.4 Related Work	16
2.4.1 A Comparative Analysis of the Security on the Internet Banking Systems	16
2.4.2 Study on User Perspective and Privacy of the Internet Banking Systems	18
2.4.3 Authentication Factors for Internet Banking Systems	19
2.4.4 Attacking and Protection Over HTTPS	20



	Page
2.4.5 An Analysis of HTTPS Ecosystem and Scan on SSL/TLS Certificates	21
2.4.6 Previous Work Analyze	23
2.5 Banks in Cambodia and Thailand	24
2.5.1 The Case Study	24
2.5.2 Cambodia Banks	25
2.5.3 Thailand Banks	25
2.6 The Internet Banking Standard of Information Safety/Security	26
2.6.1 Information Security Standards	26
2.6.2 IS Governance Standards	26
2.7 Secure Authentication of the Internet Banking Websites	27
2.7.1 Secure Socket Layers and Transport Layer Security	27
2.7.2 Digital Certificate	30
2.7.3 Two-factor Authentication	31
2.7.4 Username and Password Selection Strategies	32
2.7.5 On Screen Keyboard	32
2.8 Penetration Testing Tools, Attacking Techniques and Interview Form	33
2.8.1 Penetration Testing Tools	33
2.8.2 Most Common Attacking Techniques on Internet Banking	34
2.8.3 Interview Form and Item Objective Congruence	36
CHAPTER 3 RESEARCH METHODOLOGY	37
3.1 Overview	37
3.2 Safety Evaluation	39
3.3 Security Evaluation	41
3.4 In-depth Interview	42
3.5 Ethical Guidelines and Suggestion	44



	Page
CHAPTER 4 RESULTS AND DISCUSSION	46
4.1 Review on Observation Criteria	46
4.1.1 Open Bank Account and Internet Banking Registration	46
4.1.2 Username and Password	47
4.1.3 Call Center Authentication	48
4.1.4 Two-factor Authentication	48
4.1.5 Transaction Limitation	49
4.1.6 Alerting System and Transaction Activity	50
4.1.7 Other Additional Mechanisms	50
4.1.8 Close Bank Account and Internet Banking Systems	51
4.1.9 Mobile Phone Service Provider (Mobile Center)	51
4.1.10 Authentication of Bank Website	52
4.1.11 Experiments	53
4.2 Results on Internet Banking Deployment and Safety Evaluation	54
4.2.1 Open Bank Account and Internet Banking Registration	54
4.2.2 Username and Password	59
4.2.3 Call Center Authentication	67
4.2.4 Two-factor Authentication	68
4.2.5 Transaction Limitation and Alerting System	70
4.2.6 Other Additional Mechanisms	71
4.2.7 Close Bank Account and Internet Banking Systems	73
4.2.8 Mobile Center	74
4.2.9 Discussion for Three Banks Results in Cambodia	75
4.2.10 Discussion for Three Banks Results in Thailand	78
4.2.11 Safety Suggestion and Enhancement for the Internet Banking Systems	80
4.3 Results on Internet Banking Security Evaluation and Experiment	82
4.3.1 Bank Authentication	82
4.3.2 Experimental Results	84
4.4 Results of In-depth Interview	86



	Page
4.5 Security Suggestion and Enhancement	87
4.5.1 Implementation of ISAN-HTTPS Enforcer	88
4.5.2 Implementation of HSTS	89
4.5.3 Implementation of Password Encryption	90
CHAPTER 5 CONCLUSION	95
5.1 Goals and Achievements in this Research	95
5.1.1 Observation and Deployment	95
5.1.2 Experiments and New Design	96
5.2 Summary and Recommendations	97
REFERENCES	98
APPENDICES	104
APPENDIX A OBSERVATION CRITERIA	105
APPENDIX B PREVIOUS WORKS COMPARISON DETAIL	115
APPENDIX C INTERVIEW FORM	118
APPENDIX D EXPERIMENT AND RESULTS	126
BIOGRAPHY	135



LIST OF TABLES

	Page
Table 2.1 Authentications and Attacks	20
Table 2.2 Web for Testing on SSL	21
Table 2.3 Comparison on Previous Works	24
Table 2.4 Problems and Protections on Secure Socket Layer	30
Table 2.5 Problems and Protections on Digital Certificate	30
Table 2.6 Problems and Protections on One Time Password	31
Table 2.7 Attacking and Protection on Username and Password	32
Table 2.8 Sample Table of IOC	36
Table 3.1 Selected Banks	38
Table 3.2 Review on Safety and Security Evaluation	45
Table 4.1 Call Center Authentication Criteria	48
Table 4.2 Close Bank Account and Internet Banking Systems	51
Table 4.3 Requirements for Open Bank Account	56
Table 4.4 Apply for the Internet Banking Systems	57
Table 4.5 Internet Banking Registration Requirements	57
Table 4.6 First Time Registration for Bank A, B and C	60
Table 4.7 First Time Registration for Bank D, E and F	61
Table 4.8 Username Limitation	62
Table 4.9 Password Limitation	63
Table 4.10 Username and Password Recovery	65
Table 4.11 Changes Mobile Number	66
Table 4.12 Call Center Authentication	67
Table 4.13 One Time Password	68
Table 4.14 One Time Password Deployment	69
Table 4.15 CAPTCHA and Other Mechanism	70
Table 4.16 Alerting System and Cost of its	71
Table 4.17 Virtual Keyboard	72
Table 4.18 Pause the Internet Banking Service	72



	Page
Table 4.19 Browser Supported	73
Table 4.20 Request New Sim-card at Operators	74
Table 4.21 Exempted Visa for Cambodia and Thailand	81
Table 4.22 Digital Certificate Results	82
Table 4.23 Supported Protocols	83
Table 4.24 SSL Scan Reports	84
Table 4.25 SSL Sniff, Strip, Heartbleed and Poodle Attacks	84
Table 5.1 Results of New Protection Mechanism	97



LIST OF FIGURES

	Page
Figure 2.1 Security and Safety	7
Figure 2.2 Internet Banking Flow	8
Figure 2.3 Fake Thailand Police ID	10
Figure 2.4 Fake Document to Open New Sim-Card	11
Figure 2.5 Fake Document to Change Name	12
Figure 2.6 ATM Skimmers and Keypad Device	13
Figure 2.7 Email Scam on Victim's Side	14
Figure 2.8 Top Certificate Authorities	22
Figure 2.9 Top Signature Algorithms	22
Figure 2.10 Diagram of SHA-1 Warning on Google Chrome	23
Figure 2.11 SSL Handshake	29
Figure 2.12 HTTPS Connection	29
Figure 2.13 On Screen Keyboard	33
Figure 2.14 Kali Linux and Cain and Abel	34
Figure 2.15 SSL Strip on Kali Linux	35
Figure 3.1 Safety and Security Evaluation and Enhancement	37
Figure 3.2 Safety Evaluation and Enhancement	40
Figure 3.3 Security Evaluation and Enhancement	41
Figure 3.4 In-depth Interview	44
Figure 4.1 SSL Strip Tested in Kali Linux	53
Figure 4.2 Heartbleed Testing Tool	54
Figure 4.3 Poodle Testing Tool	55
Figure 4.4 Cambodian and Thailand Smartcard	58
Figure 4.5 Shield Letter	59
Figure 4.6 Username and Password Sent Through Email	60
Figure 4.7 Work Permit in Cambodia	75
Figure 4.8 Family Book and Birth Evidence Issued by Local Authorities	76
Figure 4.9 Cambodian Citizen Identity Card	77



	Page
Figure 4.10 Work Permit in Thailand	78
Figure 4.11 CAPTCHA Auto Pop-up	79
Figure 4.12 SSL Strip on Bank C	85
Figure 4.13 SSL Strip on Bank E and F	85
Figure 4.14 Internet Banking Log-in Webpage after Stripping Attack	87
Figure 4.15 New Protection Design for Campu Bank	88
Figure 4.16 Process of ISAN-HTTPS Enforcer	89
Figure 4.17 No HSTS Supported and HSTS Supported	90
Figure 4.18 Implementation of HSTS on Log-in Webpage	90
Figure 4.19 Structure of Password Encryption Mechanism	91
Figure 4.20 New Protection Design for Campu Bank	92
Figure 4.21 Function for Registering the Password	92
Figure 4.22 Password Hashing	93
Figure 4.23 Defined m Value and Start Session	93
Figure 4.24 User Log-in with CAPTCHA and m Value	93
Figure 4.25 Process of Decryption Function at Server Side	94
Figure 4.26 Authentication Function	94



CHAPTER 1

INTRODUCTION

1.1 Rationale of the research

In recent years, the internet technology has changed at a staggering rate. It has permeated into almost every aspect of our lives. Also, the transformation of traditional banking towards internet banking has been a leap of change. Internet banking (also known as online banking or e-banking) is a banking service system to provide financial transactions for a wide population that relies on a network environment. The internet banking system has been deployed in order to operate and connect to the global modern market. Also, it enables many convenient services for users to access account information, transfer funds, apply for credit or debit card, trade securities, and make payment for several expenses and so on. However, the safety and security issues of internet banking are still problematic. Internet banking safety focuses on management and processes of the internet banking system, while security concerns on technical issues of the internet banking systems.

Technical issues of the internet banking must always be taken care of. For example, digital certificates [1] and Secure Socket Layer (SSL) [2] are the techniques for web servers to provide authentication, data integrity, and trusted communication when users access onto a Uniform Resource Locator (URL) beginning with https. Yet, even with several security techniques, the internet banking system still has several weaknesses. From the literatures, there are many techniques that hackers have deployed to attack victims, such as SSL sniff [3], SSL strip [4], SSL split [5], Heartbleed bug [6], Poodle attack [7], and so on.

Apart from the security issues, the safety issues are also the other concern. For example, social engineering is a deceptive act that divulges confidential information of a person by another person. There are also many protection techniques that enable users to utilize and keep private information secretive, such as password restriction, two factor authentication, token devices, One Time Password (OTP), and user's information. However, without ensuring that internet banking processes are safe and



secure, the system can be compromised even for users, who implement strong privacy techniques. For example, a hacker may send a user a fake email, with a link requesting a false change of passwords for the user's bank account. This type of deceptive act is called “phishing”. Therefore, without a complete understanding of the safety issues, an internet banking system can be easily compromised.

Recently, several studies have focused on security comparisons of internet banking systems. For instance, Subsorn et.al [8] has investigated on the internet banking security system by comparing 16 banks in Australia with 12 banks in Thailand. They have also studied the customer perspective of foreign internet banking in Australia [9]. The studies have proposed checklists to evaluate and compare on general online security and privacy information, supporting service, software and system requirement, authentication technology and application security of internet banking system.

Although several studies have analyzed and compared internet banking systems, no one has evaluated the internet banking systems on both safety and security aspects. Some of them integrate only safety. Some of them integrate only security. Finally, the hacker can find out the human mistakes and exploit some security weaknesses. From literature review, there are some drawbacks on the evaluation details. Some of them have not included the existing safety/security standards. Some have not considered the real cases on the internet banking crimes in the past. Some have not observed on the process from start till the end.

Cambodian Public Bank Plc. (Campu Bank) is a subsidiary bank of Public Bank in Malaysia. It has been operating in Cambodia since 1992. It is one of the big commercial banks in Cambodia. To the best of our knowledge, none of known research has been done to investigate the security and safety issues of this bank so far. So, this thesis will use Campu Bank as a case study. This thesis proposes to evaluate both security and safety issues of the internet banking system of the Campu Bank in comparison to other banks in Cambodia and Thailand. For the criteria of the safety/security evaluation, this thesis will synthesize them from the existing safety/security standards, the real cases on the internet banking crimes in the past and the literature review. In addition, the thesis proposes to develop solutions and guidelines for both safety and security issues. For the security solution, the thesis will mainly focus



on the application layer (particularly, the login webpage and authentication of the internet banking system).

1.2 Objectives of the research

1) To evaluate the safety and security issues on the internet banking systems of Cambodian Public Bank Plc. by comparing to other internet banking systems in Cambodia and Thailand

2) To propose suggestions and solutions of safety and security issues for Cambodia Public Bank Plc.

1.3 Significance of the research

1) To contribute an evaluation framework that can be used to evaluate Cambodian Public Bank and other internet banking systems

2) To contribute evaluation results of safety and security issues on the internet banking systems in Cambodia and Thailand by comparing their strength and weakness

3) To contribute a suggestion solution to enhance both security and safety for Cambodian Public Bank that can be also useful to other i-banking systems

1.4 Scope of the research

1) Cambodian Public Bank Plc. is the case study of this research.

2) The evaluation is done on both safety and security issues.

3) For safety issues, the observation of internet banking process of management will be done on the case study, and compare it with three banks in Thailand (Bangkok Bank, Siam Commercial Bank and Thai Military Bank) and two banks in Cambodia (Acleda Bank and Canadia Bank).

4) For security issues, the observation of internet banking process will be done on the log-in webpage with focus on protection techniques and attacking simulation (testbed) to see weakness and strength of their webpage.



5) The enhanced solution will focus on safety suggestion guidelines from the observation process, and a better the log-in webpage of Campu Bank.

1.5 Glossary

1) Cambodian Public Bank Plc (CPB or Campu Bank) [10] is a subsidiary bank of Public Bank in Malaysia, and has been operating in Cambodia since 1992. It is one of the largest and strongest domestic banks in Cambodia.

2) Internet Banking System [11] is modern technology system that deployed by banking service to their consumer. It provided financial transactions for users, flexibility, and non-stop working time. Nowadays almost every bank provides the clients with access to their accounts from anywhere and anytime.

3) Safety [12-15] refers to the management side of the system to guard against unexpected damage, incidents errors, crashes, IT crimes and failure to protect customers from social engineering.

4) Security [12-15] refers to the technical side to protect against threats and weakness of the system such as firewall, intrusion detection system (IDS), operating system (OS), and other attacks by hacker.

5) Safety evaluation [12, 13] in this thesis is the process of observation on Cambodia Public Bank's security management with the focus on internet banking strengths and weaknesses. Also, the evaluation process includes comparing it against two other banks in Cambodia, and three banks in Thailand. An interview with a banker who is an expert in terms of internet banking management will also be proposed, in order to gain more knowledge and insight.

6) Security evaluation [12, 13] in this thesis is the process of investigating the internet banking system's security mechanisms, implemented on the log-in webpage. The security evaluation also includes examining the strengths and weaknesses by implementing simulated attacks. The simulated attack techniques will be applied using

7) penetration testing tools on the internet banking webpages, and then interview the bank's security technical experts on the results.



8) Safety enhancement is the improvement of the internet banking system's safety issues by proposing new guidelines and suggestions with regard to privacy, management and compliance with the law.

9) Security enhancement is the improvement of the internet banking login webpage by implementing security mechanisms for Cambodia Public Bank, based on the results of the investigation.



CHAPTER 2

LITERATURE REVIEW

2.1 Safety vs. Security

According to Merriam-Webster dictionary [14], safety is “the condition of being free from harm or risk” while security is “the quality or state of being free from danger”. So, in general sense, safety and security have more or less the same meaning. However, in the IT safety/security field, these two words mean different things.

According to Schmeh [12],

“Safety is concerned with the guarding against accidental damages. This covers technical defects, accidental deletion, transmission errors, hard disk crashes, lightning strikes, floods, bad servicing, faulty diskettes, and the like. Yet, security is concerned with guarding against intentional damage. This includes hardware sabotage, hacker intrusion, peeking at secret data, and the like.”

Puangpronpitag [15] also said that “safety is related to management (such as rules, policies, human/trust/ethic and so on), but security is related to technical issues (such as operating system, network, firewall and so on).”

Safety is translated to ‘សុវត្ថិភាព’ in Khmer (sovat-te-pheap) [16] and ‘ความปลอดภัย’ in Thai (kwam-plod-phai) [15], while security is translated to ‘សុវត្ថិភាព’, in Khmer (shon-ti-sok) [16], and ‘ความมั่นคง’ in Thai (kwam-maun-khong) [15]. Puangpronpitag [15] has also said that safety and security are equally important.





Figure 2.1 Security and Safety

Generally, security and safety work together to ensure all kinds of techniques and management go strengthen.

Figure 2.1 show that strengthening both security and safety help us protect any IT system effectively.

So, this research focuses on both safety and security issues of internet banking systems. It does not only look at the management side (such as, the processes of opening the bank account, applying for internet banking, changing the forgotten password within local and oversea, using each internet banking functions, and so on), but also look at the technical side (such as, internet banking login-web pages, HTTPS security, other related authentication processes, and so on).

2.2 Internet Banking Systems

In the early 1990s, the commercialization of the banking services from traditional brick and mortar banks became click bank or online services to reduce bank operation costs. Since then, banks have deployed banking services online for their customer needs and other financial transaction services. Internet Banking or (Online Banking or E-banking) [11] is the financial service that allows their customers to



conduct financial transactions such as inquiry balance, transfer, bill payment, viewing transaction (recent and previous), online top up and credit union etc. To use an internet banking system, customers must first register with the internet banking service. After that, the bank will generate a username and a password for each customer to access and use the online banking services.

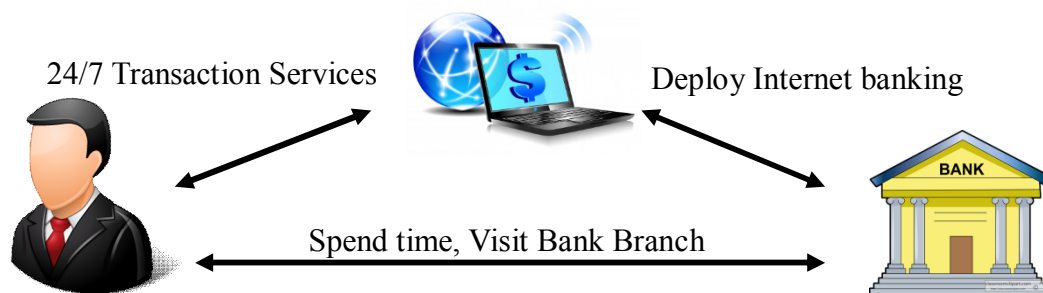


Figure 2.2 Internet Banking Flow

A customer's financial information is very important in terms of management for the bank. Financial institutions or banks have to set up various security processes to reduce the risk of unauthorized access. The security of the internet website is very vital to the integrity of the banking system, since internet banking services have become a standardized service for many financial institutions. Banking customers can now save time from having to travel to the bank and waiting on a line. Through internet banking, the customers can view balance statements, funds transfers, pay bills and online purchases. Banks also benefit by saving money on unnecessary costs, such as additional labor or longer business hours.

2.2.1 Benefit of Internet Banking

Internet banking has plenty of benefits [11]. This benefit includes convenience, better rates, quick services, easy transfers, ease of use and so on. It operates 24 hours a day, 365 days a year (24/7), which provides the full access of banking services even during the weekends and holidays. Internet banking is also fast and efficient for users to transfer funds overseas or pay bills. Users can also manage their accounts easily without going to a bank branch. Internet banking can also reduce cost, and transportation risk on keeping funds on hand to go to bank branch.



2.2.2 Problems on Internet Banking

There are many advantages of the internet banking system, but there are also some disadvantages. There was an incident where hackers stole \$300 million from one hundred banks using malware [17]. In this case, the hacker group sent malicious emails to hundreds of employees at different banks that allegedly allowed perpetrators to transfer money from the banks to fake accounts or ATMs, monitored by muggers. According to the hacker news [17], disadvantages of internet banking include:

1.-Understanding the usage of internet banking can be difficult for first time users; demo on the websites should be deployed for users to test on internet banking.

2.-No internet connection results in no access to internet banking. Slow or unreliable internet connections have also resulted in some transactions unable to complete the processes for users and banks.

3.-A secured transaction is a big problem. The internet banking can be hacked by unknown persons over the internet.

4.-Passwords can be forgotten for some users.

5.-Implementation of a new model technology can be difficult.

An improvement of internet banking has come alongside with risks. It can be useful to investigate internet banking risks and concerns to protect users from fraud and the vulnerability of their confidential information.

2.3 Crime Cases on the Internet Banking Systems and Risks

2.3.1 Counterfeit Official Documents of Victims

Evidence 1: Fake Police Identity Card to Open Bank Account

This case has happened on 4 August 2013. Mr. Rungsan Chanruangshi [18] is the victim, who has been faked his police identity card and reporting document of lost sim-card from the police. He lost 400,000 baht from his bank account. The muggers have hacked the victim as shown in Figure 2.3 and described as follows:



question for resetting password. Password cannot protect users anymore when the mugger has got their OTP.

Evidence 2: Fake Driving License to Request New Mobile Number

This case is similar to the evidence 1. It has happened on 6 February 2014. Mr. Bunaphouk Phrahumnuk [19] is the victim of this case (with the financial damage of 400,000 baht). The mugger fakes the victim's driving license and the police documents of reporting a lost sim-card, as shown in Figure 2.4

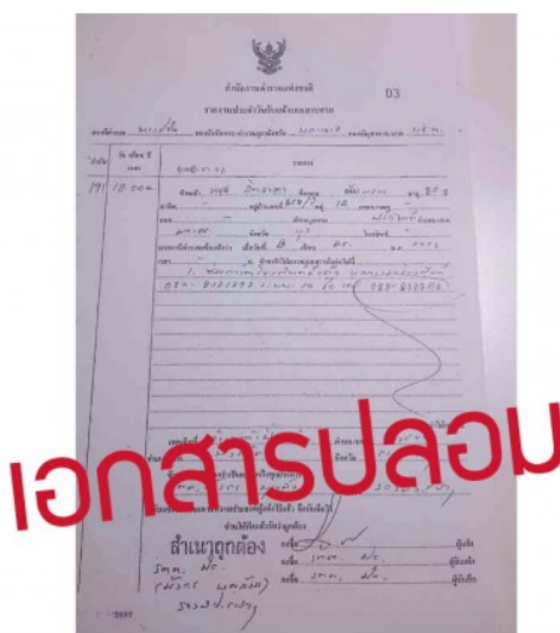


Figure 2.4 A Faked Document Reporting a Lost Sim-card

Source: [19]

From this case, the opening of online-banking can be done in the name of victim by the mugger using the faked driving license. Also, by going to a subsidiary mobile operator and requesting a new sim-card of the victim by the faked police document, the mugger can take over the victim's SMS OTP. From this case, this thesis has included the observation of requesting a new sim-card at the mobile operators as a part of observation to see the safety differences between Cambodia and Thailand mobile operators.



Evidence 3: Open bank account and register the internet banking for Victim

This case is reported on 16 August 2013. Mr. (A) Chaiyadet Siriwathanakoun (คุณไชยเดช ศิริวัฒนกุล) [20] is the victim of this case. Mr. A has never registered for internet banking. Yet, he has finally ended up with 560,000 baht lost from the internet banking. The mugger processes to change the victim's name bank account from คุณชยเดช to คุณไชยเดช (Figure 2.5) but the real name of bank account is ธนัท ศิริวัฒนกุล. On 30 April 2010, the mugger went to the (victim) a different branch of the same bank of the victim for opening bank account, and registered the internet banking in the name of Mr. A. Furthermore, the victim himself has never worked as the government warden grade 7 (เจ้าหน้าที่กรมราชทัณฑ์ระดับ 7), but the mugger has faked the document making the victim as the government warden grade 7 to open a bank account and register for the internet banking.



Figure 2.5 Fake Document to Change Name

Source: [20]



After registering the internet banking, the mugger can do all banking transactions on victim account because he have got the username, password and OTP in the name of the victim (that the victim has never even got ones). So, a part of observation criteria of our research is on faked authentication documents, alerting system and so on.

2.3.2 Skim an ATM Card

This case happened while the victim used their ATM card to withdrawal money at ATM machine. iT24hrs has reported this case on 8 May 2013 [21], 4 April 2013 [22] and 22 September 2014 [23] that, the mugger put the ATM skimming devices on ATM machine to copy victim's card and keypad to gather 4-digit password in order to withdraw money out as shown in

Figure 2.6. Our research takes this case since several bank customers can register the internet banking service through any ATM machines.

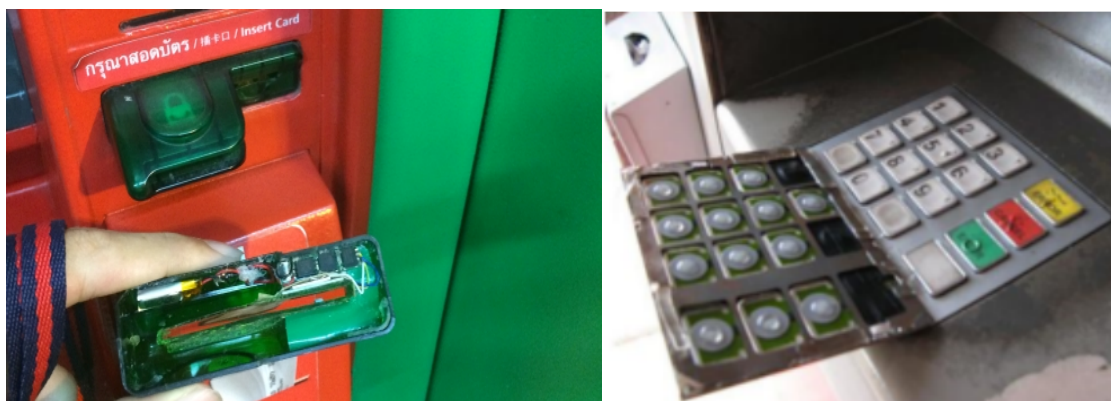


Figure 2.6 ATM Skimmers and Keypad Device

Source: [21, 23]

2.3.3 The Internet banking Risks

Risk 1: Mistake on log-in web page and user's convenience

A Pantip [24] member has posted that: "The way to make system safety by deploying the OTP every times even transfer money within owner account, it won't make sense for user convenience." It is already secured for banks that implement OTP every times for users but it has affected to user participation and the ease of use. Some



Risk 2: Phishing Mail

The screenshot shows a Yahoo! Mail interface. The left sidebar lists folders like Inbox, Drafts, Sent, Spam, Trash, and Folders. The main area displays an email from "SCB" with the subject "IMPORTANT :SCB ACCOUNT LOCKED.". The email body contains a warning about account security and includes a red box highlighting a malicious link: <http://scbeasy-web.net/Cweb/new.scbeasy.com/scbeasy.htm>.

Source: [25]

Risk 3: Movement of Hacker around the World

Hacker stole \$300 Million from 100 banks using Malware [17]. In March, 2012 – A Russian hacker (Nikokay Garifulin) was sentenced in 3 years, ordered to forfeit \$100,000 and restitution \$192,123,122 for his involvement in a bank fraud by using hundreds of phony bank account to steal over \$3 million from U.S bank accounts that was compromised by Zeus Trojan malware to record all keystrokes on the victim side. After that Garifulin started with unauthorized transfer money to the phony bank account by using visa to move and fake passport to withdraw the money in Europe with his co-conspirators.

On October 2012 – FBI arrested 14 people, who used \$1 million in 60 seconds from Citibank by withdrawing cash many times at casinos in California and Nevada. They used that money to spend on hotels, gambling and other miscellaneous for money laundry.

On May, 2013 – A gang of cyber-criminals with 7 members was sentenced in prison 10 years, 7.5 years on access device fraud and fined for \$250,000. They had stolen \$45 million from banks by target to the weakness of database of prepaid debit cards and then withdraw all the money from ATM machines, operated in 26 countries.

In July, 2013 – A group of Russian and Ukraine hackers was stolen 160 million credit card numbers over 7 years. They were accused of stealing usernames and password, personal identification information, and credit and debit card numbers.

2.3.4 Crime Cases Analysis

ACIS Research Lab [26] has shown that the internet banking hacking in Thailand has increased exponentially from 2003 to 2012. There are several problems with the management issues, according to the internet banking crime cases, reported during the last few years. These management issues could be worried by both banks and their customers.

Most cases have happened with the customer's bank account attack by some muggers. They pretend to be an account holder to register internet banking services that some users never absorbed in it. Some muggers try to steal username and password. Some muggers steal One-Time-Password (OTP) through mobile operators (like DTAC, AIS, True), or allure the call center's staff to reset username and password.



Furthermore, the popular technique that most of the hackers used is phishing mail. 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 the other country. So, the aforementioned crime cases in Thailand would also be concerned for the management issues of the internet banking systems in Cambodia.

2.4 Related Work

2.4.1 A Comparative Analysis of the Security on the Internet Banking Systems

Subsorn et al. [8, 9, 27, 28] has investigated on the security of the internet banking in Australia, Thailand and China by proposing an internet banking security checklist. The security checklist is divided in six main categories as follows: (1) general online security and privacy information to the internet banking customers; (2) information security assistance, monitoring and support; (3) software and system requirement and settings information; (4) bank site authentication technology; (5) user site authentication technology; and (6) internet banking application security features.

Subsorn et al. [27] has compared 16 Australian's internet banking that provides a good setting on the comparative analysis. They have also mentioned that two-factor authentication system for log-in should be enforce to improve, especially security policy should be improved and employed by the banks and legal institute or government to enhance the internet banking transactions for their customers. After that they [8] compared 16 Australian's bank with 12 Thai Commercial banks by using the same checklist, but some criteria are adding to be compared. General information, via email on IT support, Browser automatic or manual test feature available, Email and CAPTCHA on authentication, the maximum daily limit transfer maybe changed by the customer, notification and alerts, cookie not in use, cookie used for other purpose and support other languages have added to the checklist for comparing Australia and Thai bank.



Subsorn et al. [9] has compared 16 Australian's bank with 9 foreign subsidiary banks in Australia with the same six main security categories. The comparison was discussed on the main six categories and assigned a maximum score of 10 points for sub categories. The results showed that the category 4 (employed encryption and digital certificate technologies) got almost a full score for foreign-owned banks. It means that most of Australia foreign-owned bank's server provides enough authentications on their web site.

Finally, Subsorn et al. [28] has compared 13 selected mainland Chinese banks with 19 selected licensed Hong Kong banks, and gave a maximum feasible score of 10 value points based on 6 categories. The results found that the lack of information security was covered on categories 1, 3, 5, 6 and 7 in sub categories 1.1: Account aggregation or privacy and confidentiality, 1.2: Losses compensation guarantee, 1.3: Online/internet banking security information, 2.2: Internet banking transaction monitoring by the banks, 3.1: Compatibility "best" with the popular internet browsers, 3.2: Internet banking user device system and browser setting requirement, 5.4: Password restriction/requirement, 6.1: Automatic timeout features for inactivity internet browser, 6.4: password policy management, 6.5: session management, and 7.1: Employed multi-languages. All of these categories can increase the internet banking security awareness and confidentiality for their users.

However, all these studies have mainly focused on the general security issues of the internet banking services. They have not taken a concern on safety issues. They have not applied to deploy the real internet banking services, and learn from the real case. Also, they have not included the internet banking crime cases and safety standards to support their checklist criteria.

Putla et al.[29] have also studied on both safety and security issues of six internet banking services in Thailand. The results have found that protection management of the internet banking in Thailand is capable enough to terminate all kind spoofing to be account holder in Thailand.



2.4.2 Study on User Perspective and Privacy of the Internet Banking

Systems

Karim et al. [30] investigated on the internet banking's users in London through educational institute and internet (email and social network website). Totally 1,500 questionnaires have been distributed of 1,000 questionnaires through educational institutes in London and 500 questionnaires through the internet. They studied on several points in fields of safety and security, such as policy and technology (users, employees and training), services (bill payment, money transfer, and balance inquiry), user perspective (ease of use, quicker, and convenience), security (risks, spams, phishing, and virus software) on users' side. They investigated on the internet banking because the development on the security system is not parallel with the increasing and improving type of threats in several banks over the world. As the result, 712 questionnaires have responded (427 responses from internet and 285 responses from educational institutes) but in these 712 responses, 69 responses are not complete. They found that 62.05% using the online banking in London and the highest one on banking service is account checking equal to 41.10%. In contrast, users did not use internet banking because of they worried about security risks (43.44%). Moreover, the investigated results had shown that "customer's online banking behavior is largely dependent on the security issues. So, the organization is being suggested to take innovative technical measures to protect the internet frauds."

Loke et al. [31] investigated on the customer satisfaction of internet banking in Perak State, Malaysia. They proposed three hypotheses (Marketing Strategy, Staff Support and Knowledge, and Web security and Trust) and then distributed 500 questionnaires. 172 questionnaire were usable. They have found that "Staff Support" and "Knowledge" are significant for the internet banking service in Malaysia.

Rangsan et al. [32] studied on customer satisfaction among top three banks in Thailand by using questionnaires. That questionnaires were distributed to 450 respondents, based on the internet banking service of seven hypotheses (namely, safety reliability, transactions efficiency, customer support, service security, ease of use, performance, and service content). They conducted and measured the reliability of collected data with Cronbach's alpha coefficient. Finally, they found that top three



banks in Thailand had their strong and weakness differently. This case study is different from other works who study on customer perspective.

Al-Gharbi et al. [33] studied on internet banking in Oman by selected six banks as case studies. They observed on the eight factors, namely security and privacy issues, lack of computer adoption among people, lack of awareness and legislation (legal issues), lack of awareness and education about e-commerce, lack of government support, language and communication barrier, lack of network infrastructure in the country, and people still prefer the traditional way of doing business. So, all of these previous works above studied on customer perspective of internet banking in different country and different aspects. Especially, they investigated on the internet banking service quality and proposed a questionnaire to observe on customer perspective.

2.4.3 Authentication Factors for Internet Banking Systems

Beside username and password for log-in into the internet banking web page, we should have many authentication to carry on for access banking transactions. Furthermore, Han-Na et al. [34] have studied on authentication factor for the internet banking such as digital certificate, security card, security token, one time password and two-channel authentication. As the result, they have compared that authentication with the method of storage, insert, attack, security, authentication and exposure.

Gouling et al. [35] have investigated on security mechanisms of personal internet banking in China Bank. They defined personal internet banking security mechanism into three categories, namely 1) transmission and identity authentication, 2) payment security mechanisms, and 3) protection mechanisms. After analysis, they found that security mechanisms of China Merchants Bank were more complex but strict and strong. However, it was not simple enough for ordinary user, and seemed to have conflicted factors.



Table 2.1 Authentications and Attacks

Source: [36]

	Guessing	Exhaust search	Eaves- dropping	Malware	Phishing	Malware + Phishing
Password	✓	✓	✓	✓	✓	✓
Password + SSL	✓	✓		✓	✓	✓
SMS Code				✓		
PIN		✓	✓	✓	✓	✓
Grid Card					✓	✓
PKI				✓		
Token						

Hanacek et al. [36] have studied on the internet banking attacks with authentication, as shown in Table 2.1 . They also said that “between human non-digital communication and computer or digital communication used in different mechanism for identification”.

Moreover, they also mentioned on trusted devices that implement the security concepts. It is called temper-resistant hardware, and separated into two ways (data and secret cryptographic key). Additionally, they also said that “The secure hardware cannot be cloned or emulated”. So, from all of these previous works mainly focused on many authentication factors for the internet banking’s use and some attacks that mostly occur on the internet banking. Especially, they suggested a lot of authentication mechanisms for bank to use with the internet banking system on each country.

2.4.4 Attacking and Protection Over HTTPS

Sriwiboon et al. [4] and Tooltham et al. [37] has investigated on HTTPS certificate and SSL attacking techniques such as SSL sniff, strip and Man-in-the-middle Attack. Moreover they had tested on the HTTPS website like e-learning, internet banking and so on. After that, they designed and implemented software that was called ISAN HTTPS Enforcer. It was created by Java-script and Python programming language and support with most of the browser and operating system. ISAN-Enforcer is a kind of user friendly software that can detect SSL attack at the victim side. The other software is called Click2Enforce. It was created by HTML 5, Java-script, and CSS that’s like browser extension on the Google chrome.



Table 2.2 Web for testing on SSL

เว็บไซต์	URL
บ.กรุงเทพ	ibanking.bangkokbank.com
บ.กรุงไทย	www.ktbonline.ktb.co.th
บ.กรุงศรีอยุธยา	www.krungsrionline.com
บ.กสิกรไทย	online.kasikornbankgroup.com
บ.เกียรตินาคิน	ebanking.kiatnakin.co.th
บ.ซีทีแบงก์	www.citibank.co.th
บ.ซีไอเอ็มบี ไทย	www.cimbclicks.in.th/ibkthai
บ.ทหารไทย	www.tmbdirect.com
บ.ทีสโก้	www.tisco.co.th
บ.ไทยพาณิชย์	www.scbeasy.com
บ.ธนชาต	retailib.thanachartbank.co.th
Citi Group	online.citibank.com
Standard Chartered	online-banking.standard chartered.co.th

Moreover, they also tested on the HTTPS web site especially the internet banking web site that are shown in Table 2.2 below. Especially, they used Wireshark [38] to catch packet of sniffing username and password from HTTPS web site. Finally, SSL stripping attack is still the problem for HTTPS or SSL web site without any notifications.

As a result, most of the website above can be protected after add this extension into Google chrome web browser. It is a kind of protection software that can be applied to enhance security.

2.4.5 An Analysis of HTTPS Ecosystem and Scan on SSL/TLS Certificates

In 2013, Zakir et al. [39] has investigated on HTTPS Certificate by performing 110 times successful scans of the IPv4 address space and 1,832 CA certificate over 14-months. The way to scans and analyze this paper consists of three stages: (1) discovering hosts with port 443 (HTTPS) by using ZMap, (2) completing a TLS handshake, and (3) performing certificate parsing and validation. On March 22, 2013, Zakir et al. have scanned on certificate authorities (CA) and found that 92.4% of trusted certificates were controlled by 10 commercial CA like GoDaddy, GeoTrust, Comodo and VeriSign are the Top 4 CAs.



Organization	Signed Leaf Certificates	
GoDaddy.com, Inc.	913,416	(28.6%)
GeoTrust Inc.	586,376	(18.4%)
Comodo CA Limited	374,769	(11.8%)
VeriSign, Inc.	317,934	(10.0%)
Thawte, Inc.	228,779	(7.2%)
DigiCert Inc	145,232	(4.6%)
GlobalSign	117,685	(3.7%)
Starfield Technologies	94,794	(3.0%)
StartCom Ltd.	88,729	(2.8%)
Entrust, Inc.	76929	(2.4%)

Figure 2.8 Top Certificate Authorities

Source: [39]

Type	Trusted Certificates	
SHA-1 with RSA Encryption	5,972,001	(98.7%)
MD5 with RSA Encryption	32,905	(0.54%)
SHA-256 with RSA Encryption	15,297	(0.25%)
SHA-512 with RSA Encryption	7	(0.00%)
MD2 with RSA Encryption	21	(0.00%)
Other	29,705	(0.49%)

Figure 2.9 Top Signature Algorithms

Source: [39]

They had found that 98.7% of the browsers certificated are signed with SHA-1 and RSA encryption. Since the weakness of MD5 was issued on April 17 2013, “MD5 considered harmful today” by an Italian defense contractor. Yet, on September 2014, Google has announced that SHA-1 will expire as early as after December 31, 2015. It will warn on chrome version 39, 40 and 41 upcoming to releases.

On the version 39, it shows the yellow triangle over the lock with normal HTTPS and the blank page with no lock on version 40, but differently for version 41 that release on 26 January 2015, it will show the red cross over lock and strikethrough HTTPS.

So, we can conclude that all of these studies can use as a part of our observation criteria. It can be used to observe in-depth on the authentication mechanism that banks deployed like digital certificate, HTTPS, and so on.



Chrome Version	Earliest Release Date	SHA-1 Expires Jan.- May 2016	SHA-1 Expires June - Dec. 2016	SHA-1 Expires After 2016
39	3 Nov. 2014	No Change	No Change	Yellow Triangle Over Lock
40	15 Dec. 2014	No Change	Yellow Triangle Over Lock	Blank Page, No Lock
41	26 Jan. 2015	Yellow Triangle Over Lock (sub resources will also trigger icon)	Yellow Triangle Over Lock (sub resources will also trigger icon)	Red X Over Lock (sub resources trigger yellow icon)

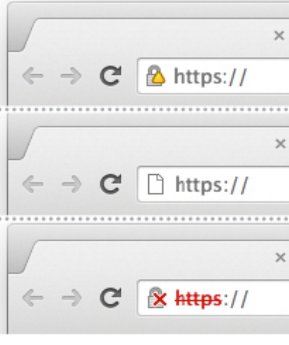


Figure 2.10 Diagram of SHA-1 Warning on Google Chrome

Source: [40]

On 29 November 2014, a group of students [41] from Khon Kaen University, who got an internship at INOX company, had scanned on digital certificates of commercial bank in Thailand, such as Bangkok Bank, Siam Commercial Bank, Thai Military Bank and so on. They then suggested the banks that opens SSL v3.0 (affected of POODLE attack) to closed it, and recommend them to apply “the forward secrecy” for the internet banking system.

2.4.6 Previous Work Analyze

From many previous works, we can say that most of the work has investigated on the internet banking system in different aspects. Some of them have not yet included safety and security standards to support their criteria. Most of them have not yet deployed the real services, and make a real observation on the cases. Some of them have not yet included the lessons learnt from the internet banking crime cases as the criteria.

Moreover, none of previous related studies have observes and compares the safety issues of the internet banking systems between Cambodia and Thailand. As shown in Table 2.3, we have separated and combined all of related works into five groups. Furthermore, the more depth details of comparison on those related works have shown in Appendix B.



Table 2.3 Comparison on Previous Works

Group of Previous Work	Safety	Security
1. A Comparative Analysis of the Security on Internet Banking (Subsorn et al., and Putla et al.)	✓	
2. Study on User Perspective and Privacy of Internet Banking System (Karim et al., Loke et al., Rangsan et al., Al-Gharbi et al.)	✓	
3. Authentication Factors for Internet Banking System (Han-Na et al., Gouling et al., Hanacek et al.)		✓
4. Attacking and Protection Over HTTPS (Puangpronpitag S., Sriwiboon N. and Tooltham A.)		✓
5. An Analysis of HTTPS and Weakness of SSL Certificates (Zakir et al., and a group of student in Khon Kaen University)		✓

2.5 Banks in Cambodia and Thailand

2.5.1 The Case Study

Cambodian Public Bank Plc. (Campu Bank) [10] has been operating in Cambodia since 1992. The first Cambodian Public Bank opened on 25 May 1992, and presently has 27 branches: 13 branches in Phnom Penh and other 14 branches, 1 each in provinces like Battambang, Bavet, Kampong Cham, Kampot, Koh Kong, Poi Pet, Preah Sihanouk, Siem Reap, Suong, Takhmao and so on. With the strong support and trust from the public, coupled with dedication of staff to Campu bank, it has grown to become one of the leading and largest commercial banks in Cambodia. On 31 December 2013, Campu bank's paid-up capital of USD 90 million is one of the highest among the commercial banks in Cambodia with total shareholder's funds and asset amounted to USD 271.5 million. Campu bank is a wholly-owned subsidiary of Public Bank Group in Malaysia.

Dr. Teh Hong Piow has been the President/ Managing Director of Combodian Public Bank on 14 May 1992 and designated as Non-Executive Chairman of Cambodian Public Bank since 28 December 2010. As of today, the executive director of Cambodian Public Bank is Mr. Phan Ying Tong. He was appointed the country's head of Cambodian Public Bank in 2007 and the executive director of Cambodian Public bank in 2010.



While operating in Cambodia, Campu bank also received many awards such as:

1.-“The Bank of the Year in Cambodia” by The Banker, London for five consecutive years from 2001 to 2005, 2008, 2009 and again in 2012 for the eighth time by the banker, London.

2.-“Domestic Retail Bank of the Year-Cambodia” for three consecutive years from 2012-2014 by Asia Banking and Finance

3.-“USD Straight-Through-Processing Excellence Award” for three consecutive years from 2011 to 2013 by Deutsche Bank, New York

2.5.2 Cambodia Banks

Aceda Bank Plc. [42] was established on January 1993, from the national Non-Government Organization, it has become a big commercial bank with coverage in all provinces and towns throughout Cambodia. It is also operating in Laos and Myanmar and employs 10,677 employees in 252 branches and makes available more than 252 ATMs throughout the Kingdom of Cambodia.

Canadia Bank Plc. [42] was established on 11 November 1991 as “Canadia Gold & Trust Corporation Ltd” and its joint-venture between National Bank of Cambodia and Canadians shareholders. It was announced as commercial bank on 16 December 2003; then it has changed its name to “Candia Bank Plc” (Public Limited Company), abbreviated as “CNB”. CNB has 50 branches, 88 ATMs and has 1,638 employees in the kingdom of Cambodia.

2.5.3 Thailand Banks

Bangkok Bank (BBL) [43] was established on 1 December 1944. BBL is the largest commercial bank in Thailand. Presently, BBL has more than 1,000 branches and more than 8,600 ATMs that covers Kingdom of Thailand. BBL employs 22,934 employees.

Thai Military Bank (TMB) [43] was established on 5 November 1957. At first, it was established to provide financial services to military personnel, their families and growth. It also opened its first public branch in 1963. Thai Military Bank has 483 branches, 2,257 ATMs and employs 8,236 employees throughout its branches in the Kingdom of Thailand.

Siam Commercial Bank (SCB) [43] was founded by King Rama V in 1904. It has established itself as one of the commercial banks in Thailand and also the first

bank in Thailand to provide internet banking services. SCB total asset was 2,534.20 billion baht (2013 annual report).

2.6 The Internet Banking Standard of Information Safety/Security

The International Organization for Standardization (ISO), established in 1947, is a non-governmental international body that collaborates with the International Electro-technical Commission (IEC) and the International Telecommunication Union (ITU) on information and communication technology (ICT) standards. Information Security [44] is the processes of protected digital information assets that include policies, procedures, authentication, web, operating system, cryptography and so on. The replacement ISO/IEC 17799 with ISO/IEC 27002:2005 said that “preservation of confidentiality, integrity and availability of information”. Generally security standards are device into two groups and common meaning about other standards are following:

2.6.1 Information Security Standards

- -ISO/IEC Security Standards Family
- -NIST 800 series: NIST (National Institute of Standards and Technology) is a set of documents that described United States Federal government computer security policies, procedures and guidelines.
- -SOX: Sarbanes-Oxley Act is known as the public company accounting reform and investor protection act.

2.6.2 IS Governance Standards

- -COBIT: Control Objective for Information and Related Technology is the framework that used to ensures
- -COSO: Committee of Sponsoring Organizations of the Treadway Commission framework is a framework that initiates an integrated process of internal controls.
- -ITIL: Information Technology Infrastructure Library is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business

There are several standards, covered on 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 has relied on the ISO/IEC 27002:2005 standard to measures on risk management of the internet banking systems.

These are all related common practices of information security control in ISO/IEC 27002:2005 apply for the internet banking such as information security policy document (section 5.1.1 of standard), allocation of information security responsibilities (section 6.1.3 of standard), information security awareness, education, and training (section 8.2.2 of standard), correct processing in applications (section 12.2 of standard), vulnerability management (section 12.6 of standard), business continuity management (section 14 of standard), management of information security incidents and improvement (section 13.2 of standard), and data protection and privacy of personal information (section 15.1.4 of standard). Moreover, this standard structure contains with 11 security control clauses collectively containing a total of 39 main security categories. All of these controls take over the information safety and security system of the bank. It provides valuable guidelines and risk management for the internet banking systems. The National Bank of Cambodia and Bank of Thailand has also relied on the ISO/IEC 27002:2005 standard to measures on risk management of the internet banking systems. So, in this paper, we choose the ISO/IEC 27002:2005 standard as a part of our criteria (Appendix A) to analyze the internet banking systems between Cambodia and Thailand.

2.7 Secure Authentication of the Internet Banking Websites

2.7.1 Secure Socket Layer and Transport Layer Security

SSL/TLS have published by Netscape as the internet protocol standardization with The Internet Engineering Task Force (IETF). It is available in Requests for Comments (RFC) 5246 [2], is the most widely deployed security protocol used today. When a web browser connect to a web server over the inherently insecure internet, SSL/TLS essentially the protocol that provides a secure data between two machines using encryption operating over the internet or an internal network, Mostly, TLS version 1.2 is standard protocol that provides secure communication in all secure web servers such as internet banking web sites, online shopping web site and other



registration web sites. The messages exchanged of the SSL/TLS handshake (Figure 2.11) [13] has shown as follow:

1) Client sends a “Client Hello” message that contain with lists cryptographic information such as the SSL or TLS version, a random byte string of client, Cipher suites supported, SSL or TLS version by the client.

2) Server responds with a “Server Hello” message that contain with cipher suite in the server chosen by the client, a random byte string of server, the session ID and digital certificate for client authentication. And then the server sends a “Client Certificate Request” that includes with certificate supported and the names of acceptable Certificate Authorities (CAs).

3) Client verifies the server’s digital certificate by checking on identification, authentication, confidentiality and integrity of SSL and TLS.

4) Client sends a random byte string for both client and server to calculate the secret key that used for encrypted message data. The random byte string was encrypted with the server’s public key.

5) If the server will sent a “client certificate request”, the client sends a random byte string with private’s key and client’s digital certificate or a warning of no digital certificate alert. With some implement the handshake is fails when the client authentication is mandatory.

6) Server verifies the client’s certificate.

7) Client sends the server a “finished” message. If the client handshake is complete, the message was encrypted by client’s secret key.

8) Server sends the client a “finished” message. If the server handshake is complete, the message was encrypted by server’s secret key.

9) So the server and client can now exchange messages that are encrypted with the shared secret key of symmetric algorithm.



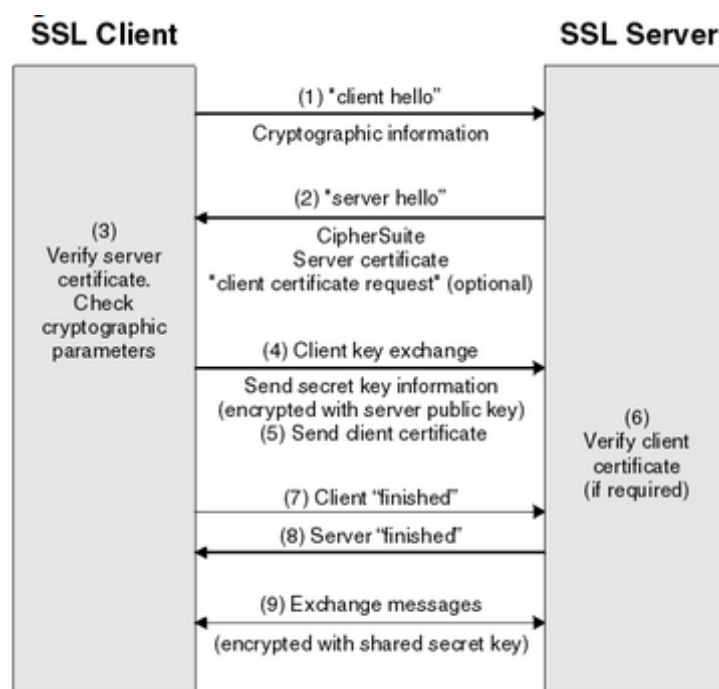


Figure 2.11 SSL Handshake

Source: [13]

Technically, SSL is a transparent protocol that requires little interaction from the end user when establishing a secure session. Moreover, SSL/TLS has combined with HTTP connections (HTTPS = HTTP + SSL/TLS) in order to secure information. It has also implemented on the web browser URL as shown in Figure 2.12



Figure 2.12 HTTPS Connection

In addition, the following Table 2.4 has shown the problem of SSL and its protection technique are:



1) Problems demonstrated: SSL Stripping is a kind of SSL attack that retard at the middle of communication between server and client, it worked to sniff all information over the internet by pushing web site to become insecure connections.

2) Protections expressed: all users should check web site before log-in, regularly upgrade web browser, connects with secure network, and set the bank server to use HTTPS.

Table 2.4 Problems and Protections on Secure Socket Layer

Source: [45]

วิธีการโจมตี	ลักษณะของโจมตีหรือปัญหา	การป้องกันปัญหา สำหรับผู้ใช้งาน	การป้องกันปัญหา สำหรับธนาคารผู้ให้บริการ
การโจมตี SSL			
SSL stripping	- โจมตีแทรกกลางการสื่อสารที่ใช้โพรโทคอล SSL แล้วบังคับให้ปลอดภัยใช้โพรโทคอล SSL	- ตรวจสอบเว็บไซต์ที่ใช้งาน - อัปเดตเว็บเบราว์เซอร์สม่ำเสมอ - ใช้งานเครือข่ายที่มีการรักษาความปลอดภัย	- กำหนดให้เครื่องแม่ข่ายของธนาคารทำงานโดยใช้โพรโทคอล HTTPS ซึ่งจะมีการเรียกใช้ SSL

2.7.2 Digital Certificate

Digital Certificate [46] is the data structure used to transport and validate keys. It protected the both keys (public and private keys) to the identity of the issuer and the owner. The digital certificate cannot be forged easily because of this certificate contained with version, serial number, signature, issuer, validity, extensions and so on. By the way, it has also verified by RFC 5280 [1] “Internet X.509 Public Key Infrastructure Certificate” standard.

Table 2.5 Problems and Protections on Digital Certificate

Source: [45]

วิธีการโจมตี	ลักษณะของโจมตีหรือปัญหา	การป้องกันปัญหา สำหรับผู้ใช้งาน	การป้องกันปัญหา สำหรับธนาคารผู้ให้บริการ
การโจมตีใบรับรองดิจิทัล			
การปลอมแปลงใบรับรอง	- การใช้บริการเกิดความเสียหาย ไม่สามารถตรวจสอบถึงความปลอดภัยในการใช้บริการได้	- ตรวจสอบใบรับรองของเว็บไซต์ที่ใช้งาน - อัปเดตเว็บเบราว์เซอร์	- ธนาคารควรมีการประยุกต์ใช้ hardware security module (HSM) เพื่อเก็บรักษากุญแจส่วนตัวให้ปลอดภัย



From Table 2.5 has shown that hacker can counterfeit the digital certificate by deploying the error certificate for users to access on the web browser. Yet, they have mentioned [45] that users should update their web browser regularly, and check the website certificate while filling any confidential information. They have also pointed out that banks should apply hardware security module (HSM) to protect their private key in securely.

2.7.3 Two-factor Authentication (2FA)

2FA [47] is one of the security methods that provide protection mechanism for online users with higher level of authentication. It requires the user to have two out of three types of authenticates before being able to access an account like:

- 1) Something you know like a personal identification number (PIN), or password
- 2) Something you have like a mobile phone, token device, ATM card, or fob
- 3) Something you are such as a biometric like a fingerprint or voice print

One time password (OTP) is the secure code for one time usage only. There are several types of OTP, such as text messaging (SMS OTP), mobile application, token devices (Token OTP), Email OTP, and so on. Most of the bank has deployed it to authenticate with user. Normally, it has used after username and password on the log-in webpage or on the other transaction activities. Yet, there are some attacks had effected on OTP like mobile phone Trojan, SMS delay and so on as shown in Table 2.6. All users should be careful on download or upgrade unknown programs on mobile phone. For banks, they should verify with the duplicate mobile number of users to received OTP.

Table 2.6 Problems and Protections on One Time Password

Source: [45]

วิธีการโจมตี	ลักษณะของโจมตีหรือปัญหา	การป้องกันปัญหา สำหรับผู้ใช้งาน	การป้องกันปัญหา สำหรับธนาคารผู้ให้บริการ
การโจมตี OTP			
Mobile phone Trojan	- รับส่งข้อมูล OTP โดยอัตโนมัติ รวมถึง ขโมยข้อมูลในโทรศัพท์	- ระมัดระวังในการดาวน์โหลดและ ติดตั้งโปรแกรมในโทรศัพท์พกพา	- มีการสร้างและตรวจสอบรหัส OTP ว่าซ้ำกับรหัสที่เคยใช้งาน มาแล้วหรือไม่
SMS delay	- ข้อความ OTP มาถึงล่าช้าทำให้การทำ ธุรกรรมติดขัด	- หลีกเลี่ยงการทำธุรกรรมใน ช่วงเวลาที่ผู้ใช้งานเครือข่าย หนาแน่น	- ใช้วิธีการสร้างรหัส OTP ที่ เรียกว่า time-based OTP (TOTP)



2.7.4 Username and Password Selection Strategies

A lot of internet users have set their username and password [13] too short and easy to guess like birthdate, phone number, name and so on. Yet, if users have assigned their username or password consisting of eight or more randomly characters with special characters and upper and lower case, even password cracker may be difficult to break the password. On the other hand, if the system generated the username or password for users, it should be hard for users to remember and less accepted by users in sometimes. Moreover, username and password were exploited easily like phishing, brute force attack, and Trojan horse as shown in Table 2.7.

Furthermore, the best approach to select password are: all passwords should set at least eight characters long and includes with uppercase, lowercase, numeric digits, and punctuation marks or special characters. Moreover, users should change password regularly in order to ensure the password is secure. For safety reason, password should be change within 30, 60, or 90 days.

Table 2.7 Attacking and Protection on Username and Password

Source: [45]

วิธีการโจมตี	ลักษณะของโจมตีหรือปัญหา	การป้องกันปัญหา สำหรับผู้ใช้งาน	การป้องกันปัญหา สำหรับธนาคารผู้ให้บริการ
การโจมตีบัญชีผู้ใช้และรหัสผ่าน			
ฟิชซิง	- ปลอมแปลงหน้าเว็บไซต์เพื่อการขโมยข้อมูลส่วนตัวของผู้ใช้งาน	- ติดตั้งและใช้งานโปรแกรม antivirus	- มีระบบการจัดเก็บรหัสผ่านที่ปลอดภัย เช่น Salted hash
Brute force attack	- การกำหนดรหัสผ่านของผู้ใช้ที่ง่ายต่อการคาดเดาหรือโจมตีได้ง่าย	- ตรวจสอบเว็บไซต์ว่าถูกต้องก่อนใช้งาน	
Trojan horse	- ขโมยข้อมูลส่วนตัวของผู้ใช้งานแล้วส่งข้อมูลไปยังผู้โจมตี	- เลือกใช้รหัสผ่านที่คาดเดาได้ยากและเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ - ระวังในดาวน์โหลดและติดตั้งโปรแกรมจากแหล่งที่น่าเชื่อถือ	

2.7.5 On Screen Keyboard

On screen keyboard [48] is the keyboard that relies on screen with high security, flexible and random keystroke that appear on screen as shown in Figure 2.13. It is very popular for the internet banking website besides using the real keyboard that are endangered by keylogger software that can gather all information such as username



and password, credit card number, and so on from capturing the keyboard pressing codes.

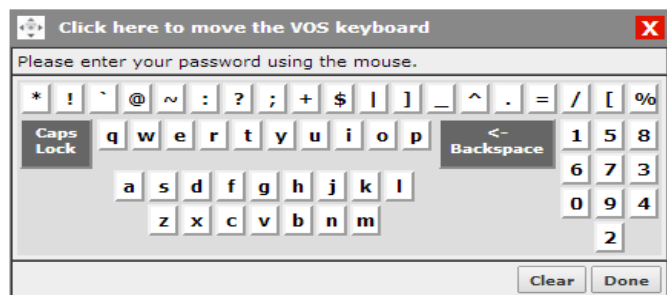


Figure 2.13 On Screen Keyboard

Source: [48]

2.8 Penetration Testing Tools, Attacking Techniques and Interview Form

2.8.1 Penetration Testing Tools

Kali Linux [49] is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It was maintained and funded by Offensive Security Ltd and developed by Mati Aharoni and Devon Kearns through the rewrite of BackTrack. There are several categories tools in Kali Linux like forensics system services, password attack, information gathering, vulnerability analysis, sniffing/spoofing and so on.

Cain and Abel [50] is a kind of tool for password recovery by sniffing the network, cracking encrypted password using dictionary, brute force attacks and analyzing routing protocols. Development of this tool is for student education, teacher, professional security staff and forensic staff. Latest release of this tool is version 4.9.56 on 07 April 2014 that support with window 8 and it was developed by Massimiliano Montoro.



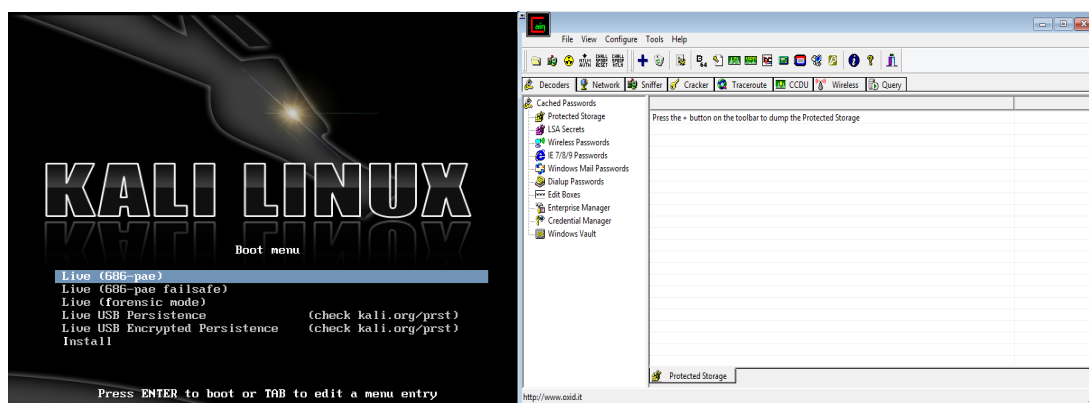


Figure 2.14 Kali Linux and Cain and Abel

Source [49, 50]

Qualys's SSL Lab [51] is the leading provider of compliance management solution and IT security risk that delivered as a service. Today, it has been used by more than 3,500 organizations in 85 countries. Moreover, we have also investigated on three categories of certificate like protocol support, key exchange support and cipher support. They also rate the server by giving scores from 0 to 100 into overall score and after that they also grade from A+, A-, B, C, D, E, to F. Qualys's SSL lab have calculated the score as a combination of protocol support equal to 30%, key exchange 30% and cipher strength is 40%. Protocol supports are SSL 2.0, SSL 3.0 and TLS 1.0, TLS 1.1 and TLS 1.2. Furthermore, most servers are relying on public cryptography for the key exchange. Private Key and Weak key have used to share and keep data in secure along the connections. Hence, we included this SSL lab to scan the bank's server in order to see the better of the bank authentication websites relies on.

2.8.2 Most Common Attacking Techniques on Internet Banking

SSL sniff, strip and split [3-5] are kinds of man-in-the-middle attack that used to demonstrate rogue CA-certificate. SSL sniff, strip and split used to stole password from victims computer which is connected in LAN. SSL strip and split are basically hijacks HTTP traffic and fake certificate of servers. Nowadays it's little difficult to steal password of some website. We use the command in kali linux as follows:

1)--**Command: echo '1' > /proc/sys/net/ipv4/ip_forward**

- Used to enable IP forwarding.



2)--Command: **iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080**

- Used to redirect requests from port 80 to port 8080 to ensure outgoing connections from SSL strip get routed to the proper port.

3)--Command: **netstat -nr**

- Used to find out gateway IP

4)--Command: **arp spoof -i interface -t target IP -r gateway IP**

- Used to redirect all network HTTP traffic through computer using ARP spoofing.

5)--Command: **sslstrip -l 8080**

- Used to listening port for specified port.

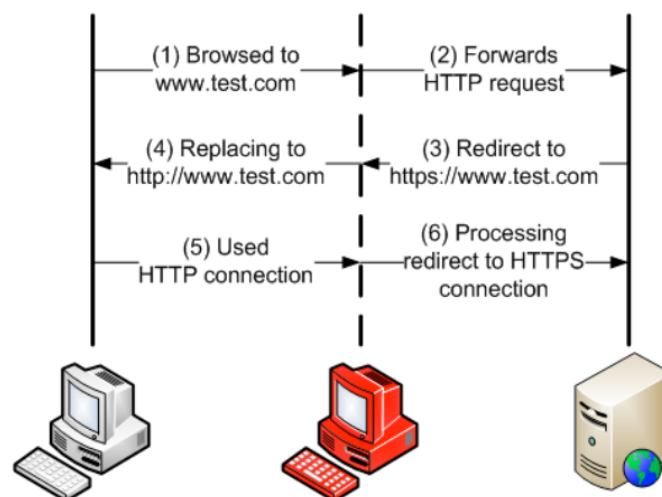


Figure 2.15 SSL Strip on Kali Linux

Source [4]

Heartbleed Bug [6] is a serious vulnerability in OpenSSL cryptographic software library. Under normal conditions, it used to compromise the secret key that identifies the service providers and to encrypt the traffic, usernames and password of the users and then allow attackers to eavesdrop on communications, steal data directly from the services and users. It was released on 7 April, 2014 and implementation of the TLS/DTLS heartbeat extension (RFC 6520) [52]. It works to exploited leads to the leak of memory contents between client and server. This means that it opened a hole for



hackers to get the information stored on the servers could be stolen. In this thesis, Heartbleed Bug is one of our security concerns.

POODLE Attack (Padding Oracle on Downgrade Legacy Encryption) [7] used to exploit against SSL 3.0 since the first well-deployed version of SSL 3.0. On September 2014, Google announced POODLE as an SSL 3.0 protocol attack. It works by getting into the browser and server to settle on SSL 3.0 and downgraded the communication of SSL and TLS protocol. When it is downgraded to SSL 3.0, the attacker can use POODLE to attack by allow items such as “secure” HTTP cookies or HTTP authorization header contents to be stolen from downgraded communications. The weakness of SSL 3.0 can be exploited by a man in the middle attack to decrypt secure HTTP cookies, using the BEAST attack technique. In this thesis, POODLE is one of our security concerns.

2.8.3 Interview Form and Item Objective Congruence

Interview Form is a kind of survey questions for the purpose of gathering information from respondents or research equipment that designed for analysis of the data that collected. All questions in the interview form contained with knowledge, clear comprehensive wording and easily understandable for all educational levels.

Item Objective Congruence (IOC) index is an instrument or technique that used to evaluate the quality of questionnaire. IOC is to find out which question should be asked to the audience. It has measured on knowledge, difficulty and discrimination of questions on writing and speaking. In this thesis, the interview form is evaluated by IOC by three experts giving their opinions if research question should be asked to audience or not. The sample of IOC evaluation is shown in Table 2.8

Table 2.8 Sample Table of IOC

Objective	Question	Score		
		1	0	-1
1.	1.			
	2.			

Meaning of the score: Accept = 1, Reject = -1 and Maybe = 0.



CHAPTER 3

RESEARCH METHODOLOGY

3.1 Overview

Figure 3.1 has shown the overall view and steps of this research. Firstly, the evaluation of the internet banking systems is done using observation (start from April to November 2015), deployment and experiments. As mentioned in chapter 2, safety and security are different but equally important. So, the evaluation is spited into two parts, for both safety and security.

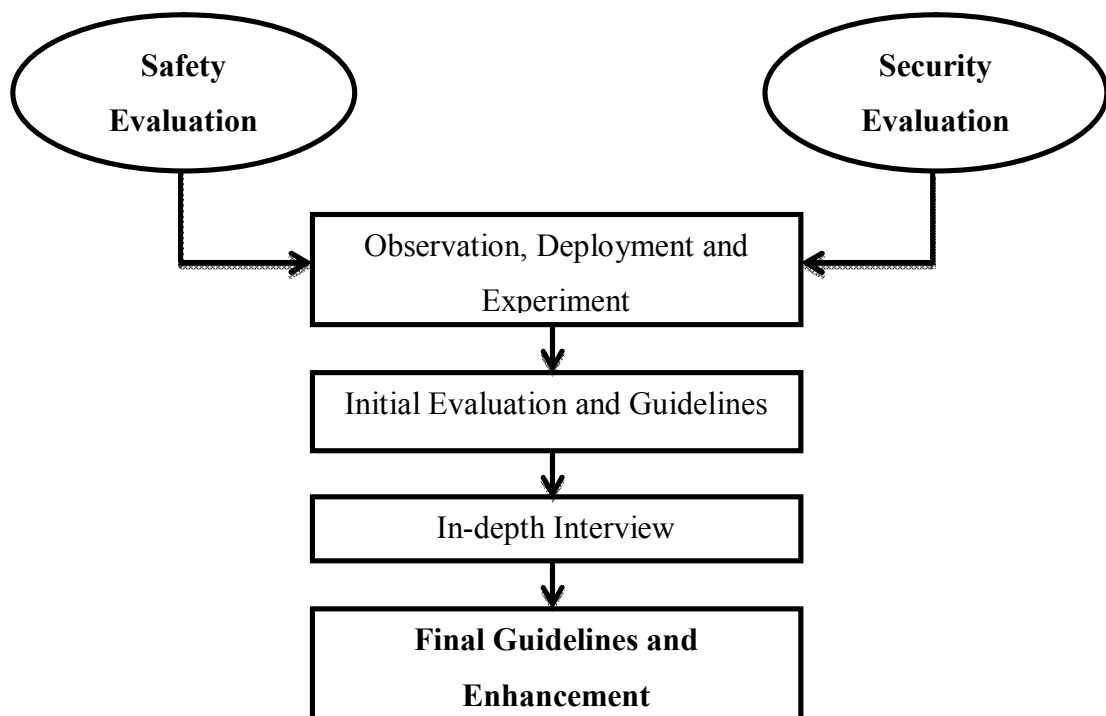


Figure 3.1 Safety and Security Evaluation and Enhancement

To gain some in-depth ideas, this research uses the Cambodia Public Bank (Campu Bank) as a specific case study. However, to gain more comparative ideas (that may give more details), the evaluation has also been done on the other top local two



banks in Cambodia and three banks in Thailand. The Table 3.1 below has shown the details criteria to select these five banks.

The research focuses on only personal banking accounts. The corporate banking accounts are out of the scope of this research. The observation, deployment and experiments are done on the internet banking systems (via web browsers only). The mobile banking (by using mobile applications on smartphones) is out of the scope of this research.

Table 3.1 Selected Banks

Cambodia Banks	Thailand Banks	Reason
Canadia Bank	Bangkok Bank	Largest Bank in country
Acleda Bank	Thai Military Bank	Government Shareholder
Cambodian Public Bank (Case Study)	Siam Commercial Bank	First deployed internet banking

The details of evaluation procedures on safety and security can be found in section 3.2: Safety Evaluation and section 3.3: Security Evaluation respectively. After that, the initial evaluation, process deployment, experiment results and protection mechanism suggestion on both safety and security will be proposed to interview with bankers. In order to gain more ideas and confirmation of initial guidelines and enhancement, two expert staffs from Campu bank will be the audience in this research's in-depth interview. One expert is from the management side and the other expert is from the technical side. After the interview, we will adjust the initial evaluation and guidelines on safety and security following their feedbacks to gain the final evaluation guidelines and enhancement for Campu bank. The details of the in-depth interview procedure can be found in section 3.4.



3.2 Safety Evaluation

Figure 3.2 has shown steps on safety evaluation. The criteria for safety evaluation come from previous works, safety/security standards and internet banking crime cases. For the previous works, most of them investigated on the user's perspective, and created some random criteria to observe on safety side of the internet banking system (such as username and password restriction, safety settings and security features on the internet banking system, software and system requirements, customer support and so on).

For the safety/security standards, we had considered many standards as shown in section 2.6 such as ISO/IEC security standard family, NIST 800 series, COBIT, ITIL, and so on. So in this thesis, we decided to choose the widely recognized as the international standard that provides information safety and security controls. ISO/IEC 27002:2005-Code of practice for information security management will be included in this research. It refers to supporting, controlling, improving, and maintaining the processes of the system such as policies, procedures, processes and so on. To make sure our safety evaluation criteria are validated by one specific procedure. In this section, we also include this standard to verify and support on safety evaluation criteria such as monitoring on the process requirements, logging (authorized access, alert, and fault), service registration, password restriction control, responsibilities of the user to protect unauthorized access, access limitation, and user identification that should be used.

For the internet banking crime cases, many problems always occurred on the internet banking as shown in section 2.3. We included crime cases in this research because it can show the real problems with users and real experience of using internet banking service in both safety and security. It can review some weakness in the management side of internet banking, and at the same time it can review some weakness of the security side too. Additionally, we can see that none of the previous works consider on this crime cases before such as Subsorn et al. [8, 9, 27, 28], Karim et al. [30], Rangsan et al. [32] and so on.

So, in this research criteria relied on previous work analysis, safety and security standards, and internet banking crime cases that differently from other literature



reviews, and also this crime cases will generate the criteria on both safety and security side on the steps of internet banking deployment and weakness that can bypass the system.

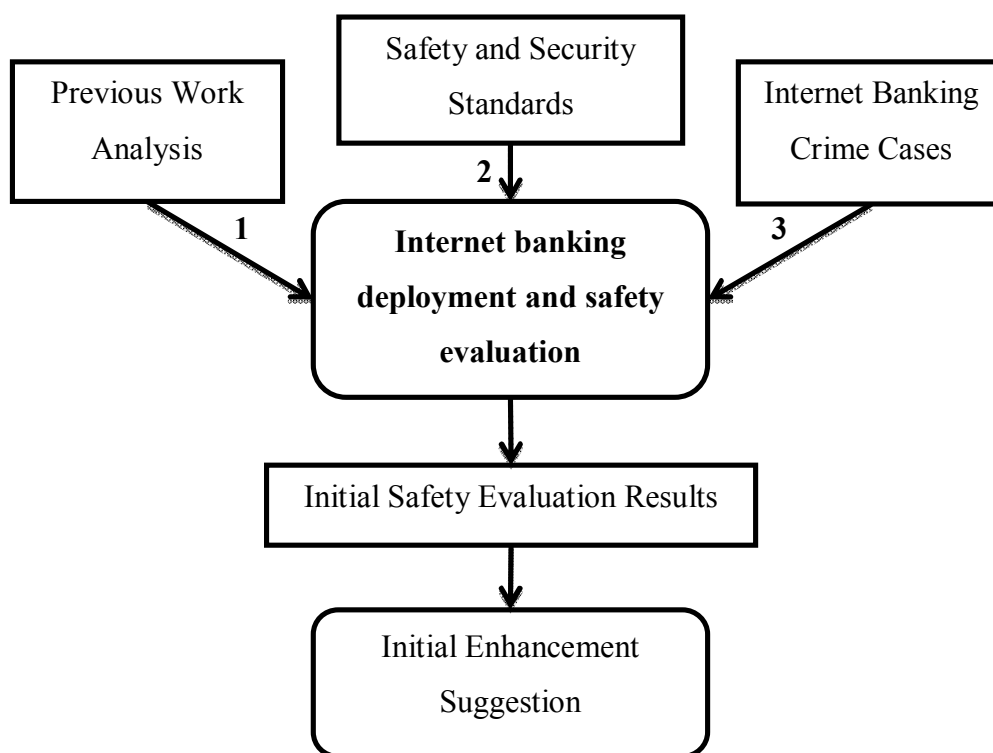


Figure 3.2 Safety Evaluation and Enhancement

After getting the safety evaluation criteria, we apply to deploy the internet banking of Campu bank and other five banks (mentioned in Table 3.1: Selected Banks). The observation on each process starting from opening bank account (observe on requirements of open bank account, internet banking registration, username and password recovery, internet banking log-in web page, safety settings (notification, transactions limitation, and so on) provided by bank, authentication factor for transactions and implementation of one time password), till closing the bank account will be done and recorded. In order to get initial safety evaluation results and enhancement suggestion, the evaluation criteria and observation on the deployment



details gaining from these steps will be the contribution of safety evaluation on the internet banking system.

3.3 Security Evaluation

In section 3.2, we have mentioned about safety evaluation. In this research, we also do the security evaluation to see the technical weakness of the systems. So, we explain the security evaluation details in this section. Similar to safety evaluation criteria, the criteria for the security evaluation mostly come from the analysis of previous works, safety/security standards and the real internet banking crime cases.

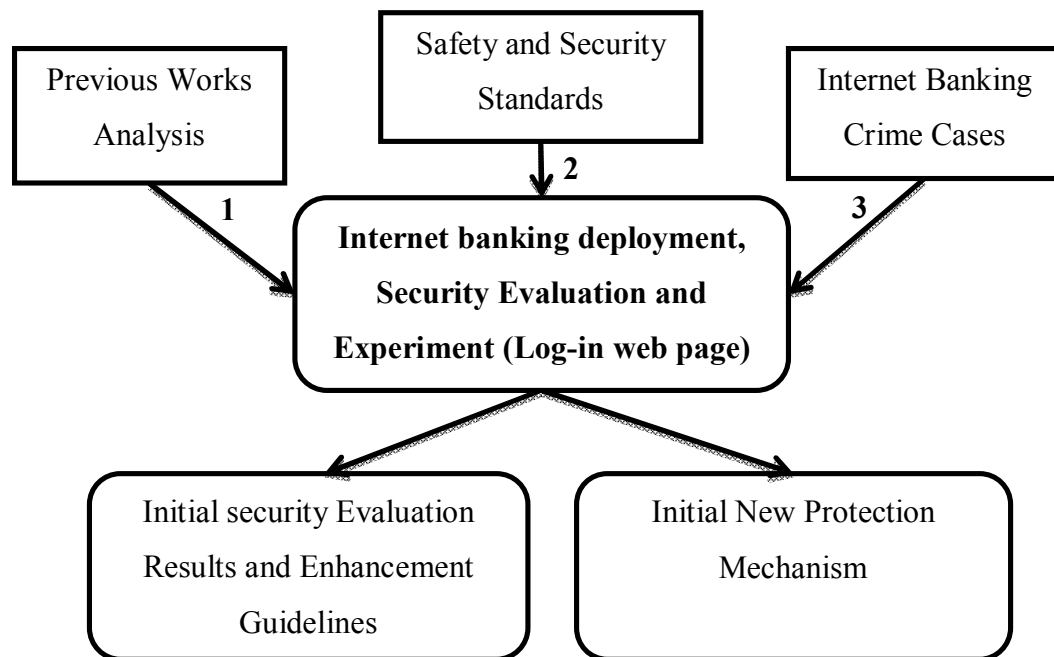


Figure 3.3 Security Evaluation and Enhancement

According to the previous works (mentioned in chapter 2), most of them investigated on security mechanisms, authentication factors, bank certificate, one time password, CAPTCHA, scramble keyboard, and so on.



According to the safety/security standards, as mentioned in section 3.2, we have selected the ISO/IEC 27002:2005 standard to control, maintain and support as parts of the security evaluation criteria in this research. The differences from the previous sections 3.2 are that we include the ISO/IEC 27002:2005 parts that mostly related to the security (technical sides) of the internet banking system, such as electronic commerce services, protection from fraudulent activity, unauthorized disclosure, electronic signatures, and confidentiality of system transactions.

According to the internet banking crime cases during the last five years, we have observed that SSL hacking using several techniques to break the log-in web page of the internet banking is the main target. In particular, the IT crime cases at DSI (mentioned in section 2.3) have shown the SSL Strip as the main technique. So, apart from evaluation on the general security of internet banking, this research will focus on SSL attacking techniques as well. So, this research also experiments on a test-bed to simulate the SSL attacks on the log-in web page of the internet banking systems. After deploying, observing and experimenting on the test-bed, the initial security evaluation results can be produced and consulted with the Campu staffs in the next step (mentioned in section 3.4). Furthermore, in this step, the security enhancement guideline is produced from what the mistakes learnt. Also, from the experimental results from the test-bed, this research will design and develop a new mechanism to improve the log-in web page to fight against the SSL attacking techniques. Finally, the evaluation criteria and observation of the deployment details, the experimental results from the test-bed, the proposed enhancement guideline, and the new mechanism against SSL attacks gaining from this step will be the contribution of security evaluation of the internet banking system.

3.4 In-depth Interview

In this research, we interview two staffs, who work relatively to the internet banking safety and security from Campu bank as shown in Figure 3.4. The first one is Mr. Hou Bunnara, the manager of Phnom Penh Economic Zone branch in Campu bank. He has expertise in the management side of internet banking for more than 10 years.



The other one is Mr. Seng Som Sopheak, the assistant security of the Campu bank head's office. He is responsible for the security side of the internet banking system by cooperating with the public bank group in Malaysia. Their opinions on our safety/security evaluation results and enhancement guidelines would help refine our research outcomes.

According to Figure 3.4, the process of in-depth interview of this thesis starts from drafting the interview form to get the opinions from Campu Bank staffs on our research results. We then validate the draft of the interview form by IOC process. Three security specialists (Suchart Khummanee, Attapol Suwannasa, and Nattavut Sriwiboon) will give opinions on this research's interview form according to the IOC as mentioned in section 2.8.3. After getting a validated interview form (Appendix C), we then run the in-depth interview. After the in-depth interview, the feedback from the Campu bank would help us refine our research results according to the opinions from the side of internet banking real implementers.



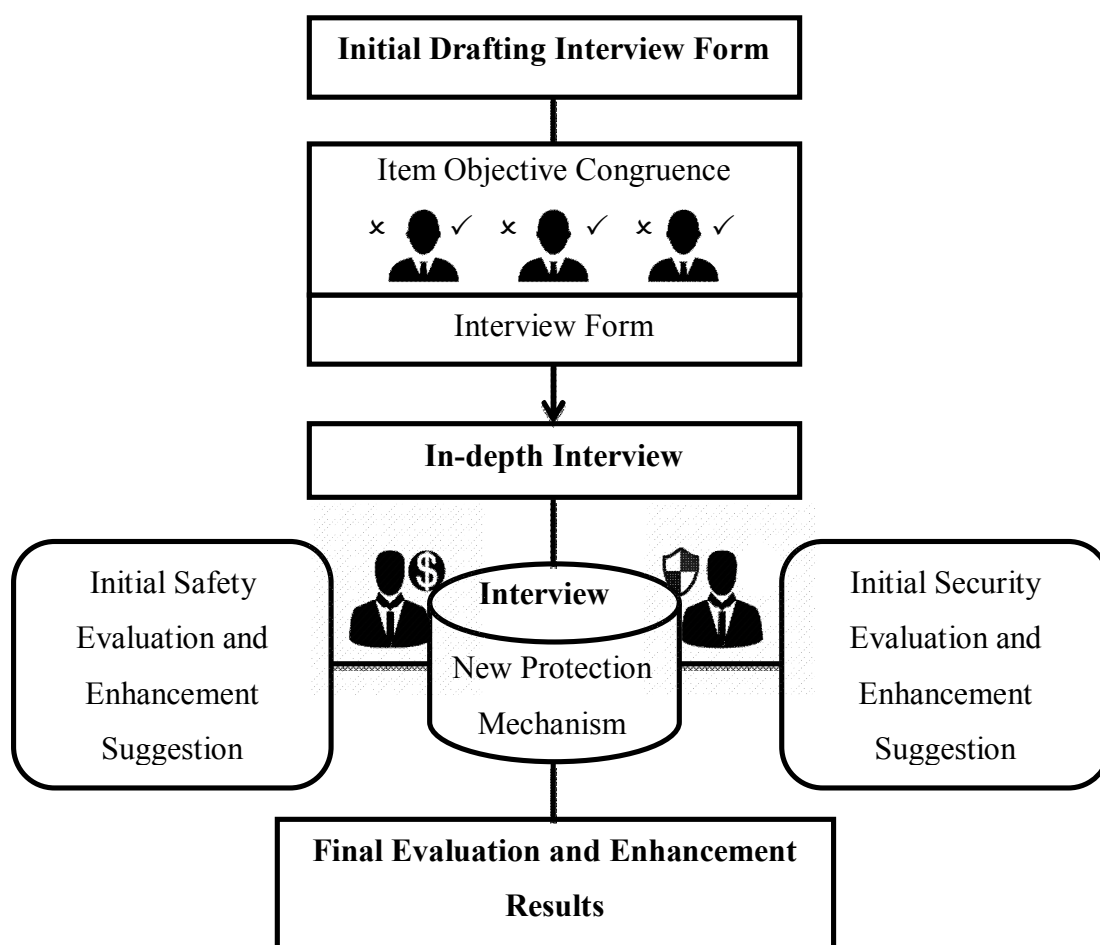


Figure 3.4 In-depth Interview

3.5 Ethical Guidelines and Suggestion

For the ethical issues, this research will carefully review on the results of evaluation on both safety and security that can probably affect the bank. If anything can be harmful, it may have to be omitted from the final report. The bank confidential information must be handled very carefully, for example:

- 1) - The name of the banks (as shown in Table 3.2) will not be revealed together with the weakness after evaluation. Yet, we will make them anonymous.
- 2) - Some weakness on our case study will be consulting with the campus bank before revealing in the final report.



3) - In our experiments on attacking the log-in web page, we will test it on our bank account, opening for this purpose, without intruding any other customers of the banks. The attacks will also be done on only our make-up victim machine in our test-bed without attacking any public facilities.

Table 3.2 Review on Safety and Security Evaluation

Safety and Security Observation Criteria	Bank A	Bank B	Bank C	Bank D	Bank E
.....	✓	✗	✗	✓	✓
.....	✗	✓	✗	✓	✗



CHAPTER 4

RESULTS AND DISCUSSION

4.1 Review on Observation Criteria

This research mainly aims to evaluate and compare the internet banking systems of three banks in Cambodia and three banks in Thailand (as mentioned in Chapter 3), particularly focusing on the safety and security 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 scope of this work. We will also propose a suggestion guideline to reinforce on safety and security issues. As mentioned in section 3.2 and 3.3, the observation criteria come from previous work analysis, the safety and security standard, the internet banking crime cases and experiment. So, our observations to evaluate internet banking are listed as follows:

4.1.1 Open Bank Account and Internet Banking Registration

We observe deeply on the step of opening bank account till closing the bank account. We also observe on 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.

From the evidence 1, 2, 3 in chapter 2, it demonstrated that mugger forge a police identity card, driving license and other related documents issued by government to open the new sim-card with same mobile number. Moreover, these illegal documents



had used to open bank account and register the internet banking for the victim as showed in evidence 3 even victim did not have internet banking but mugger can open it for them. Yet, social engineer or mugger is clever enough to gather all victim information to fulfill with bank authentication requirements. Especially, all of observation criteria assured with the ISO/IEC 27002:2005 best practice standard to verifying on authorized user access, preventing unauthorized access to information system and managing user access rights at regular period using a formal process based on section 11.2.1 user registration, 11.2.3 Privilege management, 11.2.4 Review of user access rights of this ISO standard.

In addition, there is an only way of open bank account by going to the bank branch but for the internet banking service is different from open bank account. They can register through bank branches, ATM machines, online and so on. Moreover, some special cases that should be included are opening bank account by other third party, duplicate registration of the internet banking with different branches, automatic adding all account after registered the internet banking (for users who have more than one bank accounts or related services of user's identity card).

4.1.2 Username and Password

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. 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. According to ISO Standard, section 10.10.5 fault logging, 11.2.3 user password management, 11.3.1 password use, 11.3.2 unattended user equipment, 11.5.2 user identification and authentication, 11.5.3 password management system, 11.5.4 use of system utilities are covered on the username and password policy. So, it is important in our criteria to observe on this research because some banks allowed their users to reset or recovery username and



password through multi ways and also some banks have different method for username and password settings.

4.1.3 Call Center Authentication

Call center is a convenient 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 (Table 4.1).

Table 4.1 Call Center Authentication Criteria

Account Number	Phone Number	Video Conference
Birthdate, Day of Birth	ATM Expiration Date	ATM PIN Number
Username, Account Name, Nickname	Identity card Number, Passport Number	Last Transaction, Account Activity
Email Address, Current Address	Account Holder Branch	Memorable question and Answer

In order to provided standard observation and supported idea in this research. The Standard ISO section 10.10.2 Monitoring system use, 11.6.1 Information access restriction, 11.7.1 Mobile computing and communication, 11.7.2 Teleworking had included in this call center authentication to protected on risk of using mobile in public environment and personal banking information to access banking transaction meet with bank requirements and policies.

4.1.4 Two-Factor Authentication

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 in almost all transactions of the internet banking



systems, such as fund transfer, bill payment, top-up, and so on. So, the observing on OTP is one of our criteria as follows:

- 1) Type of OTP (SMS /Email /Mobile /Token) by observing on length of OTP, expiration and cost
- 2) Type of CAPTCHA (Number, Character, Picture, All)
- 3) Transactions deployment (First time registration, Log-in webpage, Transfer within bank account (local bank, different interbank account and international transfer, Bill payment, Top-up, Add account and Other card payments)
- 4) Change Settings (Username, Password, Phone number, Transaction limitation and Update personal details)

According to the internet banking crime cases in chapter 2, we found that SMS OTP has been hacked by social engineering. They used the simple way to hacked victim (without malicious software) of forging the issued government document to open a new sim-card of the victim at mobile center. After that they go to log-in webpage of the bank, then click on “forget password” to reset new password that new password confirmed with the SMS OTP. However, muggers had the victim mobile number on their hand that came from mobile center of new sim-card requested (old sim-card is blocked).

Moreover, the ISO best practice standard in section 10.9.1 electronic commerce, 10.10.1 audit logging, 11.4.1 policy on use of network service, 11.4.2 user authentication for external connections, 11.5.1 secure log-on procedure, and section 11.5.2 user identification and authentication had included in this research to enhance on observation criteria of two-factor authentication that most of the banks used it.

4.1.5 Transaction Limitation

Transaction limitation can help users from transferring money-out in unpredictable amounts by hackers. This limitation and the method to change it are parts of our observation points. Furthermore, banks have set user’s transaction limitation (transfer, payment, top-up per day and per transaction) in order to prevent unauthorized access or unauthorized transfer for their users. It was set carefully by policy and bank law. Moreover, this limitation amount is depended on the bank policy, privilege or account type, local bank and third party account wanted. We observe on this transaction



limitation because of this limitation can protect users from hacker transfer huge amount of money from users account.

Particularly, fund transfers are classified into several services such as transfer between bank account, to another interbank account (third party account), to another bank account and international fund transfer. So, it is important for banks and users to concentrate on this transaction limitation. In some aspects, it can protect users and banks from social engineering or hackers steal their money incidentally.

4.1.6 Alerting System and Transaction Activity

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.

Furthermore, we also observed on the session timeout (minutes). It is one of the safety mechanism to protect users eventually forget to log-out, if it is on own user's computer is not problem but for a public computer it can be a serious problem. It is really important for the bank to access, integrate and determined the interval time or period on internet banking after inactivity or standby after users' transactions. Surely the time-out delay should be reflected to the security risks of the area that we applied (follow by best practice standard section 11.5.5: session time-out and 11.5.6: limitation of connection time). So in this section we observe on the session timeout and alerting system that bank deployed on their internet banking system in differently.

4.1.7 Other Additional Mechanisms

Banks had deployed a lot of safety mechanisms for their customers according to the bank supported system differently like scramble keyboard (to avoid keylogger) and browser supported for making users secure and convenience with the internet banking service. Moreover, some banks allowed their customer to suspend or re-new the internet banking service while having some problems with banking service or emergency facts. So, the additional mechanisms that some banks are listed as follow:

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



2) 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.

3) Browser Supported (Chrome, Firefox, Internet Explorer, Opera, Safari and others)

These all mechanism should be observed because it can help users immediately while they had some problems with the internet banking services.

4.1.8 Close Bank Account and Internet Banking Systems

Closing the bank account and its internet banking service is the last thing of our observation. Although this point has no effect to the robing attack, it can cause a DoS (Denial of Service) attack to the internet banking customer. Depending on the bank policy, most banks would allow a customer to close his/her bank account and the internet banking service within 3 months. In this step of observation, we focus on the authentication documents and details, required to close the bank account. So in this research we will observe on the authentication requirements and the way to close the internet banking according to four approaches that we already mentioned in Table 4.2.

Table 4.2 Close Bank Account and Internet Banking Systems

Close bank account and internet banking service with authentication requirements	
Through Bank Branches	Authentication Requirements: <ul style="list-style-type: none"> • Citizen identity card • Passport • Other valid documents
Through ATM	
Through Call Center	
Through Online	

4.1.9 Mobile Phone Service Provider (Mobile Center)

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 card, 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, we mainly observe on authentication documents, required to request a new mobile sim-card at the operator branches.

At this point, some muggers have known about victim's mobile number and go to the mobile center to request a new the sim-card with the same number of the victim with and without any authentication requirements. So, this research will observe on the ways of requesting the new sim-card with same number through branch office provider and small operator office and also observed on the authentication requirements is needed to request a new sim-card like identity card (original or copy), passport, and other supported documents as required. We selected top three mobile provider companies through subscribers [53] like Metfone (Me = 9 million in 2015), Smart Axiata (Sm = 5.4 million in 2013), Cellcard (Ce = 2.5 million in 2010), AIS (A = 44.3 million in 2014), DTAC (Dt = 30.6 million in 2014) and Truemove (Tr = 23.2 million in 2014).

4.1.10 Authentication of Bank Website

Normally, identification card is used to prove and identify the identity holder and personal information of the holder. It is issued by the government and other entitlements. So, the banking websites also has their own identity to identify the real bank like digital certificates and so on. Digital certificate covered with authorizer, expiration date, bank web site, its version and so on. Moreover, in this section we also observe on the supported protocol of bank's website. One of the security protocols for encrypt and decrypt all of user's confidential information over the internet.

- 1) Digital Certificate (version, signature algorithm, public key, valid from, valid until, common names, and issuer)
- 2) Supported Protocols (TLS and SSL)
- 3) SSL Analysis Report (Overall rating, forward secrecy, extended validation certificate, HTTPS supported and key exchanged)

We will observe on the security of internet banking website through three above, because of some attacks exploited on security of user's browser by using SSL



Mahasarakham University

Figure 4.1 SSL Strip Tested in Kali Linux

Mostly, the internet users use web browser to search information over the internet without type https:// in URL before web address. It can be affected by SSL stripping attack, if user's connection is being attacked. So all users should notice something is missing in the browser URL, for example like EV-SSL bar or HTTP without S and so on. It is important to test on the log-in web page of the bank at user side and username and password while they are log-in.

[illegible]

Heartbleed bug is a kind of bug in the Open SSL's implementation of the TLS (transport layer security protocols) heartbeat extension. It was disclosed the vulnerability publicly on 07 April, 2014. It leads to the leak of memory contents between the server and clients. It's the programming mistake in OpenSSL library. This kind of attack mostly target on internet banking, in order to steal username and password from internet banking's users and other sensitive information. To check this vulnerability, we use the "https://filippo.io/Heartbleed/" website to scan on this attack.

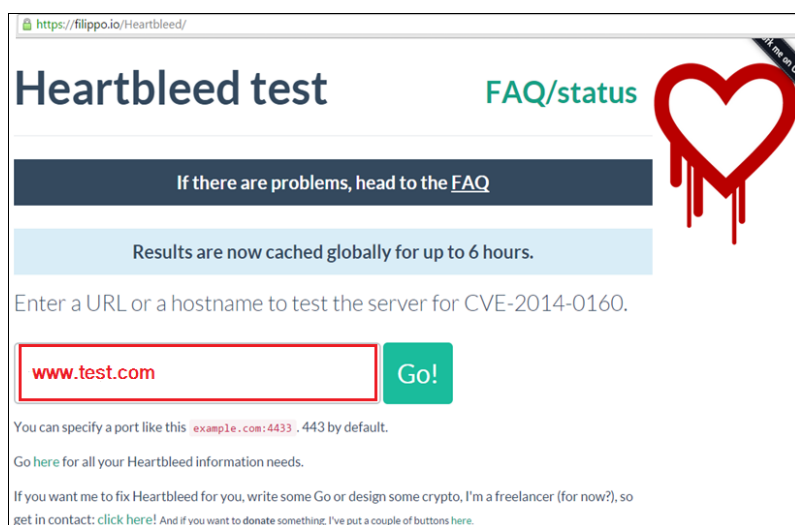
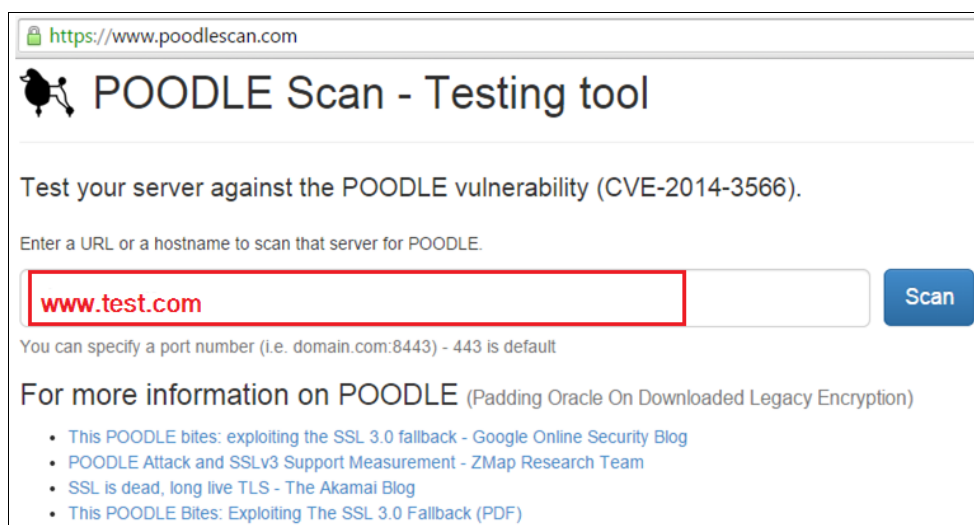


Figure 4.2 Heartbleed Testing Tool

POODLE (Padding Oracle On Downgraded Legacy Encryption) attack is a kind of exploit that takes advantage on the web setting by using man in the middle attack technique to downgrade the SSL 3.0 and deal with encryption. It was disclosed the vulnerability publicly on 14 October, 2014 and it is as serious as the Heartbleed Bug. So in this research, we observe on the log in web page of the internet banking by using this website "www.poodlescan.com" to scan on the internet banking log in web page. So we scan it to make sure the internet banking have capabilities and update to against this attack.





https://www.poodlescan.com

POODLE Scan - Testing tool

Test your server against the POODLE vulnerability (CVE-2014-3566).

Enter a URL or a hostname to scan that server for POODLE.

You can specify a port number (i.e. domain.com:8443) - 443 is default

For more information on POODLE (Padding Oracle On Downloaded Legacy Encryption)

- [This POODLE bites: exploiting the SSL 3.0 fallback - Google Online Security Blog](#)
- [POODLE Attack and SSLv3 Support Measurement - ZMap Research Team](#)
- [SSL is dead, long live TLS - The Akamai Blog](#)
- [This POODLE Bites: Exploiting The SSL 3.0 Fallback \(PDF\)](#)

Figure 4.3 Poodle Testing Tool

4.2 Results on Internet Banking Deployment and Safety Evaluation

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 bank to avoid conflicting with the bank. Without providing the real name, it can also help avoid guiding the hackers to the specific vulnerabilities of specific banks. So, the observation and deployment of internet banking service on three banks in Cambodia and three banks in Thailand are in the following section.

4.2.1 Open Bank Account and Internet Banking Registration

On the deployment and observation results on open bank account have found that all banks required a lot of authentication documents from their customers. In order open bank account, all of six banks required the original and valid citizen identity card contain with the local residential address (local citizen). For foreigners, all of six banks required the original and valid passport carried with valid visa and other supported evidences as show in Table 4.3.



Table 4.3 Requirements for Open Bank Account

Authentication Documents	A	B	C	D	E	F
1. Valid Identity Card	✓	✓	✓	✓	✓	✓
2. Valid Passport	✓	✓	✓	✓	✓	✓
3. Supported Evidence for Foreigner						
3.1 Non-immigration or Business Visa (> 30 days)	✓	✓	✓	✓	✓	✓
3.2 Work Permit	✓	✓	✓	✓	✓	✓
3.3 Local Residential Address	O	O	O	✓	O	✓
3.4 House Registration for permanent residency	O	O	O	O	O	O
3.5 Other Identity Card Issued by organization or university	O	O	O	O	O	O
3.6 Letter of recommendation with name issued by a local authorities or embassy	O	O	O	O	O	O
<i>Note: ✓: Accepted on original only; O: Optional</i>						

Three banks in Cambodia allow their customers to open bank accounts and register the internet banking through bank branch only. Three banks in Thailand allowed their users to open bank account at bank branch only but for the internet banking they can register through a bank branch, ATM and mobile application (for bank F only) as show in Table 4.4. 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 4.4 Apply for the Internet Banking

The Internet Banking Registration	A	B	C	D	E	F
1. Through Bank Branch	✓	✓	✓	✓	✓	✓
2. Through ATM	✗	✗	✗	✓	✓	✓
3. Through Call Center	✗	✗	✗	✗	✗	✗
4. Through Online/ Mobile Application	✗	✗	✗	✗	✗	✓

Moreover, the required authentication documents for opening bank account between these two countries are quite the same as shown in Table 4.5. For example, citizen identity card plus with local residential address, and valid passport plus with work permit or other related documents issued by government authorities, organization or university. We also notice that all banks process rather strictly on the foreigner to open bank account and internet banking registration. They focus on valid visa and the staying period. If it is less than 30 days, opening the bank account and internet banking account are not allowed.

For the foreigners, work permit and other documents, issued by local authorities are extra required for open the bank and internet banking accounts. According to our observation on the local citizen, we have found that all five banks require the real ID. Yet, there is a bank in Thailand (the bank F), allowing the customer to use soldier ID to open the bank account. None of them allows the photocopy of ID for opening the bank account.

Table 4.5 Internet Banking Registration Requirements

Must Have	Optional Requirement	Supported Requirement
Passbook	Driving License	Memorable Question
Citizen Identity Card	Phone Number	ATM Card
Passport	Email	PIN Number

In Cambodia, some banks have also trained their staffs how to carefully check whether the ID is real or fake. According to the crime cases in reference [18-20],

the hackers have used the faked documents of other government authority ID 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 soldier ID document. Generally, the citizen ID is very familiar to bank staffs. However, other government authorities' documents (such as army ID or soldier ID 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 ID and soldier ID properly. Otherwise, this would be vulnerability.



Figure 4.4 Cambodian and Thailand Smartcard

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 ID is now a smartcard with an EV chip while the Cambodia ID (Figure 4.4) can be a non-smart card. Since the smartcard is more difficult to be faked, Thai ID is safer from spoofing in comparison to the Cambodia one.

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. To register for an internet banking in Cambodia, all three banks require the customers to register the 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 term 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.

4.2.2 Username and Password

After registration completed, all banks deliver the username/password in different ways. We have found that there are four ways to delivery temporary or permanent username and password to their customers like via email, post office, ATM slip and shield letter. From the observation results in Table 4.6, for Cambodian Banks (A, B, C), bank A delivers a temporary username and password through bank slip or shield letter as show in Figure 4.5 while users registered at the bank branches and alert users to change its within 30 days.

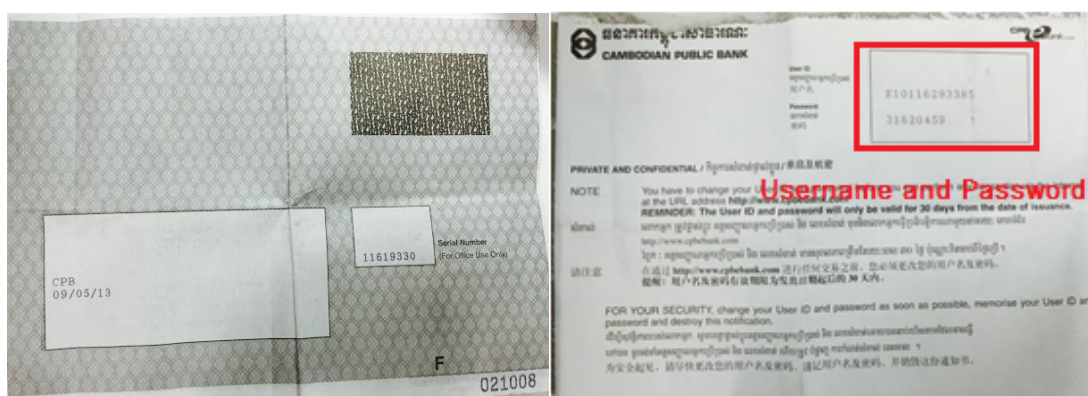


Figure 4.5 Shield Letter

For bank B, they have delivered the temporary username and password through email with expiration 2 days. Especially, the temporary username that bank B sent through email is the permanent username (cannot change) as show in Figure 4.6.



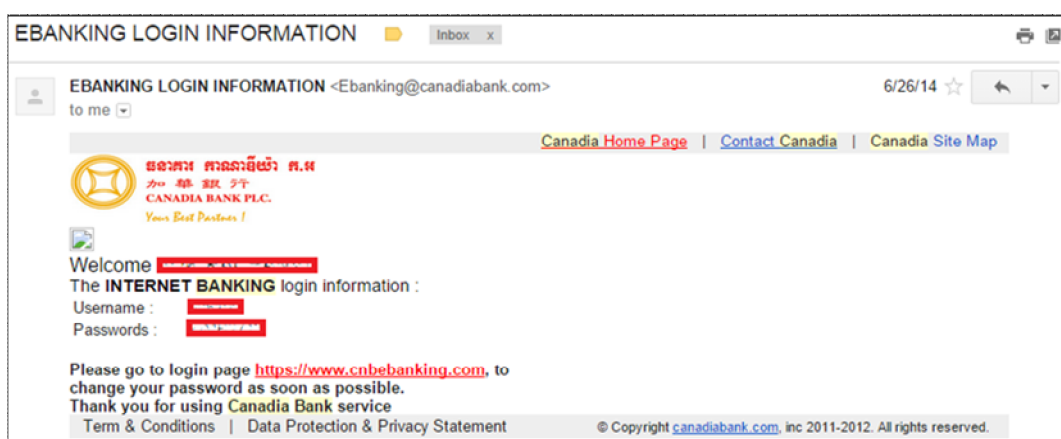


Figure 4.6 Username and Password Sent Through Email

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.

Table 4.6 First Time Registration for Bank A, B and C

First Time Registration Through Branch	A	B	C
1. Provision of Temporary Username and Password	✓	✓	✓
1.1 Through Email	✗	A	P
1.2 Through Shield Letter	A	✗	✗
1.3 Expiration	30days	2days	7days
2. Manually Set By User	✗	✗	U
3. Fixed Set By Bank	✗	U	✗
<i>Note: ✓: Have; ✗: Don't have; U: Username; P: Password;</i> <i>A: All (Username + Password);</i>			

According to the internet banking service's registration in section 4.1.1 for bank D, E and F in Thailand, there are two ways to register the internet banking services (through branch and ATM). From the results in Table 4.7, 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 allow 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 allow setting the username and password at its internet banking web page.

Table 4.7 First Time Registration for Bank D, E and F

First Time Registration	Through ATM			Through Branch		
	D	E	F	D	E	F
1. Provision of Temporary Username and Password	✓	✓	✗	✓	✓	✗
1.1 Through Email	✗	✗	✗	U	✗	✗
1.2 Through Shield Letter	✗	✗	✗	✗	A	✗
1.3 Through ATM Slip	U	U	✗	✗	✗	✗
1.4 Through Post	✗	✗	✗	Pi	✗	✗
1.5 Through SMS	✗	✗	✓	✗	✗	✓
1.6 Expiration	3days	2days	3hr	3days	2days	3hr
2. PIN Number through ATM	✓	✓	✗	✗	✗	✗
3. Online Set By User	P	P	A	P	✗	A
4. Activation Code	✗	✗	✓	✗	✗	✓
<i>Note: ✓: Have; ✗: Don't have; U: Username; P: Password; A: All (Username + Password); Pi: PIN; hr: Hour</i>						



All these different ways of authenticating the customer in registering for the internet banking seem to be 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.

The bank staffs of all six banks have recommended the customers to set a good password, containing with special characters, uppercase, lowercase, and numeric (Table 4.8). 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).

Table 4.8 Username Limitation

Username Limitation	A	B	C	D	E	F
1. Minimum Length of Characters	6	F	A	6	6	8
2. Maximum Length of Characters	12	F	A	32	12	20
3. Contain with Characters (Minimum)	1	F	A	1	1	1
3.1 Contain with Special Characters	×	F	A	×	×	**
3.2 Contain with Uppercase, Lowercase	1	F	A	×	×	×
4. Contain with Number (Minimum)	1	F	A	1	1	1
5. Others Cases	*	×	×	×	×	***
<p><i>Note: A: Any by user; ×: Don't have; F: Fixed set by Bank; 1: At least one character or number;</i></p> <p><i>** : Supported only "." or "_"; ***: No Repeat Characters</i></p> <p><i>*: First and second characters must be alphabetical;</i></p>						



For the safety reason, long passwords 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”.

Table 4.9 Password Limitation

Password Limitation	A	B	C	D	E	F
1. Minimum Length of Characters	8	6	10	8	8	8
2. Maximum Length of Characters	12	16	14	32	20	20
3. Contain with Characters (Minimum)	1	1	1	1	1	1
3.1 Contain with Special Characters	✗	1	**	1	1	1
3.2 Contain with Uppercase, Lowercase	1	1	1	1	1	1
4. Contain with Number (Minimum)	1	1	1	1	1	1
5. Others Cases	✗	✗	✗	✗	*	***
<i>Note: ✓: Have; ✗: Don't have; 1: At least one character or number; ***: No Repeat Characters; *: except (“”, “”, “&” and “Space”); **: Supported “@” or “#” or “\$”</i>						



According to Table 4.9, all banks have set the restriction on password for their users in average from 6 to 20 characters. We also found that one bank (bank A) not allowed their users with special characters on password and bank C allowed only three special characters like “@”, “#”, and “\$”. For bank E and F are different from other banks but bank E have a special case like they allowed all special characters except “”, “”, “&” and “space” and special case of no repeat characters for bank F on their users password.

The lockout policy is the 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 help 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 from the accident. From our observation on the six banks, Bank C (from Cambodia), Bank D and E (from Thailand) allows 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 no allow the first name as the username.



Table 4.10 Username and Password Recovery

Username and Password Recovery	A	B	C	D	E	F
1. Through Call Center (Call Center Authentication)	P	×	P	A	A	A
2. Through Online (Two-factor authentication)	×	P	A	P	P	P*
3. Through ATM	×	×	×	A	×	P
4. Through Branch (Authentication Documents)	A	A	A	A	A	A
<i>Note: ×: Don't have; U: Username; P: Password;</i> <i>A: All (Username and Password); P*: Password through Mobile Application</i>						

According to Table 4.10, 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 of changing username and password, OTP has used to authenticate with real customers by sent 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.

In addition, all banks allowed their users to reset username and password through branch bank with authentication requirements like citizen identity card/passport and passbook but it is effect to user's convenience (spend time) to go to the branch.

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.

Table 4.11 Change Mobile Number

Changed Through	A	B	C	D	E	F
Internet Banking System	✗	✗	✗	✗	✗	✓
Bank Branch	✓	✓	✓	✓	✓	✓
Call Center	✗	✗	✗	✗	✗	✗
ATM	✗	✗	✗	✗	✗	✓
<i>Note: ✓: Allowed; ✗: Not Allowed</i>						

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 except bank F as shown in Table 4.11. 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 4.11. For changing it via call center is not possible for all six banks in our research.



4.2.3 Call Center Authentication

From the observation results of call center authentication have showed that some questions to authenticate with 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 those 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.

Table 4.12 Call Center Authentication

User Confidential Information Asked	A	B	C	D	E	F
1. Account Number or Phone Number	✓	✓	✓	✓	✓	✓
2. Username or Account Name or Nickname	✓	✓	✓	✓	✓	✓
3. Birthdate or Day of Birth	✓	✓	✓	✓	✓	✓
4. Email Address	✓	✓	✓	✓	✓	✓
5. Identity Card Number or Passport Number	✓	✓	✓	✓	✓	✓
6. ATM Expiration Date or ATM PIN Number	✓	✓	✓	✓	✓	✓
7. Branch of Open Bank Account	✓	✓	✓	✓	✓	✓
8. Current Address	✓	✓	✓	✓	✓	✓
9. Last Transaction and Activity	✓	✓	✓	✓	✓	✓
10. Memorable Question and Answer	✓	✗	✓	✗	✗	✗
<i>Note: ✓: Have; ✗: Don't have</i>						

It is really important for call center to authenticate with users (user's identification) or account owner. Also some questions should be asked to identify with the real user as shown in Table 4.12. From the observation results, all of criteria or information in Table 4.12 can be asked through call center while the user reset their



username or password and other information related to account transactions. In conclusion, some questions can be asked for authenticate with users but some questions could not asked like phone number, identity card number, birthdate and so on (should be compromised by social engineering).

4.2.4 Two-factor Authentication

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).

Table 4.13 One Time Password

One Time Password	A	B	C	D	E	F
1. Type of OTP						
1.1 SMS OTP	✓*	✓	✗	✓	✓	✓
1.2 Email OTP	✗	✗	✗	✗	✗	✗
1.3 Mobile or Soft OTP	✗	✗	✓ ^{\$}	✗	✗	✗
1.4 Token OTP	✓* ^{\$}	✓* ^{\$}	✓ ^{\$}	✓* ^{\$}	✓* ^{\$}	✓* ^{\$}
2. OTP Length (Character)	6	6	6	8	6	6
3. Cost	✓	✓	10-15\$	✓	✓	✓
4. Expiration (minutes)	5	5	1	5	5	5
Note: ✓: Have; ✗: Don't have; ✓*: PAC(Personal Authentication Code); ✓* ^{\$} : High Class Customers are allowed and cost money; ✓ ^{\$} : Allowed with costing money						

We also found that three banks in Thailand used SMS OTP to confirm with customers transactions (Table 4.14). 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 4.14 One Time Password Deployment

OTP Deployment	A	B	C	D	E	F
1. Transactions Activity						
1.1 First Time Registration	✗	✗	✗	✓	✓	✓
1.2. Log-in Webpage	✗	✗	✓	✗	✗	✗
1.3 Transfers to 3 rd Party Within Bank Account	✓	✓	✓	✓	✓	✓
1.4 Transfers to 3 rd Party At Others Bank Account	✓	✓	✓	✓	✓	✓
1.5 Bill Payment	✓	✓	✓	✓	✓	✓
1.6 Top-Up	✗	✗	✓	✓	✓	✓
1.7 Add New Account	✓	✗	✓	✓	✓	✓
1.8 Others Payments (Credit Card, Debit Card and so on)	✓	✗	✓	✓	✓	✓
2. Change Settings						
2.1 Username	✓	✗	✗	✗	✓	✓
2.2 Password	✓	✓	✓	✗	✓	✓
2.3 Phone Number	✓	✗	✗	✗	✗	✓
2.4 Daily Transaction Limitation	✓	✓	✓	✓	✓	✓
2.5 Update Personal Details	✓	✓	✗	✗	✗	✓
<i>Note: ✓: Have; ✗: Don't have</i>						

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 provide 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 4.15 CAPTCHA and Other Mechanism

CAPTCHA and Others	A	B	C	D	E	F
1. First Time Registration	✗	✗	✗	✓	✗	✓
2. Log-in Webpage	✗	✗	✗	✗	✗	✓
2.1 Auto Pop-up	✗	✗	✗	✗	✗	✗
2.2 Failure Pop-up	✗	✗	✗	✗	✗	✓
3. Transactions	✗	✗	✗	✗	✗	✗
4. Change Settings	✗	✗	✗	✗	✗	✗
5. Secure Code (Log-in Webpage)	✗	✓	✗	✗	✗	✗
6. Activation Code	✗	✗	✗	✗	✗	✓
<i>Note: ✓: Have; ✗: Don't have</i>						

Particularly, we also observed on the implementation of CAPTCHA in the internet banking transactions as show in Table 4.15. 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.

4.2.5 Transaction Limitation and Alerting System

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.



Table 4.16 Alerting System and Cost of its

Alerting System	A	B	C	D	E	F
1. Transaction Activities						
1.1 Log-in	✗	✗	✗	✓	✓	✓
1.2 Log-out	✗	✗	✓	✓	✓	✓
1.3 Transactions (Transfer, Payment, Top-up and so on)	✓	✓	✓	✓	✓	✓
1.4 Money-In and Out	✓	✓	✓	✓	✓	✓
1.5 Change Settings (Username, Password, and so on)	✗	✓	✓	✓	✓	✓
2. Type of Alert and Cost						
2.1 Through Email	✓	✓	✗	✓	✓	✓
2.2 Through SMS + Cost	✓	✗	✗	✓	✓	✓
2.3 Through Web Browser	✗	✗	✓	✓	✓	✓
3 Session Time-out	✓	✓	✓	✓	✓	✓
<i>Note: ✓: Have; ✗: Don't have</i>						

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 charged 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 4.16, we found that three banks in Cambodia give the alert for financial transaction (such as transfer, payment, and top-up) only.

4.2.6 Other Additional Mechanisms

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 4.17. We can conclude that both Thailand and Cambodia are still not take it serious on using screen keyboard to protect the key logger problem. Only one bank from each country supports the screen keyboard option. One big problem has found in the usage of 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 4.17 Virtual Keyboard

Virtual Keyboard	A	B	C	D	E	F
1. Username	✗	✗	✗	✗	✗	✗
2. Password	✗	✓	✗	✗	✗	✗
3. One Time Password	✗	✗	✗	✗	✓	✗
4. Amount Money	✗	✗	✗	✗	✗	✗
5. Visible	✗	✗	✗	✗	✓	✗
6. Others (PIN or Card Number)	✗	✗	✗	✗	✓	✗
<i>Note: ✓: Have; ✗: Don't have</i>						

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 as show in Table 4.18. This can be very serious when the customer wants to report the hacking case and pauses their internet banking.

Table 4.18 Pause the Internet Banking Service

Pause the Internet Banking	A	B	C	D	E	F
1. Through call center	✗	✓	✗	✓	✓	✓
2. Through branch	✓	✓	✓	✓	✓	✓
3. Through online	✗	✗	✗	✗	✗	✗

To use the internet banking services, all users need to have their own computer and web browser for log-in. So in this section, we also observed on the top 5 browsers that are popular in nowadays like Chrome, Firefox, Safari and so on.



Table 4.19 Browser Supported

Browser Supported	A	B	C	D	E	F
1. Chrome	✓	✓	39/43	14	✓	20
2. Firefox	✓	3.1	34	6	✓	4
3. Internet Explorer	5.5	7	8-11	8	✓	8
4. Safari	✓	3.5	8.0	5	✓	5
5. Opera	✓	9.5	×	✓	✓	✓
6. Others	✓	✓	✓	✓	✓	✓
<i>Note: ✓: Have</i>						

Most of the banks in our research are supported with all browsers that we mentioned in Table 4.19 but only bank C is not supported in the past (supported only IE and required to add bank log-in webpage in compatibility view settings of IE).

However, in nowadays they had upgraded their internet banking system to support with all browsers in august 2015. Moreover, all banks had deployed many ways to help users like frequently ask questions (FAQ = popular questions had asked to bank with the banking services) when users had problem with all banking services especially the internet banking services. Most of the bank in our research allowed users to contact through email and call center, it is convenience and flexible with questions. However, to provide services with the modern technology some banks (bank E and F) allowed users to communication with bank's staff and reduce users cost through via web chatting, call back service, online application and web collaboration (bank E only).

4.2.7 Close Bank Account and Internet Banking Systems

Closing bank account and the internet banking systems required all users go to the account holder branch holding with initial registration documents. Surely, from the experience withdraw all money out and keep that account with non-activity within 3 months, the bank account will be suspended. However, we found that only bank (bank E) in our research allowed users to close the internet banking through online by clicking on cancel membership. All of them required all users to close the internet banking at the account holder branch.



4.2.8 Mobile Center

We totally observed on six mobile centers, three operators in Cambodia and three operators in Thailand. Most of the operator branch office in these two countries required strictly on 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 the crime cases happened similar to Thailand on requesting 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 the weakness for some Thai operators.

Table 4.20 Request New Sim-card at Operators

Authentication Requirements (B: Branch Office, S: Small Office)	Mobile Phone Provider											
	Me		Sm		Ce		Dt		A		Tr	
	B	S	B	S	B	S	B	S	B	S	B	S
1. Identity Card (Original/ Copy)	O	A	O	A	O	A	A	×	A	×	A	×
2. Passport (Original/ Copy)	O	×	O	×	O	×	O	×	O	×	O	×
3. Driving License	/	✓	/	✓	/	✓	✓	×	✓	×	✓	×
4. Student ID Card	✓	✓	✓	✓	×	×	/	×	/	×	/	×
5. Other identity documents	✓	✓	✓	✓	✓	✓	✓	×	✓	×	✓	×
Note: ✓: Accepted; ×: Not Accept; /: Optional; O: Original; A: All (Original or Copy); Me: Metfone; Sm: Smart; Ce: Cellcard; Dt: Dtac; A: AIS; Tr: Truemove												

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 giving them a wrong sim (the sim of other phone number). We have found that they do 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 the signal, and our pretended hacker can get the victim SMS OTP. This lesson guides to any bank customers that if their mobile phone, deployed as SMS OTP receiver, happen to have no signal without reason, they should try to ring their own number. If they found that it can be rung up 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.

4.2.9 Discussion for Three Banks Results in Cambodia

According to the observation and the internet banking deployment results, we found that all banks in Cambodia allowed their customers to open bank account at bank branches only. They must carried with the original citizen identity card (for local citizen) and the original passport with valid visa and work permit (for foreigner) or other supported evidence make sure with their current address or any evidence that ensure for them can open bank account. We can see that some supported document just covered with name and address only as show in Figure 4.7 and Figure 4.8. If the mugger can bypassed this section by faking the supported evidence, everything will be compromised comparing with the crime cases that already happened in Thailand.



Figure 4.7 Work Permit in Cambodia



However, there are no differences between three banks in Cambodia to register the internet banking services. They must go to the account holding branch or other bank branches for register this service. It is really difficult for the mugger to bypass this section in Cambodia because the customer services will verify the current register user with the authentication documents of real account owner before register the internet banking services for them.

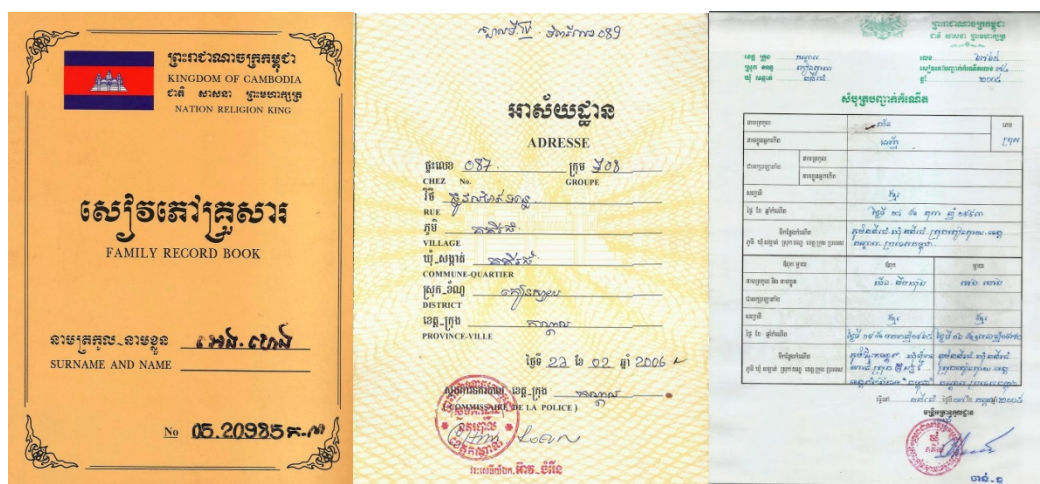


Figure 4.8 Family Book and Birth Evidence Issued by Local Authorities

In addition, we found that there are several citizen identity cards in Cambodia as show in Figure 4.9. It is difficult to recognize the real citizen identity card and valid one but now government try to decrease the type 1 and type 2 to become type 3 as quiet as they can. So, we can conclude that all of authentication requirements are secure enough to prevent social engineering but it has some weakness on recognized with the original documents like citizen identity card, passport and documents issued by government with the bank's staff.





Figure 4.9 Cambodia Citizen Identity Card

Moreover, we also found that the banks have sent username and password through shield letter is better than sent it through via email. For the username and password restriction of three banks in Cambodia was set in differently and strictly confirm. However, all banks in Cambodia suggested their users to reset username through bank branches only and password can be reset through call center and online according to the bank procedures.

Most of the banks in Cambodia do not place the alerting system automatically for users. It can be placed but the user has to cost money on this service. Moreover, only one bank (bank B) in Cambodia employed virtual keyboard at the password area for their users. So, we can see that all banks in Cambodia deployed the internet banking service differently even they are in one country but some authentication transactions and requirements almost the same according to the bank procedures.



4.2.10 Discussion for Three Banks Results in Thailand

All banks in Thailand are strictly with foreigners who want to open bank account, and they need many evidences from foreign users especially passport, visa and work permit (Figure 4.10). Also, the internet banking registration can be done over via online, ATM and mobile application. It is convenience and secure for users to register the internet banking through ATM and online/mobile application. However, we found that one bank (bank F) in Thailand placed automatic add all account after the internet banking completed. If we compare to the internet banking crime cases, this point should be placed as manually because of the mugger can bypassed the internet banking registration and then all victim account will be insecure if it is auto add all account.



Figure 4.10 Work Permit in Thailand

We also found that all banks in Thailand allowed their users reset username and password through call center, ATM and online/mobile application. Yet, only one bank (bank E) not allowed foreigner to reset username and password through ATM but local citizen can do it through ATM. For the call center authentication, some questions almost the same as Cambodia like bank account, account holder name, birthdate and so on. Some information of the user can know easily, if social engineer to capture all users information. The bank should be set some secure questions to verify with the real user beside some general questions, notable point at call center authentication.

Moreover, SMS OTP and Token OTP (for high class users only) have been occupied all around Thailand to verify with real user and some transactions activities



like transfer funds, bill payment, top-up, add account, change account settings and other miscellaneous payment. However, we found that OTP did not use at the internet banking log-in webpage for all banks in Thailand and one bank (bank D) did not use it at change account settings excepted changing limitation of daily transactions.

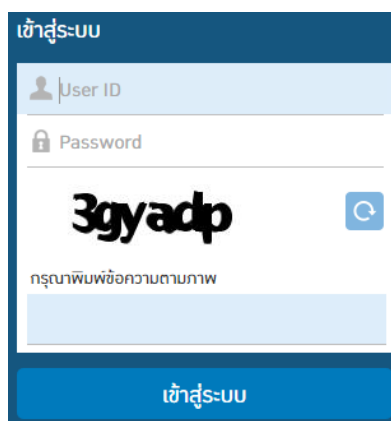


Figure 4.11 CAPTCHA Auto Pop-up

In addition, we also found that CAPTCHA had been used in bank F for failure log-in. When the user log-in fail within two times, CAPTCHA is automatically popup (as shown in Figure 4.11) to make sure it is not the malware or some brute force attack software of the hacker. We also found that one bank (bank D) used this CAPTCHA at the first time registration only.

Moreover, we found that all banks in Thailand deployed another security mechanism for their users like alerting system for the internet banking transactions. They used it for the log-in into account, transfer funds and other services through via email but it will cost some money if it is alert through via mobile SMS. We also found that virtual keyboard has been used in OTP textbox and PIN number inserting box for bank E only and also it is visible. So, we can conclude that all banks in Thailand conduct the internet banking service in different ways for their users but also some implementation from open bank account till close account and other authentication requirements are the same just some parts are different from each other according to the bank policies.

4.2.11 Safety Suggestion and Enhancement for the Internet Banking

Systems

To register for the internet banking, authentication documents requirement are different between Cambodia and Thailand. For Cambodia's bank, all three banks require the customers to register the internet banking only at their bank branch. The required documents are citizen identity card or passport, passbook, a phone number, and an e-mail. Driving license or officer identity cards may be used instead of the identity card. ATM card is optional. For Thailand's bank, the registration can be done at the bank branch, or other choices. If registering at the bank branch, the required documents are more or less the same as the Cambodian banks. One of the Thai internet banking registration choices is registering via ATM if the customers have 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 is obviously safe. Yet, it is not convenient for the bank customers, and creates a lot of workload at the bank branch. So, the ATM option of Thai banks can be a good choice. It would be rather difficult to compromise the ATM registration because the hackers would need to steal the customer's ATM card, knowing his PIN and get his mobile phone.

After registration completed we found that all bank in our research delivered the username and password differently like bank A delivered temporary username and password of users through shield letter with expiration 30 days while registration at bank branch, for bank B sent permanent username and temporary password through via email with expiration 2 days and username is set by bank (cannot changed), for bank C sent only temporary password through via email with expiration 7 days to reset new password and permanent username is manually set by user at bank branch while registering.

For bank D sent temporary username through email and PIN number through post office with expiration 3 days, bank E sent temporary username and password through shield letter like bank A but it is special for foreigner can register the internet banking through bank branch only, for bank F sent only activation code through SMS with expiration 3 hours and set username and password on log-in web page. For ATM registration, we also found that bank D and E sent temporary username through ATM slip with expiration 2 to 3 days and log-in with PIN number to set new password.



Bank F sent only activation code through SMS and set username and password through log-in web page.

Furthermore, Cambodia and Thailand is the near border countries in Southeast Asia. For foreigners who want to open the bank account in these two countries, they need to have passport, visa and work permit or other evidences to ensure they have rights to open bank account. As show in Table 4.21, we found that Cambodia and Thailand's authorities exempted visa for tourist visa that stayed less than 14 days for regular passport and 30 days for diplomatic and service passport.

Table 4.21 Exempted Visa for Cambodia and Thailand

Countries	Duration of Tourist Visa		
	Diplomatic Passport	Service Passport	Regular Passport
Cambodia	30 days	30 days	14 days
Thailand	30 days	30 days	14 days

Moreover, we can see that all banks in our research are using SMS OTP more than Token OTP. Token OTP is more secure than SMS OTP because nowadays mobile malware had distributed all around the world to capture all users' information by hacker. However, all banks should recommend their users to use Token OTP even it costs some money but more secure and more confident than SMS OTP.

From the observation results of call center authentication, call center's staff should be asked some strict question or memorable question that had set at the first time registration make sure the user information is not compromised. However, bank's staff will recognized well on the real user otherwise they will suggested the user to go to the branch as possible as user can beside giving some information to them, if the answer is wrong.

According to crime cases, we can see that mugger faked victim's identification card and go to small operator of mobile center to request the new sim-card by confirm with operators that mobile lost. From the observation results, we found that all small operators in Cambodia accept all kind of citizen identity cards (copy and original), driving license, student identity card to request new sim-card but now is



changed. If users want to request new sim-card they have to go to head or nearest branch office operators to request it. It is the same as Thailand in nowadays, all mobile users has to go to register sim-card at nearest branch office operator otherwise it will be terminated within one month.

4.3 Results on Internet Banking Security Evaluation and Experiment

4.3.1 Bank Authentication

For the digital certificate is really important to identify that is the real bank web page. As the result in Table 4.22: Digital Certificate Result, it showed that all banks in both countries using version 3 of digital certificate, 2048 bits of public key, and specific common names and valid dates of certificate's expiration.

Table 4.22 Digital Certificate Results

Digital Certificate	A	B	C	D	E	F
1. Version	3	3	3	3	3	3
2. Signature Algorithm	SHA2	SHA2	SHA2	SHA1	SHA1	SHA2
3. Public Key	2048bits	2048bits	2048bits	2048bits	2048bits	2048bits
4. Valid From	03/2015	12/2014	03/2015	05/2015	09/2014	05/2015
5. Valid Until	05/2017	12/2016	03/2017	06/2016	10/2015	10/2016
6. Common Names	✓	✓	✓	✓	✓	✓
7. Issuer	SG3	SG3	SG3	SG2	EL1E	EL1M
<p><i>Note: ✓: Have; ✗: Don't have; EL1M: Entrust Certification Authority- LIM</i> <i>EL1E: Entrust Certification Authority- L1E;</i> <i>SG2: Symantec Class 3 EV SSL CA- G2;</i> <i>SG3: Symantec Class 3 EV SSL CA- G3</i></p>						

Moreover, all banks supported with SHA2 algorithm excepted bank D and E supported with SHA1. Also, three banks (bank A, B and C) issued by Symantec Class 3 EV SSL CA – G3 (SG3). Bank D issued by Symantec Class 3 EV SSL – G2 (SG2).



Bank E and F issued by Entrust Certification Authority just bank E (L1E) and bank F (L1M).

According to Table 4.23, all banks certificate supported with protocols of TLS version 1.0 to 1.2 that is different with supported protocols of SSL version 2 and 3, some bank supported and some bank are not supported. However, none of banks supports SSL version 2. For bank C and E, they support SSL version 3, which is a weak protocol for the bank. This is because it can be vulnerable to POODLE attack on the downgrade SSL version 3.

Table 4.23 Supported Protocols

Supported Protocols	A	B	C	D	E	F
1. TLS 1.2	✓	✓	✓	✓	✓	✓
2. TLS 1.1	✓	✓	✓	✓	✓	✓
3. TLS 1.0	✓	✓	✓	✓	✓	✓
4. SSL 3	✗	✗	✓	✗	✓	✗
5. SSL 2	✗	✗	✗	✗	✗	✗
<i>Note: ✓: Have; ✗: Don't have;</i>						

Moreover, we had scanned on the SSL by using Qualy's SSL lab as shown in Table 4.24. The results have shown that three banks (bank A, D and F) got grade A-, two banks (bank C and E) got grade C and one bank (bank B) got grade F. Mostly, they have supported with extended validation certificate (EV-bar) and HTTPS for their banking websites. Also, the entire banks in our research have supported with RSA key exchanged for secure data connection. However, we found that none of banks have supported HSTS [54] (is a new mechanism of web security used to secure HTTPS connections on websites and is specified in RFC 6797). Moreover, the details of scan results have shown in Appendix D.



Table 4.24 SSL Scan Report

SSL Scanning	A	B	C	D	E	F
1. Overall Rating	A-	F	C	A-	C	A-
2. Extended Validation Certificate	✓	✓	✓	✓	✓	✓
3. HTTPS Supported	✓	✓	✓	✓	✓	✓
4. Key Exchanged	RSA	RSA	RSA	RSA	RSA	RSA
5. HSTS Supported	✗	✗	✗	✗	✗	✗
<i>Note: ✓: Have; ✗: Don't have; HSTS: HTTPS Strict Transport Security</i>						

4.3.2 Experimental Results

From the experimental results (in Table 4.25) have shown that all browsers and all banks log-in webpage at the client side is secure enough to protect users from SSL sniffing attack.

Table 4.25 SSL Sniff, Strip, Heartbleed and Poodle Attacks

Attacking	A	B	C	D	E	F
1. SSL Sniff	S	S	S	S	S	S
2. SSL Strip	V	V	U	V	U + P	U + P
3. Heartbleed	S	S	S	S	S	S
4. Poodle	S	V	V	S	V	S
<i>Note: S: Secure; V: Vulnerable; U: Username; P: Password</i>						

However, there are three banks affected with the SSL stripping attack (bank C, bank E and F). We can capture all of users' information (username (U) and password (P)) from bank E and F as shown in Figure 4.13. Especially, for the bank C, we can capture only the username of the user as shown in Figure 4.12. After scanning on the Heartbleed Bug and the POODLE attack, it has been shown that bank A and B are affected by Heartbleed bug, and bank C and E are affected by the POODLE attack.



```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ls
Desktop sslstrip.log
root@kali:~# sslstrip.log
bash: sslstrip.log: command not found
root@kali:~# cat sslstrip.log
2015-09-27 05:16:19,438 POST Data (10.99.92.10):
username=[REDACTED]&password=[REDACTED]&pwd=[REDACTED]&secret=true
2015-09-27 05:22:42,675 POST Data ([REDACTED]):
loginid=[REDACTED]&uipassword=&languageName=en_US&locale=en_US&password1=7c33
787c98c13f39f427facdd37c424c&password2=643d47ba7041c3c35790992c0a877681004b65b99
05727922067c8f6f98af185&sessionId=p7vPwH7KmNJS58DqpQh3pfTM66kSgp0GN1wn1XXs13c3C6
5wJr48%212036392842%21778071599%211443331018578&authenticateToken=true
root@kali:~#

```

Figure 4.12 SSL Strip on Bank C

```

root@kali: ~
File Edit View Search Terminal Help
05727922067c8f6f98af185&sessionId=p7vPwH7KmNJS58DqpQh3pfTM66kSgp0GN1wn1XXs13c3C6
5wJr48%212036392842%21778071599%211443331018578&authenticateToken=true
2015-09-27 05:27:02,121 SECURE POST Data ([REDACTED]):
timestamp=&localeId=en_US&platform=D&appID=TMB&appver=1.0.12.25&serviceID=getPh
rases&locale=en_US&channel=wap&platform=thinclient&cacheid=&tknid=&rcid=spadeskt
opweb&
2015-09-27 05:27:03,324 SECURE POST Data ([REDACTED]):
widgetName=segCampaignImage&formName=frmIBPreLogin&appChannel=I&prelogin=Y&appID
=TMB&appver=1.0.12.25&serviceID=GetCampaign&locale=en_US&channel=wap&platform=th
inclient&cacheid=&tknid=&rcid=spadesktopweb&
2015-09-27 05:27:55,747 SECURE POST Data ([REDACTED]):
loginId=[REDACTED]&userid=[REDACTED]&password=[REDACTED]&appID=TMB&a
ppver=1.0.12.25&serviceID=IBVerifyLoginEligibility&locale=th_TH&channel=wap&plat
form=thinclient&cacheid=&tknid=1185E45766BB99E2C2D0E938CE58978B8FF309D35E7E9DFDC
684FF44F5D0841B&konyreportingparams=%7B%22plat%22%3A%22windows%22%2C%22aid%22%3A
%22TMB%22%2C%22aver%22%3A%221.0.12.25%22%2C%22aname%22%3A%22vit 1.0.12.25 build8
3%22%2C%22did%22%3A%221443331675909-0fd5-3376-650f%22%2C%22os%22%3A%2245%22%2C%2
2stype%22%3A%22b2c%22%2C%22dm%22%3A%22%22%2C%22ua%22%3A%22Mozilla%2F5.0%20(Windo
ws%20NT%206.3)%20AppleWebKit%2F537.36%20(KHTML%2C%20like%20Gecko)%20Chrome%2F45.
0.2454.101%20Safari%2F537.36%22%2C%22chnl%22%3A%22desktop%22%2C%22atype%22%3A%22
spa%22%2C%22fid%22%3A%22frmIBPreLogin%22%2C%22kuid%22%3A%22%22%2C%22rsid%22%3A%2
21443331675910-949a-11f9-f7e0%22%2C%22metrics%22%3A%5B%5D%7D&rcid=spadesktopweb&
2015-09-27 05:27:56,957 SECURE POST Data ([REDACTED]):
rqUUId=&LoginInd=login&TriggerEmail=yes&activationCompleteFlag=Login&appID=TMB&a
2015-09-27 05:40:11,324 SECURE POST Data ([REDACTED]):
LOGIN=[REDACTED]&PASSWD=[REDACTED]&lgln.x=31&lgln.y=4
2015-09-27 05:40:12,157 SECURE POST Data (www.scbeasy.com):
SESSIONEASY=07085573657269643D30393031323031353033335377C53636F64653D585230326633
394A3669747472785058674756566F73766C465850366B6E426A7035316878520503
2015-09-27 05:41:00,872 SECURE POST Data ([REDACTED]):
SESSIONEASY=07085573657269643D30393031323031353033335377C53636F64653D585230326633
394A3669747472785058674756566F73766C465850366B6E426A7035316878520503&undefined=u
ndefined
root@kali:~#

```

Figure 4.13 SSL Strip on Bank E and F



4.4 Results of In-depth Interview

As we mentioned in section 3.4 about in-depth interview follow by IOC, we found that the interview question is good enough gather information and opinion from well-versed staff of Campu bank. They have mentioned that all crime cases already happened in Thailand should be concerned very well. Yet, the way that muggers faked authentication documents is not a big problem for Campu bank. Campu bank's human resource department has initiated their staffs every six months at Campu bank's training center. It means that all bank staffs have capable enough to recognize on three types of Cambodian original citizen identity card. For foreigner, bank controls very well on authentication documents (passport, work permit and visa). Especially, the bank set the limitation strictly on money-in and out of foreign account.

For the internet banking registration, Campu bank has sanctioned their customers to register through account holder branch only. Moreover, to catch up with the real account owner bank has captured the account owner face, identity number and signature store in the bank system already. They also have an opinion on the registration of internet banking through ATM that it can be secured in sometime for the developed countries with era of the internet banking. Yet, for the infancy of Cambodia's internet banking, it may not make sense. Some of the customers are not well operated with ATM machines. Sometimes, the ATM card can also be skimmed by hackers.

“Username and password that sent through shield letter is very secured for our customers, face to face communication and confirm on access deployment” said by bank staffs. Moreover, they have also mentioned that username and password restriction has recommended to their customers very well by operation staffs at the beginning of registration. Campu bank has also allowed their customer to reset password through call center (one time only), if their customers bypassed the authentication questions and the secure questions. Otherwise, the customer will go to the account holder branch in order to reset a new password. For the username, it can be reset through the bank branch only. They have also mentioned that the fixed username was set by bank. It may secure, easy to control, and verification with the owner but it can be risky with negligence of user's information management.

“We did not do that on auto adding all accounts like one bank in Cambodia and one bank in Thailand have deployed it. It makes a lot of complexity for customers in



Cambodia.” said by Campu bank staff. However, they have implemented it in different ways by allowing the customer call to call center or bank branch to add account and confirm with authentication questions and documents respectively. It has affected to user’s convenience but it is secure for customers’ transaction.

For alerting system of Campu bank, they have mentioned that it has deployed for financial transaction only (like transfer, top-up or payment and so on). It won’t make sense to implemented this alerting system in all transactions even log-in and log-out. Sometimes it can make users annoy with the system but sometimes it can be secure for them (real time helping services).

For the security observation, they have mentioned that bank’s log-in website not hundred percent relies on digital certificate and HTTPS. Sometimes it can be exploited according to our experiment but we have encrypted very well on the confidential data of users. Moreover, they have also interested on the new protection mechanism, proposed by this thesis (mentioned in the next section).

4.5 Security Suggestion and Enhancement

As the normal connection defined, all of internet banking log-in webpage used HTTPS connections and EV-SSL certificate to protect their log-in webpage. In contrast, we found that all of banks in our research are remain in effect of SSL stripping attack as showed in section 4.3.2 and Figure 4.14.

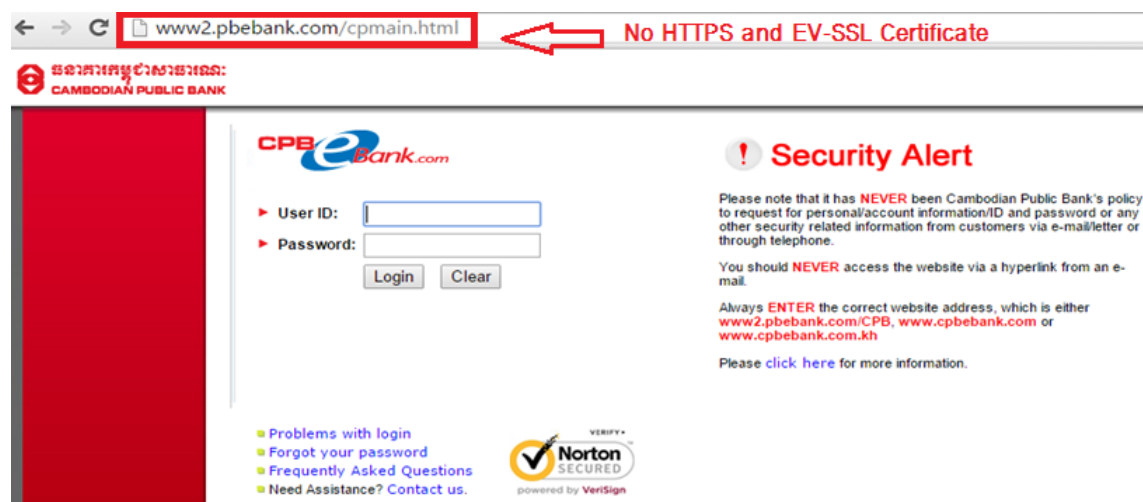


Figure 4.14 Internet Banking Log-in Webpage after Stripping Attack



So, we propose to design a new protection mechanism for the internet banking log-in webpage of Campu Bank. First, we introduced ISAN-HTTPS Enforcer from ISAN research lab to reinforce the HTTPS at the log-in webpage even users don't type HTTPS at the URL. Second, we integrate the HSTS (HTTPS Strict Transport Security) mechanism to protect and inform web browsers that connect to sites should always use TLS/SSL. If the hacker capable enough to bypassed these two steps, we also integrated the password encryption mechanism as the finally protection. It works to encrypted all password together with a CAPTCHA code at the log-in webpage of the internet banking as showed in Figure 4.15.

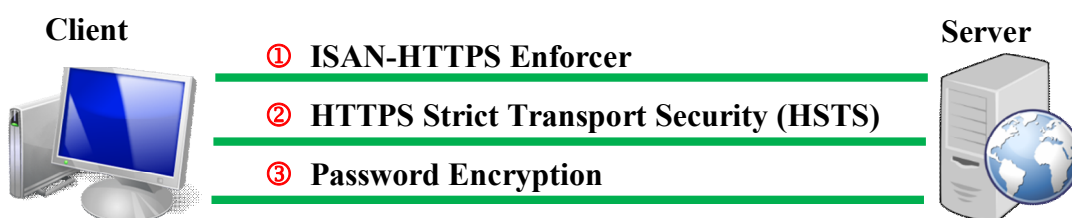


Figure 4.15 New Protection Design for Campu Bank

4.5.1 Implementation of ISAN-HTTPS Enforcer

From observation, we have found that most of the bank in our research and user's behavior do not recognize well on the internet banking log-in webpage. Mostly, it is happened on the client web browser side (Users type the internet banking log-in webpage wrong at the browser URL and search internet banking log-in webpage through search engine). So, we introduced this mechanism that was created in JavaScript and HTML program language to reinforce the HTTPS of the internet banking log-in webpage.

1) User requests to the internet banking log-in webpage by type it on URL with or without https:// at head of address bar (for example, https://www.test.com or test.com), it will stay as normal connection is HTTP to server

2) For the server side, server redirects http to https connections. After that, the server responds to the user. The connection between server and client uses HTTPS connection.



3) ISAN-HTTPS Enforcer works to check the list of URLs, if it is on the list of HTTPS connections. It will then redirect the connection to HTTPS as show in Figure 4.16.

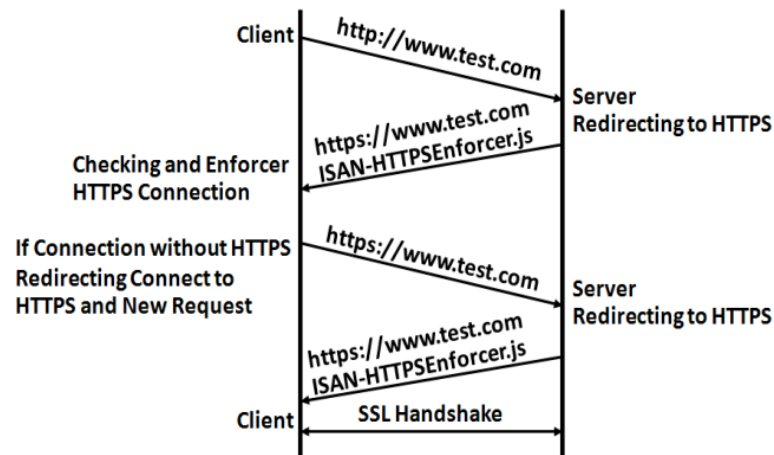


Figure 4.16 Process of ISAN-HTTPS Enforcer

Source: [4]

4.5.2 Implementation of HSTS

In this section, we integrate the HSTS as the second security mechanism for Campu bank log-in webpage by using PHP program language. From the observation result on the security side of the internet banking log-in webpage, we have found that Campu bank and also other banks still not supported HSTS yet. So, we integrate this HSTS mechanism to protect HTTPS at the header response of Campu internet banking log-in webpage as show in Figure 4.17. Moreover, we simulate the Campu internet banking log-in webpage for educational testing.

This HSTS supports with several web browsers, for example, Opera (version 12), Chrome (version 4.0.211.0), Firefox (version 4), Internet Explorer (version 11), and Safari as of OS X Mavericks.



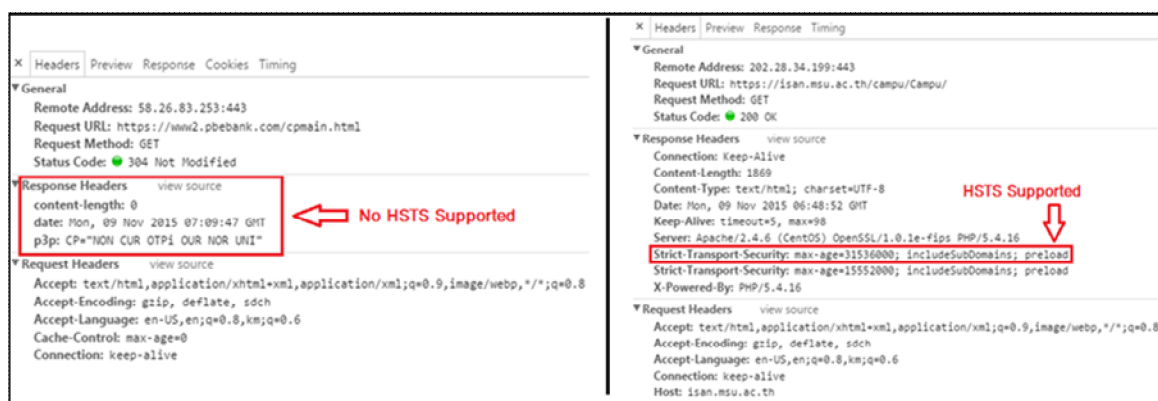


Figure 4.17 No HSTS Supported and HSTS Supported

It work as following source codes:

- 1) “*Strict-Transport-Security: max-age:1234; includeSubDomains; preload*”
- 2) “*max-age:1234*” is specified in seconds, mean that the period to remember to only connect to this host via HTTPS (for example, 31536000 is approximately one year)
- 3) “*includeSubDomains*” is the optional option to connect over HTTPS for sub-domains as show in Figure 4.18.

```
<?PHP
use_sts = true;
if ($use_sts && isset($_SERVER['HTTPS']) && $_SERVER['HTTPS'] != 'off') {
    header('Strict-Transport-Security: max-age=31536000; includeSubDomains; preload');
} elseif ($use_sts) {
    header('Location: https://'.$_SERVER['HTTP_HOST'].$_SERVER['REQUEST_URI'], true, 301);
    die();
}
?>
```

The code is annotated with three red circles and arrows: (1) points to the `use_sts` variable, (2) points to the `max-age=31536000` value, and (3) points to the `includeSubDomains` option.

Figure 4.18 Implementation of HSTS on Log-in Webpage

4.5.3 Implementation of Password Encryption

For this section, we integrate this password encryption for final security protection mechanisms for Campu bank log-in webpage. If the hacker bypasses the two



steps above, it is difficult for them to bypass this step. Password Encryption mechanism is worked as follows:

- 1) Develop the CAPTCHA code for Campu bank log-in webpage
- 2) Message Digest (MD) is the object function that collect password from client to hash in t times (t is set by developer) and then take the result of hashing plus with secure word (is set by admin or developer) and hash it again 1 times

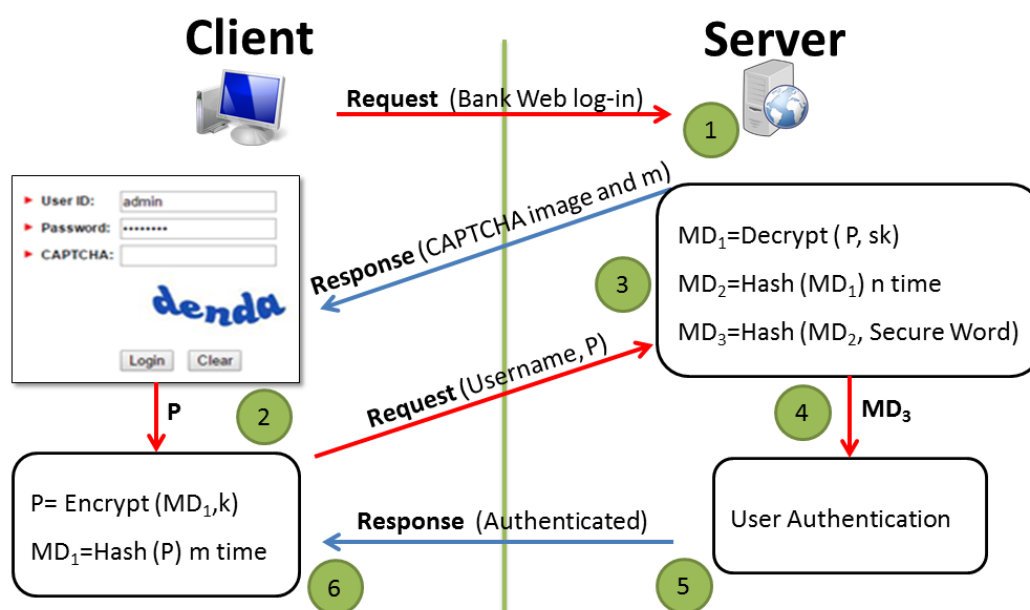


Figure 4.19 Structure of Password Encryption Mechanism

1) From the Figure 4.19, the client request to the server and then the server respond with 'CAPTCHA Image' and value of 'm' (m is random by program of developer that value of m is less than or equal to value of t)

2) Client defined value of P ($P = \text{Encrypt}(MD_1, k)$) by MD_1 is the value of hashing password in 'm' times, and k is the key come from CAPTCHA image filling of users

3) Client requests username and P to the server

4) Server defined value of MD_1 ($MD_1 = \text{Decrypt}(P, sk)$) by P and sk is the CAPTCHA key that store at the server side, and then defined the value of MD_2 by $MD_2 = \text{Hash}(MD_1)$ in 'n' times ($n = t - m$) and result of MD_2 plus with Secure word to hash again for the MD_3



- 5) Take MD₃ to authenticate with User Authentication
- 6) Send the authentication password access to the internet banking systems of users

Hence, this last protection mechanism can avoid all vulnerabilities or password sniffing at the client effectively. It was designed for Campu bank log-in web page as shown in Figure 4.20 and also the implementation of code as shown from Figure 4.21 to Figure 4.26.

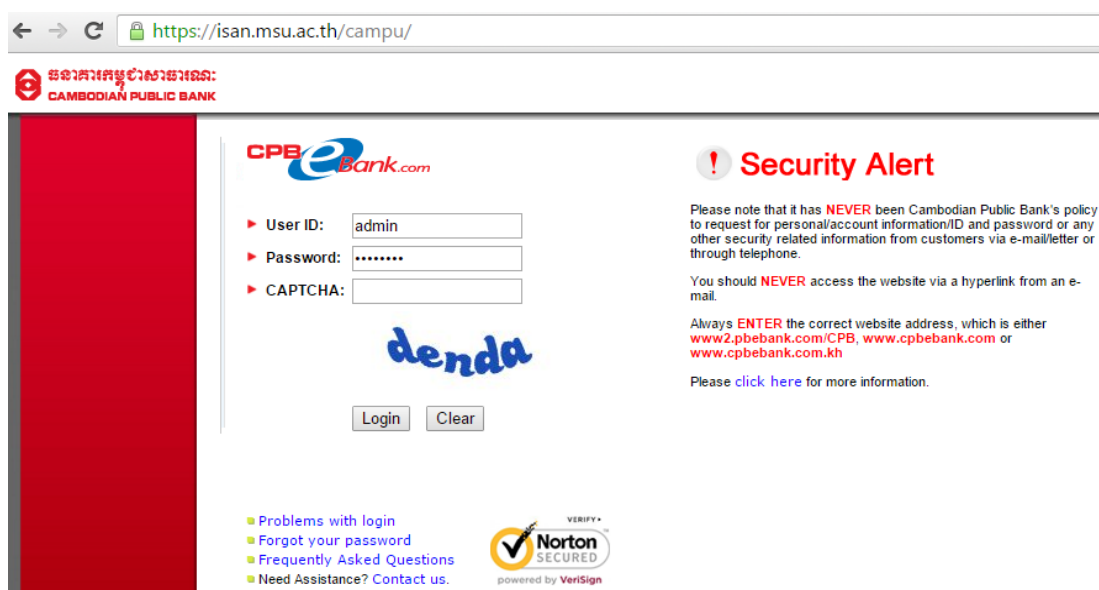


Figure 4.20 New Protection Design for Campu Bank

```

13 <script language="JavaScript">
14 function regist(){
15     var password = document.form1.password.value;
16     if(password!=""){
17
18
19         var data = PasswordProtectionFunctionAPI.PasswordProtectionRegister(password);
20
21         document.form1.pwdMD.value=data;
22
23         return true;
24     }else{
25         alert("Empty..!");
26         return false;
27     }
28 }
29
30 </script>

```

Figure 4.21 Function for register the password



```

9  if (!empty($_REQUEST['pwdMD'])) {
10
11      $obj = new PasswordProtectionFunctionAPI();
12      $pwdMD=$_POST['pwdMD'];
13      print "MD 10 Time form Client: ".$pwdMD;
14      $password = $obj->PasswordProtectionRegist($pwdMD);
15      print "<br>". "Password MD: ".$password."<br>";
16
17  }else{
18      print "Empty..!";
19  }

```

Figure 4.22 Password Hashing

<pre> 134 <? 135 \$m=rand(2, 10); 136 \$_SESSION['m'] = \$m; 137 ?> </pre>	<pre> 1 <?PHP 2 if(!isset(\$_SESSION)) 3 { 4 session_start() ; 5 } 6 ?> </pre>
--	--

Figure 4.23 Defined m Value and Start Session

```

12  <script src="AntiSniffAPI/PasswordProtectionFunctionAPI.js"></script> ①
13
14  <script language="JavaScript">
15  function encrypt(){
16      var username = document.form1.username.value;
17      var password = document.form1.password.value.trim(); ②
18      var key = document.form1.key.value;
19
20      if(username!="&&password!="&&key!=""){
21          var keyLength=256;
22          var m = document.form1.m.value;
23          var data = PasswordProtectionFunctionAPI.PasswordProtectionEncrypt(password, key, keyLength,m);
24          var result = data.split(" ");
25          var passwordEncrypt = result[0];
26          var CAPTCHAEncrypt = result[1];
27          document.form1.passwordEncrypt.value=passwordEncrypt;
28          document.form1.CAPTCHAEncrypt.value=CAPTCHAEncrypt;
29          document.form1.password.value = "";
30          document.form1.key.value = "";
31          document.form1.m.value = "";
32          return true;
33      }else{
34          alert("Empty..!");
35          return false;
36      }
37  }
38  }
39  </script>
40

```

Figure 4.24 User Log-in with CAPTCHA and m Value



```

10 // PasswordProtectionFunctionAPI Server
11 class PasswordProtectionFunctionAPI{
12
13     function PasswordProtectionDecrypt($passwordEncrypt,$CAPTCHAEncrypt,$t){
14         $img = new Securimage();
15         $cryptoHash = 'sha1' ;
16         $keyLength=256;
17         $SecureWord="isan@!#$1117Aa"; ← Secure Word
18         //===== Get key from CAPTCHA code in server
19         // $sk=$_SESSION['securimage_code_value'];
20         $sk="isan@!#$1117Aa";
21         //===== Decrypt CAPTCHA
22         $CAPTCHADecrypt = AESDecryptCtr($CAPTCHAEncrypt,$sk , $keyLength) ;
23         $CAPTCHAForCompare= sha1(sha1($sk));
24         //if($CAPTCHAForCompare==$CAPTCHADecrypt){
25         //===== Decrypt Password
26         $passwordDecrypt = AESDecryptCtr($passwordEncrypt, $sk, $keyLength) ;
27
28         //===== Compute n
29         $n=$t-$_SESSION['m']; ← Compute n= t - m
30         $passwordCompute=$passwordDecrypt;
31         //===== Compute message digest of password n times
32         for($i=0;$i<$n;$i++){
33             $passwordCompute=sha1($passwordCompute);
34         }
35         //===== Compute message digest of password and SecureWord
36         $password=sha1($passwordCompute.$SecureWord);
37         //===== Return message digest of the password and CAPTCHA

```

Figure 4.25 Process of Decryption Function at Server Side

```

12 if (!empty($_REQUEST['CAPTCHAEncrypt'])) {
13
14     print "Valid captcha."<br>";
15     print "Plain Text Password: ". "abcd1234."<br>";
16     $obj = new PasswordProtectionFunctionAPI();
17     $t = 10;
18     $passwordEncrypt=$_POST['passwordEncrypt'];
19     $CAPTCHAEncrypt=$_POST['CAPTCHAEncrypt'];
20     $password = $obj->PasswordProtectionDecrypt($passwordEncrypt,$CAPTCHAEncrypt,$t);
21     $database="b858e009b5594a36c7c3b3b06bfcae4f10b7f03e";
22     print "<br>";
23     print "<hr>";
24     print "Password in Database&nbsp;: ".$database."<br>";
25     print "<hr>";
26
27     if($password==$database){
28         print "<b>Verify Valid</b>";
29     }else{
30         print "<b>Verify Invalid</b>";
31     }
32 }
33
34 }else{
35     print "Empty CAPTCHA..!";
36 }
37
38 $request_captcha = htmlspecialchars($_REQUEST['captcha']);

```

Figure 4.26 Authentication Function



CHAPTER 5

CONCLUSION

This thesis set out to evaluate the safety and security issues on the internet banking systems of Campu bank. For safety issues, we have proposed an enhancement guideline to eliminate some impacts on the internet banking systems for Campu bank and for another bank between Cambodia and Thailand. For security issues, we have also proposed a new protection mechanism on the log-in webpage of Campu bank. This last chapter of this thesis addresses specifically on conclusions of observations, experiments, and appropriate recommendations.

5.1 Goals and Achievements in this research

So, the aims of this thesis were explored as follows:

- 1) To evaluate the safety issues on the internet banking systems based on observation and deployment results of Campu bank and compare with other banks between Cambodia and Thailand
- 2) To evaluate the security issues on the internet banking systems based on experiment results and propose solutions for Campu bank to enhance bank websites

5.1.1 Observation and Deployment

From the observation results, we can conclude that all banks in our research are strictly control on authentication documents to open bank account for foreigner. Bank requires a lot of authentication documents from them like passport plus with valid visa, work permit and local residential address. Especially, the authentication documents for registering the internet banking systems, for example some documents issued by government or related organization, with or without photo should be recognized clearly before authorized.

Moreover, among 80 Cambodian university students in Cambodia are not familiar and don't know about the internet banking services. Comparing to Thailand, Thai 80 students in Mahasarakham University have internet banking on their hands. As mentioned section 2.4.2, the barrier of user's perception is important for the internet



banking service in developing countries. For Cambodia, we suggest for all banks to implement the internet banking registration through ATM and online. It makes a lot of users secure and save time on queue and reduce some workloads at counter. For Thailand, the internet banking call center should add some secure questions to authenticate with their users. This kind of questions should be set at the beginning of internet banking registration.

Finally, we suggest all banks in Cambodia and Thailand to deploy the token devices for normal customers (even with some charges) and CAPTCHA on the log-in webpage of the bank to avoid malware or attacks. Moreover, on-screen keyboard should be used at the internet banking log-in webpage. It can protect their users from keyboard capture software. Alerting message through SMS must be used for the internet banking transaction. It can help users in some reasons (even its charge) of attacks. For all users, individual information should keep in secret. They also take control on the mobile phone very well when it lost signal, immediately call or contact to mobile operators in order to avoid some attacks.

5.1.2 Experiments and New Design

From the experiment results, we can conclude that all banks in this research relies on digital certificates, https and extended validation certificates to secure data on the way to communication with users. Yet, most of them do not support HSTS that is a new mechanism enable bank websites accessible via secure connections. Furthermore, most of the banks in this research have affected to SSL Stripping Attack. It allows hackers to capture username and password of users easily.

So, this thesis has proposed a new protection mechanism for Campu bank. We strongly tested on our testbed website based on client side of the internet banking systems. Moreover, we have also proposed a new protection mechanism for Campu bank by using ISAN lab server to implement this mechanism as shown in section 4.4 of Chapter 4.

Finally, we have also discussed with well-versed staff from Campu bank to let them give their opinions on this protection mechanism. They have felt that this mechanism would be able to protect their customers and bank websites as shown in Table 5.1.



Table 5.1 Results of New Protection Mechanism

New Three Layer Protection Mechanism	
SSL Stripping Attack	Protected
Password Vulnerability	Protected
Sniffing and HTTPS Modification	Protected

5.2 Summary and Recommendations

Based on the findings of this thesis to observe and test on the internet banking systems between Cambodia and Thailand, our recommendations are offered as possible ways to improve users and banks as followings:

1) For users, all individual information should keep in secret especially on the socialization of social network. Moreover, bank's users or internet banking's users have to apply the alerting system that banks deployment and all times checking while log-in into internet banking websites.

2) For banks, all banks should deploy authentication device beside SMS OTP and password. They should also provide a training on how to safely use the internet banking service for their customers and staffs. Moreover, we suggest all banks to cooperate with government or related ministry to integrate a verification system of citizen identity card.

Finally, it would be important to conduct a study more on the mobile banking. Apart from the internet banking, more and more banks now deploy mobile banking services to ease and facilitate their customers. Mobile banking systems have been claimed as more secure comparing to the internet banking. So, it would be good to examine on the mobile banking issues for the future work.



REFERENCES



REFERENCES

- [1] Cooper D, Santesson S, Farrell S, Boeyen S, Housley R, Polk W. "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". IETF, RFC 5280, May 2008.
- [2] Dierks T, Rescorla E. "The Transport Layer Security (TLS) Protocol Version 1.2". IETF, RFC 5246, August 2008.
- [3] Marlinspike M. "SSL Sniff Attack". [Online]. 2012. [cited 2015]; Available from: <http://www.thoughtcrime.org/software/sslsniff/>.
- [4] Puangpronpitag S, Sriwiboon N. "Simple and Lightweight HTTPS Enforcement to Protect Against SSL Stripping Attack". Proceedings of 4th International Conference on Computational Intelligence, Communication Systems and Networks; 24-27 June 2012; Phuket, Thailand. pp. 229-234.
- [5] Philipp C.H. "Use SSL Split to Transparently Sniff TLS/SSL Connections". [Online]. 04 August 2013 [cited 2015]; Available from: <http://blog.philippheckel.com/2013/08/04/use-sslsplit-to-transparently-sniff-tls-ssl-connections/>.
- [6] Codenomicon. "The Heartbleed Bug". [Online]. April 2014 [cited June 2015]; Available from: www.heartbleed.com.
- [7] Moller B, Duong T, Kotowicz K. Google Security Advisory. "This POODLE Bites: Exploiting The SSL 3.0 Fallback". [Online]. September 2014 [cited January 2018]; Available from: <https://www.openssl.org/~bodo/ssl-poodle.pdf>.
- [8] Subsorn P, Limwiriyaikul 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) 2011; 23 March 2011; Nakhon Pathom, Thailand. pp. 260-272.
- [9] Subsorn P, Limwiriyaikul S. "An Analysis of Internet Banking Security of Foreign Subsidiary Banks in Australia: A Customer Perspective". Proceedings of the International Journal of Computer Sciences Issues (IJCSI) 2012; March 2012; Perth, Western Australia. pp. 8-16.
- [10] Campu Bank Groups. "Cambodian Public Bank Plc.". [Online]. 2014 [cited 2007]; Available from: <http://www.cpbebank.com/cpeb/index.html>.
- [11] Wikipedia. "Internet Banking Systems". [Online]. 10 December 2014 [cited 5 March 2015]; Available from: http://en.wikipedia.org/wiki/Online_banking.
- [12] Schmeih K. "Cryptography and Public Key Infrastructure on the Internet". The Atrium, Southern Gate, Chichester: John Wiley & Sons Ltd.; 2003.



- [13] Stallings W. "Cryptography and Network Security, Principles and Practice". 4th Edition. Prentice Hall: Pearson Education Inc.; 2011.
- [14] "Merriam-webster's Collegiate Dictionary". Online. America: Meriam-Webster, Inc.; 1847-2015.
- [15] Puangpronpitag S. "Introduction to Safety/Security and Classical Cryptology". n.p.: n.p.; n.d.
- [16] "The Orkida Dictionary of English-Cambodian Language". Virey An; 1998.
- [17] The Hacker News. "Hackers Stole \$300 Million from 100 Banks using malware". [Online]. 2015. [cited 15 February 2015]; Available from: <http://thehackernews.com>.
- [18] ไอที 24 ชั่วโมง เปิดโลกไอที พลิกสู่ชีวิตที่ดีกว่า. "เตือนภัย Internet Banking รูปแบบใหม่!! ปลอมเป็นคุณ ด้วยหลักฐานปลอม สวมรอยโอนเงินออก สูญหลายแสน!". [ข่าวไอทีออนไลน์]. 04 สิงหาคม 2013 [สืบค้นเมื่อ 15 ธันวาคม 2515]; ได้จาก: <http://www.it24hrs.com/2013/hack-otp-banking-change-new-sim-card/>.
- [19] ไอที 24 ชั่วโมง เปิดโลกไอที พลิกสู่ชีวิตที่ดีกว่า. "อีกแล้ว! คนร้ายสวมรอยเป็นเจ้าของบัญชี Internet Banking โอนเงินออก สูญหลายแสน!". [ข่าวไอทีออนไลน์]. 06 กุมภาพันธ์ 2014 [สืบค้นเมื่อ 8 พฤศจิกายน 2015]; ได้จาก: <http://www.it24hrs.com/2014/hack-otp-banking-change-new-sim-card-2/>.
- [20] ไอที 24 ชั่วโมง เปิดโลกไอที พลิกสู่ชีวิตที่ดีกว่า. "อีกแล้ว!! เตือนภัย ลูกค้ายธนาคาร แม้ไม่ได้เปิด e-Banking ก็โดนขโมยเงินได้! [ข่าวไอทีออนไลน์]. 16 สิงหาคม 2013 [สืบค้นเมื่อ 16 ตุลาคม 2015]; ได้จาก: <http://www.it24hrs.com/2013/stealing-money-criminal-subrogate-bank/>.
- [21] ไอที 24 ชั่วโมง เปิดโลกไอที พลิกสู่ชีวิตที่ดีกว่า. "เตือนภัยผู้ใช้ ATM หลังโจรแฮค ATM ขโมยเงินไปรัสเซียและยูเครน. [ข่าวไอทีออนไลน์]. 08 พฤศจิกายน 2013 [สืบค้นเมื่อ 5 ธันวาคม 2015]; ได้จาก: <http://www.it24hrs.com/2013/hack-atm-skimming/>.
- [22] ไอที 24 ชั่วโมง เปิดโลกไอที พลิกสู่ชีวิตที่ดีกว่า. "เตือนผู้ใช้บริการ ATM และ E-Banking!! เช็คยอดเงินบัญชีธนาคาร หลังเงินหายหลายแสน!!! [ข่าวไอทีออนไลน์]. 04 เมษายน 2013 [สืบค้นเมื่อ 5 ธันวาคม 2015]; ได้จาก: <http://www.it24hrs.com/2013/hack-and-lost-money-in-bank-account-online-atm/>.



- [23] ไอที 24 ชั่วโมง เปิดโลกไอที พลิกสู่ชีวิตที่ดีกว่า. "เตือนภัย! พบตู้ ATM ติดเครื่อง SKIMMER อีกแล้ว เนียนกว่าเดิม!". [ข่าวไอทีออนไลน์]. 22 กันยายน 2014 [สืบค้นเมื่อ 20 ตุลาคม 2015]; ได้จาก: <http://www.it24hrs.com/2014/atm-skimming-warning/>.
- [24] Pantip. "TMB direct ห่วยไปไหม?". [Online]. 2013 [cited 01 October 2015]; Available from: <http://pantip.com/topic/32644251>.
- [25] ANZ RG. "Email Scams and Fake Websites". [Online]. 2013 [cited 2014]; Available from: <http://anzroyal.com/en/Personal/Ways-Bank/Internet-Banking/protect-banking/types-fraud/>.
- [26] "ACIS Research LAB – Information Security Research on Thailand's Internet Banking/Mobile Banking". [Online]. 20 September 2014 [cited 2 November 2015]; Available from: <https://www.acisonline.net/?p=908>.
- [27] Subsorn P, Limwiriyaikul S. "A Comparative Analysis of the Security of Internet Banking in Australia: A Customer Perspective". Proceedings of the 2nd International Cyber Resilience Conference (ICR) 2011; 1-2 August 2011; Perth, Western Australia. pp. 70-83.
- [28] Subsorn P, Limwiriyaikul 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 2012; 24-26 July 2012; Phuket, Thailand. pp. 189-195.
- [29] Puangpronpitag S, Putla P. "An Analysis of Safety and Security for Internet Banking in Thailand". Proceedings of National Conference on Computing and Information Technology (NCCIT) 2015; 2-3 July 2015; Bangkok, Thailand. pp. 99-105.
- [30] 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) 2009; 9-12 November 2009; London, UK. pp. 1-6.
- [31] 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) 2012; 3-4 December 2012; Kota Kinabalu, Sabah, Malaysia. pp. 159-163.
- [32] 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.



- [33] 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 the International Conference on Computing and Informatics (ICOI) 2006; 6-8 June 2006; Kuala Lumpur, Malaysia. pp. 1-6.
- [34] Han-Na Y, Jae-Sik L, Jung-Jae K, Moon-Seog J. "A Study on the Two-Channel Authentication Method which provides Two-Way Authentication in the Internet Banking Environment". Proceedings of 5th International Conference on Computer Science and Convergence Information Technology (ICCIT) 2010; 30 November-02 December 2010; Seoul, Korea. pp. 539-543.
- [35] Guoling L, Xinwang W. "Study of Security Mechanisms in Personal Internet Banking - Take China Merchants Bank as an example". Proceedings of the International Conference on Computational Intelligence and Software Engineering (CiSE) 2010; 10-12 December 2010; Wuhan, China. pp. 1-4.
- [36] Hanacek P, Malinka K, Schafer J. "E-Banking Security - A Comparative Study". Proceedings of the International Conference on Aerospace and Electronic Systems Magazine, IEEE; January 2010; pp. 29-34.
- [37] Puangpronpitag S, Tooltham A. "The Evaluation of the SSL Stripping Attack Problem". Proceedings of the National Conference on Computer Information Technologies; January 2013; Sakon Nakhon, Thailand. pp. 43-48.
- [38] "Wireshark". [computer program]. Version 1.12.2. Wireshark Team; 12 November 2014.
- [39] Zakir D, James K, Michael B, Alex HJ. "Analysis of the HTTPS Certificate Ecosystem". Proceedings of International Conference on Internet Measurement Conference (IMC) 2013; 23-25 October 2013; Barcelona, Spain. pp. 291-304.
- [40] Google Inc., Microsoft. "Gradually Sunseting SHA-1". [Online]. 2014 [cited 05 September 2014]; Available from: <http://blog.chromium.org/2014/09/gradually-sunseting-sha-1.html>.
- [41] วรวรรต พงษ์ศิริ, ณราชัย กิตติสิริโธ. "สำรวจความปลอดภัยของ SSL ของธนาคารออนไลน์ในประเทศไทย". [Online]. 29 November 2014 [cited July 2015]; Available from: <https://www.blognone.com/node/63319>.
- [42] "National Bank of Cambodia". [Online]. 2011 [cited 2015]; Available from: <http://www.nbc.org.kh>.
- [43] "Bank of Thailand". [Online]. 2008 [cited 2015]; Available from: <http://www.bot.or.th>.



- [44] Wikipedia. "Standard ISO/IEC 27002:2005". [Online]. 01 July 2007 [cited 16 July 2015]; Available from: http://en.wikipedia.org/wiki/ISO/IEC_27001:2005.
- [45] Phukseng T, Boonkrong S. "A Survey of Internet Banking Security of Thailand's Commercial Banks: Personal Customer Perspective". *Journal of Science and Technology (Scholar Article)* 2558; 23[1]: 141-152.
- [46] OmniSecu.com. "Public Key Infrastructure". [Online]. 2008-2014 [cited 2015]; Available from: <https://www.omniseclu.com/security/public-key-infrastructure>.
- [47] Eldefrawy MH, Alghathbar K, Khan MK. "OTP-Based Two-Factor Authentication Using Mobile Phones". *Proceedings of 2011 8th International Conference on Information Technology: New Generations*; 11-13 April 2011; Las Vegas, USA. pp. 327-331.
- [48] Shangfu G, Jun L, Yizhen S. "Design and Implementation of Anti-Screenshot Virtual Keyboard Applied in Online Banking". *Proceedings of 2010 International Conference on E-Business and E-Government*; 7-9 May 2010; Guangzhou, China. pp. 1320-1322.
- [49] "Kali Linux". [computer program]. Version 1.0.9a. Offensive Security Team; 06 October 2014.
- [50] "Cain and Abel". [computer program]. Version 4.9.56. 07 April 2014.
- [51] Ristic I. Qualys Inc. "SSL Server Rating Guide". [online]. 08 December 2014 [cited 6 November 2015]; Available from: <https://www.ssllabs.com/projects/rating-guide/index.html>.
- [52] Seggelmann R, Tuexen M, Williams M. "Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension". *IETF, RFC 6520*, February 2012.
- [53] Wikipedia. "Mobile Network Operators of Asia Pacific Region". [Online]. 02 May 2014 [cited 6 November 2015]; Available from: https://en.wikipedia.org/wiki/List_of_mobile_network_operators_of_the_Asia_Pacific_region.
- [54] Hodges J, Jackson C, Barth A. "HTTP Strict Transport Security (HSTS)". *IETF, RFC 6797*, November 2012.



APPENDICES



APPENDIX A
OBSERVATION CRITERIA



Safety and Security Observation Criteria

Observation Criteria	A	B	C	D	E	F
1. Open Bank Account and Internet Banking Registration						
1.1 Authentication Requirements						
For Open Bank Account						
1.1.1 Valid Identity Card (Copy or Original)	O	O	O	A + ①	A + ①	A + ①
1.1.2 Valid Passport	✓ + ②/①	✓ + ②/①	✓ + ②/①	✓ + ②/①	✓ + ②/①	✓ + ②/①
1.1.3 ① Evidence of a local residential address						
1.1.4 ② Other documents issued by government authorities						
For Internet Banking Services						
1.1.5 Identity Card or Passport (Copy or Original)	A + ②/①	A + ②/①	A + ②/①	A + ②/①	A + ②/①	A + ②/①
1.1.6 Driving License	✓ + ②/①	✓ + ②/①	✓ + ②/①	✓ + ②/①	✓ + ②/①	✓ + ②/①
1.1.7 Passbook	✓	✓	✓	✓	✓	✓
1.1.8 ATM Card Number	x	x	x	✓	✓	x
1.1.9 PIN Number	x	x	x	✓	✓	✓
1.1.10 Phone Number	✓	✓	✓	✓	✓	✓
1.1.11 Memorable Question + Answer	✓	x	✓	x	✓	x
1.2 Apply for Internet Banking						
1.2.1 Through Branches	✓	✓	✓	✓	✓	✓
1.2.2 Through ATM	x	x	x	✓	✓	✓
1.2.3 Through Call Center	x	x	x	x	x	x
1.2.1 Through Online/ Mobile Application	x	x	x	✓	✓	✓
1.3 Additional Cases						
1.3.1 Open Bank Account By 3 rd Party	x	x	x	x	x	x

Observation Criteria	A	B	C	D	E	F
1.3.2 Duplicate of Internet Banking Registration With Different Branch or ATM	✗	✓	✓	✓	✓	✓
1.3.3 Automatic Add All Account (Other, credit and so on)	✗	✓	✗	✗	✗	✓
1.3.4 Manual Add Account	✓	✓	✓	✓	✓	✓
2. Username and Password						
2.1 First Time Registration						
2.1.1 Provision of Temporary Username (U) and Password (P)	✓	✓	✓	✓	✓	✗
2.1.1.1 Through Email	✗	U + P	P	✗	✗	✗
2.1.1.2 Through SMS	✗	✗	✗	U	✗	Ac
2.1.1.3 Through Bank Slip	U + P	✗	✗	✗	U+P	✗
2.1.1.4 Through ATM Slip	✗	✗	✗	U	U	✗
2.1.1.5 Through Post	✗	✗	✗	Pi	✗	✗
2.1.1.6 Expiration	30 days	2 days	7 days	3 days	2 days	3 hours
2.1.2 PIN Number	✗	✗	✗	✓	✓	✗
2.1.3 Auto Generate Username and Password By Bank	✓	✓	✓	✓	✓	✓
2.1.4 Fixed Username – Set By Bank (Cannot Changed)	✗	✓	✗	✗	✗	✗
2.2 Username Limitation						
2.2.1 Length of Characters	6-12	Fixed	Any	6-32	6-12	8-20
2.2.2 Contain with Characters (Minimum)	1	Fixed	Any	1	1	1
2.2.2.1 Contain with Special Characters	✗	Fixed	Any	✗	✗	“.”, “_”
2.2.2.2 Contain with Uppercase, Lowercase and Normal	✓	Fixed	Any	✗	✗	✓
2.2.3 Contain with Number (Minimum)	1	Fixed	Any	1	1	1
2.2.4 Others	1+2= Char	✗	✗	✗	✗	NRC 3
2.3 Password Limitation						
2.3.1 Length of Characters	8-12	6-16	10-17	8-32	6-8	8-20

Observation Criteria	A	B	C	D	E	F
2.3.2 Contain with Characters (Minimum)	1	1	1	1	1	1
2.3.2.1 Contain with Special Characters	✗	✓	(@, #, \$)	✓	✓	✓
2.3.2.2 Contain with Uppercase, Lowercase and Normal	✓	✓	✓	✓	✓	✓
2.3.3 Contain with Number (Minimum)	1	1	1	1	1	1
2.3.4 Others	✓	✓	✓	✓	‘ “ , & sp	NRC 2
2.3.5 Force to Change Password within period	90 days	30 days	✗	✗	✗	✗
2.4 Username Recovery						
2.4.1 Username Blocked (Failure Log-in)	3 times	3 times	3 times	3 times	3 times	3 times
2.4.2 Through Call Center (Call Center Authentication)	✗	✗	✗	✓	✓	✓
2.4.3 Through Online (Two-factor authentication)	✗	✗	✓	✗	✗	✗
2.4.4 Through ATM	✗	✗	✗	✓	✓	✓
2.4.5 Through Branch (Requirement)	✓	✓	✓	✓	✓	✓
2.4.5.1 Identity Card or Passport	✓	✓	✓	✓	✓	✓
2.4.5.2 Passbook or ATM Card	✓	✓	✓	✓	✓	✓
2.4 Password Recovery						
2.4.1 Through Call Center (Call Center Authentication)	✓	✗	✓	✓	✓	✓
2.4.2 Through Online (Two-factor authentication)	✗	✓	✓	✓	✓	✗
2.4.3 Through ATM	✗	✗	✗	✓	✗	✓
2.4.4 Through Branch (Requirement)	✓	✓	✓	✓	✓	✓
2.4.4.1 Identity Card or Passport	✓	✓	✓	✓	✓	✓
2.4.4.2 Passbook	✓	✓	✓	✓	✓	✓
3. Call Center Authentication						
3.1 User Confidential Information						
3.1.1 Account Number	✓	✓	✓	✓	✓	✓
3.1.2 Username or Account Name or Nickname	✓	✓	✓	✓	✓	✓



Observation Criteria	A	B	C	D	E	F
3.1.3 Birthdate or Day of Birth	✓	✓	✓	✓	✓	✓
3.1.4 Email Address	✓	✓	✓	✓	✓	✓
3.1.5 Phone Number	✓	✓	✓	✓	✓	✓
3.1.7 Identity Card Number or Passport Number	✓	✓	✓	✓	✓	✓
3.1.8 ATM Expiration Date	✓	✓	✓	✓	✓	✓
3.1.9 Branch of Open Bank Account	✓	✓	✓	✓	✓	✓
3.1.10 Current Address	✓	✓	✓	✓	✓	✓
3.1.11 Last Transaction and Activity	✓	✓	✓	✓	✓	✓
3.1.12 ATM Pin Number	✓	✓	✓	✓	✓	✓
3.2 Memorable Question and Answer	✓	✗	✓	✗	✗	✗
3.2.1 Automatic Question	✓	✗	✓	✗	✗	✗
3.2.2 Manual Answer	✓	✗	✓	✗	✗	✗
4. Two-factor Authentication						
4.1 One Time Password (OTP)						
4.1.1 Type of OTP (SMS/ Email/ Mobile/ Token)	PAC	S/T	M/T	S/T	S/T	S/T
4.1.2 OTP Length	6-digit	6-digit	6-digit	8-digit	6-digit	6-digit
4.1.3 First Time Registration	✗	✗	✗	✓	✓	✓
4.1.4 Log-in Webpage	✗	✗	✓	✗	✗	✗
4.1.5 Allow to Activate or Block	✗	✗	✗	✓	✗	✗
4.1.6 Cost	Free	Free	\$10-\$15	Free	Free	Free
4.1.7 Expiration	10 mins	5 mins	1 min	5 mins	5 mins	5 mins
4.1.8 Transactions	✓	✓	✓	✓	✓	✓
4.1.8.1 Transfers to 3 rd Party Within Bank Account	✓	✓	✓	✓	✓	✓
4.1.8.2 Transfers to 3 rd Party At Others Bank Account	✓	✓	✓	✓	✓	✓
4.1.8.3 Bill Payment	✓	✓	✓	✓	✓	✓
4.1.8.4 Top-Up	✗	✗	✓	✓	✓	✓

Observation Criteria	A	B	C	D	E	F
4.1.8.5 Add New Account	✓	✗	✓	✓	✓	✓
4.1.6.6 Others Payments (Credit Card, Debit Card and so on)	✓	✗	✓	✓	✓	✓
4.1.9 Change Settings	✓	✓	✓	✓	✓	✓
4.1.9.1 Username	✓	✗	✗	✗	✓	✓
4.1.9.2 Password	✓	✓	✓	✗	✓	✓
4.1.9.3 Phone Number	✓	✗	✗	✗	✗	✓
4.1.9.4 Daily Transaction Limitation	✓	✓	✓	✓	✓	✓
4.1.9.5 Update Personal Details	✓	✓	✗	✗	✗	✓
4.2 CAPTCHA						
4.2.1 Log-in Webpage	✗	✗	✗	✗	✗	✓
4.2.1.1 Auto Pop-up	✗	✗	✗	✗	✗	✗
4.2.1.2 Failure Pop-up	✗	✗	✗	✗	✗	✓
4.2.2 Transactions	✗	✗	✗	✗	✗	✗
4.2.3 Change Settings	✗	✗	✗	✗	✗	✗
4.2.4 Frist Time Registration	✗	✗	✗	✓	✗	✗
4.3 Secure Code (Log-in Webpage)	✗	✓	✗	✗	✗	✗
4.4 Activation Code	✗	✗	✗	✗	✗	3 hours
5. Transaction Limitation						
5.1 Transfer (Maximum Amount Per Day)						
5.1.1 To Own Account	\$10,000	\$10,000	U.L	฿500,000	฿500,000	฿700,000
5.1.2 To 3 rd Party Account	\$1,000	\$1,000	U.L	฿500,000	฿300,000	฿700,000
5.2 Payment (Maximum Amount Per Day)	\$1,000	\$1,000	U.L	฿100,000	฿500,000	฿700,000
5.3 Top-up (Maximum Amount Per Day)	\$1,000	\$1,000	U.L	฿100,000	฿500,000	฿700,000
5.4 Maximum Add Account	5	5	5	5	20	5



Observation Criteria	A	B	C	D	E	F
6. Alerting System						
6.1 Account and Transaction Activity						
6.1.1 Log-in	✗	✗	✗	✓	✓	✓
6.1.2 Log-out	✗	✗	✓	✓	✓	✓
6.1.3 Transactions (Transfer, Payment, Top-up and History)	✓	✓	✓	✓	✓	✓
6.1.4 Money-In and Out	✓	✓	✓	✓	✓	✓
6.1.5 Change Settings (Username, Password, and so on)	✗	✓	✓	✓	✓	✓
6.2 Type of Alert and Cost						
6.2.1 Through Email	✓	✓	✗	✓	✓	✓
6.2.2 Through SMS + Cost	1\$/M	1\$/M	Free	Free	฿20/M	฿10/M
6.2.3 Through Web Browser	✗	✗	✓	✓	✓	✓
6.3 Session Time-out	15 mins	15 mins	15 mins	15 mins	15 mins	16 mins
7. Others Mechanism						
7.1 Virtual Keyboard or Scramble Keyboard						
7.1.1 Username	✗	✗	✗	✗	✗	✗
7.1.2 Password	✗	✓	✗	✗	✗	✗
7.1.3 One Time Password	✗	✗	✗	✗	✓	✗
7.1.4 Amount Money	✗	✗	✗	✗	✗	✗
7.1.5 Invisible	✗	✗	✗	✓	✓	✗
7.1.6 Others (PIN or Card Number)	✗	✗	✗	✓	✓	✗
7.2 Re-new or Pause the Internet Banking						
7.2.1 Through Call Center	✗	✗	✗	✗	✗	✗
7.2.2 Through Branch	✓	✓	✓	✓	✓	✓
7.2.3 Through Online	✗	✗	✗	✗	✗	✗

Observation Criteria	A	B	C	D	E	F
7.3 Browser Supported and Others Browser Settings						
7.3.1 Chrome	✓	✓	39/43	14	✓	20
7.3.2 Firefox	✓	3.1	34	6	✓	4
7.3.3 Internet Explorer	5.5	7	8-11	8	✓	8
7.3.4 Safari	✓	3.5	8.0	5	✓	5
7.3.5 Opera	✓	9.5	x	✓	✓	✓
7.3.6 Others	✓	✓	✓	✓	✓	✓
7.4 Help Center						
7.2.1 Email, Call Center and Frequently Ask Questions (FAQ)	✓	✓	✓	✓	✓	✓
7.2.2 Video Call	x	x	x	x	x	x
7.2.3 Remote Desktop (like co-browsing)	x	x	x	x	✓	x
7.2.4 Online application + Web chat	x	x	x	x	✓	✓
8. Close Bank Account and Internet Banking						
8.1 Authentication Requirements						
8.1.1 Valid Identity Card or Passport	✓	✓	✓	✓	✓	✓
8.1.2 Passbook	✓	✓	✓	✓	✓	✓
8.1.3 Other Valid Documents	✓	✓	✓	✓	✓	✓
8.2 Close Internet Banking						
8.2.1 Through Call Center	x	x	x	x	x	x
8.2.2 Through Branch	✓	✓	✓	✓	✓	✓
8.2.3 Through ATM	x	x	x	x	x	x
8.2.4 Through Online	x	x	x	x	✓	x
9. Mobile Center						
9.1 Requirement for request new sim-card (Head Office)						
9.1.1 Identity Card (Copy or Original)	A	A	A	A	A	A

Observation Criteria	A	B	C	D	E	F
9.1.2 Passport (Copy or Original)	A	A	A	A	A	A
9.1.3 Driving License	/	/	/	/	/	/
9.1.4 Other related documents	+	+	+	+	+	+
9.1.5 Old Phone Number	✓	✓	✓	✓	✓	✓
9.2 Requirement for request new sim-card (Small Office)						
9.2.1 Identity Card (Copy or Original)	A	A	A	A	A	A
9.2.2 Passport (Copy or Original)	A	A	A	A	A	A
9.2.3 Other related documents	+	+	+	+	+	+
9.2.4 Old Phone Number	✓	✓	✓	✓	✓	✓
10. Bank Authentication						
10.1 Digital Certificate						
10.1.1 Version	3	3	3	3	3	3
10.1.2 Signature Algorithm	SHA2	SHA2	SHA2	SHA1	SHA1	SHA2
10.1.3 Public Key	2048bits	2048bits	2048bits	2048bits	2048bits	2048bits
10.1.4 Valid From	03/2015	12/2014	03/2015	05/2015	09/2014	05/2015
10.1.5 Valid Until	05/2017	12/2016	03/2017	06/2016	10/2015	10/2016
10.1.6 Common Names with WWW	✓	✓	✓	x	✓	✓
10.1.7 Issuer	SG3	SG3	SG3	SG2	EL1E	EL1M
10.2 Supported Protocols						
10.2.1 TLS 1.2	✓	✓	✓	✓	✓	✓
10.2.2 TLS 1.1	✓	✓	✓	✓	✓	✓
10.2.3 TLS 1.0	✓	✓	✓	✓	✓	✓

Observation Criteria	A	B	C	D	E	F
10.2.4 SSL 3	✗	✗	✓	✗	✓	✗
10.2.5 SSL 2	✗	✗	✗	✗	✗	✗
10.3 SSL Report						
10.3.1 Overall Rating	A-	F	C	A-	C	A-
10.3.2 HSTS	✗	✗	✗	✗	✗	✗
10.3.3 Extended Validation Certificate	✓	✓	✓	✗	✓	✓
10.3.4 HTTPS Supported	✓	✓	✓	✓	✓	✓
10.3.5 Key Exchanged	RSA	RSA	RSA	RSA	RSA	RSA
10.4 Experiment Capture						
10.4.1 SSL Sniff	S	S	S	S	S	S
10.4.2 SSL Strip	V	V	U	V	U + P	U + P
10.4.3 Heartbleed	S	S	S	S	S	S
10.4.4 Poodle	S	V	V	S	V	S

***Note:

+: Plus; ✓: Yes; ✗: No; /:Optional; S: Secure; V: Vulnerable; U:Username; P: Password;
 UL: Unlimited; Sm: SMS; E: Email; M: Mobile or Soft; SHA1: SHA 128; SHA2: SHA 256;
 T: Token; V: Vulnerable; NRC: No Repeat Character; PAC: Personal Authentication Code;
 M: Month; O: Original; C: Copy; A: All (Copy + Original); mins: Minutes;
 EL1E: Entrust Certification Authority – L1E; EL1M: Entrust Certification Authority – L1M
 SG2: Symantec Class 3 EV SSL CA – G2; SG3: Symantec Class 3 EV SSL CA – G3
 1+2= Char: First and Second Characters must be alphabetical;

APPENDIX B

PREVIOUS WORKS COMPARISON DETAIL



Previous Works	Safety and Security Observation		Drawback		
	Safety	Security	Crime Cases	Standard	Experiment
“A Comparative Analysis of Internet Banking Security in Thailand: A Customer Perspective”, Subsorn P. and Limwiriyakul S.	✓		✗	✗	✗
“A case study of Internet Banking Security of Mainland Chinese Banks: A customer perspective”, Subsorn P. and Limwiriyakul S.	✓		✗	✗	✗
“A comparative analysis of the security of internet banking in Australia: A customer perspective”, Subsorn P. and Limwiriyakul S.	✓		✗	✗	✗
“An Analysis of internet banking security of Foreign Subsidiary banks in Australia: A customer perspective”, Subsorn P. and Limwiriyakul S.	✓		✗	✗	✗
“The impact of internet banking service on customer satisfaction in Thailand: A case study in Bangkok”, Rangsan N. and Titida N.	✓		✗	✗	✗
“Customer Satisfaction Towards Internet Banking Services: Case analysis on Malaysian Bank”, Loke. et al	✓		✗	✗	✗
“Towards Secure Information Systems in Online Banking”, Karim. et al		✓	✗	✗	✗
“An Analysis of Safety and Security for Internet Banking in Thailand”, Putla. et al		✓	✓	✓	✓

Previous Works	Safety and Security Observation		Drawback		
	Safety	Security	Crime Cases	Standard	Experiment
“Problems of Electronic Commerce Applications in a Developing country: A Descriptive case study of the banking Industry of Oman”, Al-Gharbi. et al.	✓		✗	✗	✗
“Simple and Lightweight HTTPS Enforcement to Protect Against SSL Stripping Attack”, Puangpronpitag S. and Sriwiboon N.		✓	✗	✗	✓
“The Evaluation of the SSL Stripping Attack Problem”, Puangpronpitag S. and Tooltham A.		✓	✗	✗	✓
“Analysis of the HTTPS Certificate Ecosystem”, Zakir Durumeric et al.		✓	✗	✗	✓
“E-banking Security – A Comparative Study”, Hanacek P. et al.		✓	✗	✗	✓
“A study on the two-channel authentication method which provides two-way authentication in the internet banking environment”, Han-Na Y. et al.		✓	✗	✗	✓
“Design and Implementation of Anti-Screenshot Virtual Keyboard Applied in Online Banking”, Shangfu G. et al.		✓	✗	✗	✗
“Study of Security Mechanisms in Personal Internet Banking – Take China Merchants Bank as an Example”, Guoling L. et al.		✓	✗	✗	✗
“Security Testing and Compliance for online Banking in Real-World”, Chen H. and Corriveau JP.	✓		✗	✓	✗
“Information Security Management”, Modiri N. and Sobhanzabeh YM.	✓		✗	✓	✗
“Comparing different information security standards: COBIT vs. ISO 27001”, Arora V.	✓		✗	✓	✗

APPENDIX C
INTERVIEW FORM



Campu Bank Interview Form

No	Interview Question	IOC Grade			Comment
1	<p>From the observation results, we can see that in Cambodia have three types of citizen identity card. Comparing to Thailand has only one type of citizen identity card. It is the same as last version (type 3) of Cambodian's identity card carried with chip. So, what do you think about these kind of citizen identity card in Cambodia? Did your staff capable enough to recognize which one is the real citizen identity card while open bank account and the internet banking service?</p> <p>.....</p> <p>.....</p> <p>.....</p>	1	1	1	
2	<p>According to the internet banking crime cases in Thailand, muggers faked the warden and police identity card to open bank account at different bank branch of victim and then register the internet banking service. After that the internet banking system automatic add all account to mugger faking account because of victim and mugger identity number is the same. So, what do you think about this case, if the mugger can bypassed through this step? Why?</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p>	1	1	1	
3	<p>According to our observation results, we found that other banks in Thailand are strictly with foreigner to open bank accounts because of international hacker are moving around world especially in Thailand. The bank required many evidences from them, especially valid visa and work permit or local residential address issued by government authorities. As we found some documents that issued by government authorities contain with name and address only. So, what do you think about these requirements in term of safety for the bank and user's ease of use?</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p>	1	0	1	

No	Interview Question	IOC Grade			Comment
4	Another case that we found from the internet banking crime cases in Thailand, victim A do not register the internet banking but the mugger register for them by faking some documents issued by government authorities and then register the internet banking for the victim. What do you think about this problem even register through bank branch can be cheat by muggers?	1	1	1	
5	We found that all banks in Thailand allow their customer to register through ATM. Do you think it is secure for users or not? Why?	0	1	1	
6	Do you think it is secure or not for some banks that deployed auto add all account for their user after register the internet banking service? Why?	1	1	1	
7	We also found that some banks in Cambodia and Thailand still used email to send username and password, Do you think it is secure for customers or not? Why?	1	1	-1	

No	Interview Question	IOC Grade			Comment
8	Do you think it is secure or not for bank set username of the internet banking in fixed that cannot change even reset the new username? Why?	1	-1	1	
9	How do you feel about first time registration of the internet banking registration that send username and password through via email with long expiration? Why?	0	1	1	
10	What do you think about all banks in Cambodia, required their customers to reset username and password through bank branch? Why?	1	1	0	
11	Do you think all questions that call center authenticate to reset username and password with users is secure? Why?	1	-1	1	
12	What is your recommendation about your bank that let your customers to reset username and password through bank branches besides using call center to reset it?	1	1	0	



No	Interview Question	IOC Grade			Comment
13	<p>According to the observation results of call center authentication, we found that your bank has used a memorable question for user to select and answer by them self. If the user forgets their password, this question's answer will authenticate with user. What happen if the user answer it incorrectly even their password they forgot?</p> <p>.....</p> <p>.....</p> <p>.....</p>	0	1	1	
14	<p>Do you prefer to employ the Token device for your general customers to use it?</p> <p>.....</p> <p>.....</p> <p>.....</p>	1	0	1	
15	<p>We found that one bank in Cambodia used OTP at the log-in webpage and also one bank in Thailand used CAPTCHA at log-in webpage after the user type username or password incorrect two times. Why did your bank not use OTP or CAPTCHA to avoid your customers from vulnerable on the log-in webpage of the bank?</p> <p>.....</p> <p>.....</p> <p>.....</p>	1	1	1	
16	<p>Why did your bank not employ the alerting system through via email or SMS while the user log-in or log-out into their account?</p> <p>.....</p> <p>.....</p> <p>.....</p>	1	0	1	

No	Interview Question	IOC Grade			Comment
17	<p>We found that all banks in Thailand deployed the alerting system in all financial transactions, activities and settings like log-in, transfer, payment, change username or password and so on. So, What do you think about alerting system that all banks in Thailand deployed for their users? Why?</p> <p>.....</p> <p>.....</p> <p>.....</p>	1	1	0	
18	<p>We also found that one bank in Cambodia use on screen keyboard at password area and other one bank in Thailand use virtual keyboard at OTP or PIN number area. Do you think it can help users from vulnerabilities or some malware? Why?</p> <p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <p>.....</p> <p>.....</p> <p>.....</p>	1	0	1	
19	<p>Do you prefer to use on screen keyboard at your bank log-in webpage one bank in Cambodia and one bank Thailand that already used it?</p> <p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <p>.....</p> <p>.....</p> <p>.....</p>	-1	1	1	
20	<p>What is your recommendation for users who want to pause the internet banking services through call center and bank branch?</p> <p>.....</p> <p>.....</p> <p>.....</p>	0	1	1	

No	Interview Question	IOC Grade			Comment
21	How does your bank verify with user's mobile phone? If your bank used SMS OTP through mobile number?	-1	1	1	
22	How did your bank keep HTTPS and EV-bar a live on the URL of browser?	1	-1	1	
23	How confidential your bank trust on HTTPS and EV-bar of bank digital certificate? Why? <input type="checkbox"/> Very Convinced <input type="checkbox"/> Convinced <input type="checkbox"/> Usual <input type="checkbox"/> Awful <input type="checkbox"/> Very Awful	1	0	-1	
24	According to our experiment, we found that most of the bank in our research affected by SSL stripping attack also your bank too. Did you know about this attack? How did you protect your users from it?	1	1	0	

Comments

.....

.....

.....

.....

.....

.....

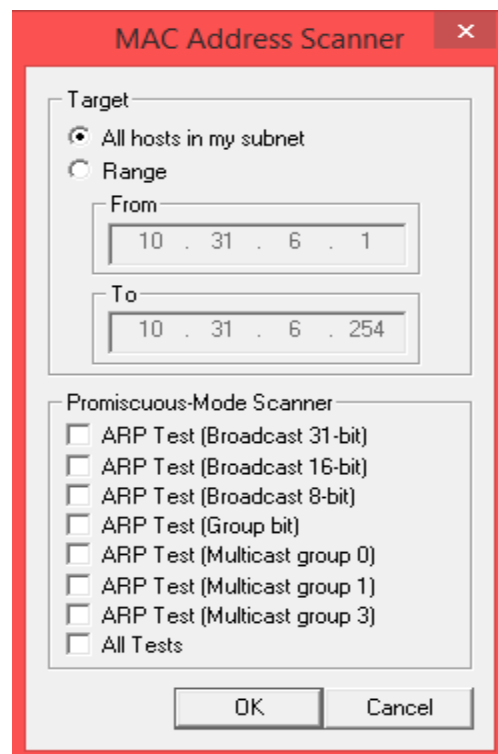
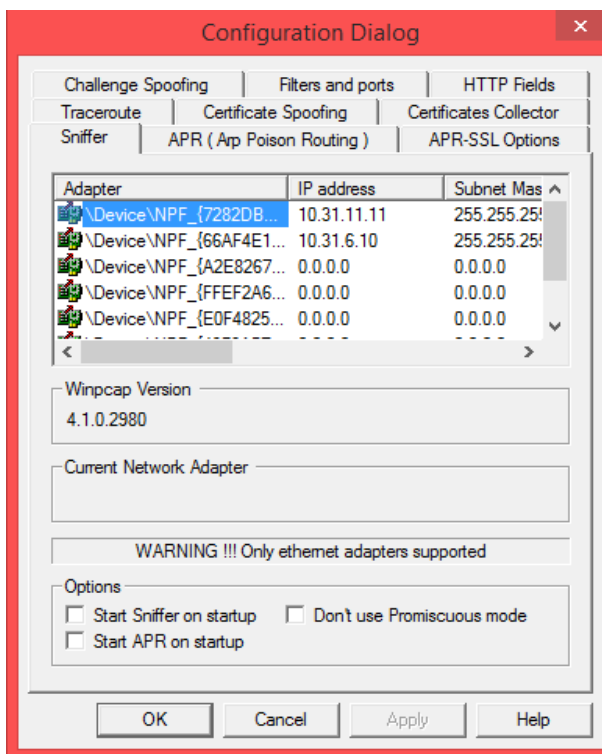
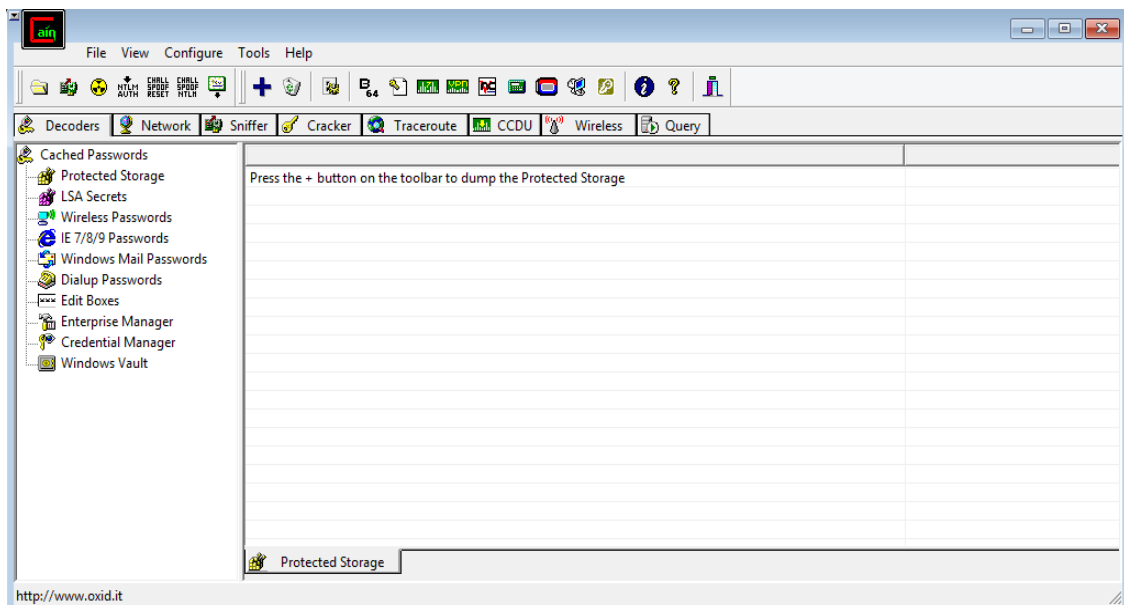


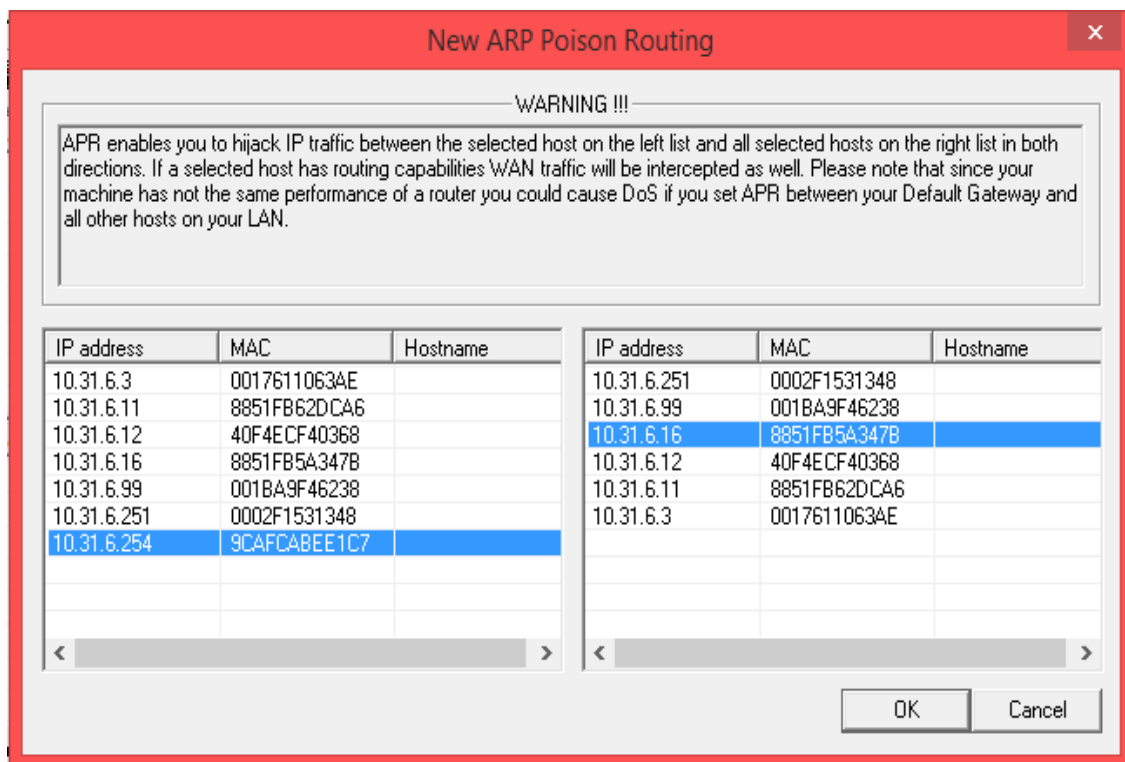
APPENDIX D

EXPERIMENT AND RESULTS

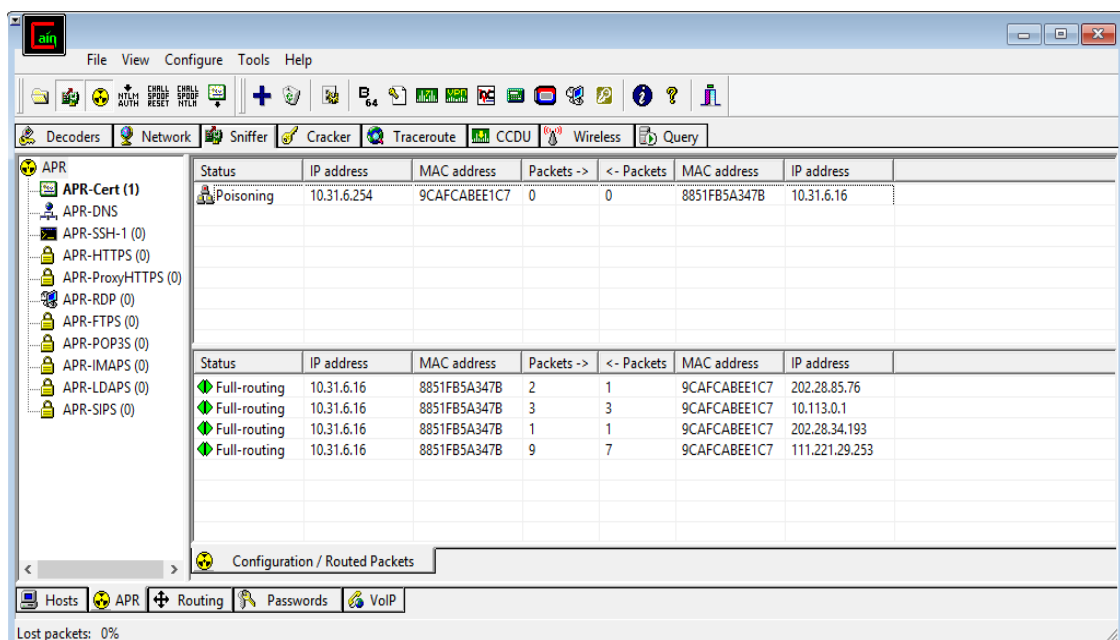


1, SSL Sniff By Using Cain and Abel





Click on this icon to start or stop ARP




```

root@kali: ~
File Edit View Search Terminal Help
0%24ctl12%24txtValidateCode=61168&ctl00%24ctl12%24btnLogin=Login
2015-09-27 05:38:42,622 SECURE POST Data ( [REDACTED] ):
  EVENTTARGET=&_EVENTARGUMENT=&_LASTFOCUS=&_VIEWSTATE=Klou8msxwGV25Fgg56x50Gd
mRGcStBDIEgcVGXAuNSJdshDRHzp5oUKPt9H7DpfZZnzGkUTb0Ca0hMppgtNLGCwNXAr3KdaBh8ikJHg
mIkbzo6oV%2B%2FuP3G2yJsdPeIBcvMYkHX46MbFWF7Z0EiPvRv%2FxEcPJc%2B0xEu23XuRsuDUYF0
x3nRVZRYLerb8lJezswmsToBJnVMI%2F%2BEP8LfvopaAYN4XGdKmqY1l0g04MijR73MAvPHxMEcv7JM
5D%2Fzkg%2FTbU%2F7zzh0Qi0qtR09c0PGBdK0TD1ieUNL5eXag4gJ5luGwiS3mYu5LdhmBdX4nGf5JZ
o2%2FMyvdVVi2y9JZq1%2Fj8Z0ArrzjanzM8X4mi5FYDkjFoPDog64S3ioTm0SYaSUaKDEExXW0LKQep
kZB5XNus83ChSKmjBn52Qim9Epv3H4SxrSWuRwKS6RBh53L6YTz0iua4%2F06SoelWud2wvC3aVLfhoQ
0Hkh2wvftZP5SPfgK%2BJU%2BDvo%2Bp40Pjqumz0qjlfxHdY4kF1%2Bjhp9EIC%2Bqm%2FE%2FasLF
g0m622m9S64Na%2B%2BV0KQ4DJWbepv5xppTN1BfonFN5Wi rv00dCwxGxTVyLE%2FzLuI4Kyoy0cLTmW
zRpsHjKQtuotzsbLLxdE0FgbnQ8CRhrw64Yp8mXxwIDZRCG7raYC5yaYbnVM1akr57f7TNhw%2BXjYD
mlv70nJAhYyJGQbSD5n%2FPSC418ziIsfmvjWFPVzkJtIdAUqPisT4HKPmuX3s4PRqbTnpwSjzzTNGFL
KvfRx2j7lopF%2FQj fEub%2FjykpUua6L3xX9C5TA1vBtxVvs5XhkI fhH3w7hIXULZI9JPzyk0ff7%2B
MpdiaUML%2BAQtuAh8uNGmZlNRV3zChuzLEBjxDyEtyKSjWmdzLym%2FaJOM6GBdB%2FXkkm9bzJgT6z
XHRSfC9woP%2F8y02SkGICQyfQVkw5NlXqcIxLShd7fzhui1cVdfawAchnR8QILFqNnp0E42rR%2FNpo7
8Fxnaf0hjoWLBCE6w8MtCQEzAYrBo40L0L1057UXF75ouM%2BU5bHjmhB5f0IEoFhPzqL91uYsp12u
tib%2FbKttukcFkY3Pga4yT0M0ItWBSAek9msUGzIIrhvRhcz10S9ArJJ3EUhw%2BX2K4w6DBH0o0LnL
8M0UjuB%2F2FBM0an3WY9MkjsGqX65r4KL8qixNiZ%2FFQ0wk4eHVXQzZ7c0xP7btujIdNLq7jEQ9Fwx
LncMPKE9YmaKei9i5xUgzprSRGH2xxAYH5TB3BuvvDnDiXu090IhRy4o2wkLR2SBe9FicoDR4cQ0Syq
hRHxqj8zP82dsf6qUIJP12wve4PyK5AXliYElzUtZQBnmqz1luGcLAai8EXfjMQYiPxy6I0SnPJZnbkk
Zi%2B7e823q%2Bews9wxDaEECChkXz85dwIRgxWhzwGd3%2B08LyTWPaZawoWb%2B6339UcT4adJskFC
dS%2FZjC7n2ok3ogMjiZw76vZ0xF8IhBC1Bs2nhKwHvJRUBPwoGpHuZz7QmJ9MF8ehjY4nJNITRkF483
RGn068EXp27RIaeh2Z4d04r6UjCLMmSkxKn0N5xyw%2Bvf%2B%2BVVpMvSa9Up8ojh5WxQaHsIn50dy2

```

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ls
Desktop  sslstrip.log
root@kali:~# sslstrip.log
bash: sslstrip.log: command not found
root@kali:~# cat sslstrip.log
2015-09-27 05:16:19,438 POST Data (10.99.92.10):
username=[REDACTED]&password=[REDACTED]&pwd=[REDACTED]&secret=true
2015-09-27 05:22:42,675 POST Data ([REDACTED]):
loginid=[REDACTED]&uipassword=&languageName=en_US&locale=en_US&password1=7c33
787c98c13f39f427facdd37c424c&password2=643d47ba7041c3c35790992c0a877681004b65b99
05727922067c8f6f98af185&sessionId=p7vPwH7KmNJS58DqpQh3pfTM66kSgp0GN1wn1XXsl3c3C6
5wJr48%212036392842%21778071599%211443331018578&authenticateToken=true
root@kali:~#

```



```

root@kali: ~
File Edit View Search Terminal Help
2015-09-27 05:50:33,000 SECURE POST Data ( [REDACTED] ):
IBLang=EN
2015-09-27 05:50:48,301 SECURE POST Data ( [REDACTED] ):
__EVENTTARGET=&__EVENTARGUMENT=&VAM_Group=GROUPMAIN&__VIEWSTATE=%2FwEPDwUKMTM2Mj
MzNjAzNA8WAh4EbGFuZwspZkJCTC5VdGlsaXR5cy5CQkxMYW5ndwFnZSwgQkJKMLmCYW5raw5nLlV0aW
xpdHksIFZlcnNpb249MzguMi4zLjYsIEN1bHRlcmU9bmV1dHJhbCwgUHViYGljS2V5VG9rZW49bnVsbA
EWAgIDDxYCHgdvbnJlc2V0BUVpZiAod2luZG93LnNldFRpbWVvdXQpIHdpbmRvdy5zZXRUaW1lb3V0KC
dWQU1fT25SZXNldChmYWxzZSk7JywgMTAwKTsWCAIBD2QWFGYPdxYCHgRUZXh0BQIxMmRkAgEPDxYCHw
IFA0VuZ2RkAgIPDxYCHwIFCeC5hOC4l%2BC4omRkAgMPFgYeA3NyYwU5flxXb3JrU3BhY2VcU2lnbm9u
SW1hZ2VzXGVuXExhcmdlXDFcMjAxNTA4MTkwNjQ1MDAyOTQuZ2lmHgdPbkNsawNrBX5qYXZhc2NyaXB0
0k9wZW5UaWw1KkdodHRwOi8vd3d3LmJhbmdb2tiYw5rLmNvbS9PbmtpbmVfYw5raw5nLlB1cnNvbmsFs
QmFua2luZy9pQmFua2luZy9CdWfsdWfuZ2lCYW5raw5nLlBhZ2VzL3Ntc2ZyYXVklmFzcHgnKTseBWNs
YXNzBQRIYW5kZAIEdW9kFgIeCXdhbGVyYwFyYwUHVNlciBJRGQCBg8PZBYCHwYFDFBJTj9QYXNzd29y
ZGQCA8PFgIfAgUGTG9nIE9uZGQCCQ8PFgIfAgUPUmVnaXN0ZXIgt25saw5lZGQCCg8WAh4Jaw5uZXJo
dG1sBcgGPGRpdj48ZG12IGNsYXNzPSd0ZXdzSGVhZGVyJz5XYXJuaW5nIGFnYwUuc3Qgc2lhcncRwaG9u
ZSB2aXJlc2wvZG12PjxkaXYgY2xhc3M9J05ld3NUaXR5ZSc%2BQmFuZ2tvaYBCYw5rIHdpbGwgbmV2ZX
Igc2VuZCBhbiBTTVMvTU1TL0VtYWlsIHJlcXVlc3RpbmcgeW91IHRvIGRvd25sb2FkIG9yIGluc3RhbG
wgYw55IHNVZnR3YXJlL2FwcGxpY2F0aW9uIG9udG8geW91ciBtb2JpbGUgcGhvbmluIFBsZWZzZSBiZS
Bhd2FyZSB0aGF0IG1hbG1jaW91cyBhcHBsaW5ndG1vbnMgY2FuIHN0ZWFsIHLvdXlVXNlciBJRCwgUG
Fzc3dvcmlQgYw5kIE9UUA8YSBocmVmpSdqYXZhc2NyaXB00k9wZW5UaWw1KkdodHRwOi8vd3d3LmJhbm
drb2tiYw5rLmNvbS9PbmtpbmVfYw5raw5nLlB1cnNvbmsFsQmFua2luZy9pQmFua2luZy9CdWfsdWfuZ2
lCYW5raw5nLlBhZ2VzL3Ntc2ZyYXVklmFzcHgiKTsnPk1vcmlU8L2E%2BPC9kaXY%2BPC9kaXY%2BPGRp
dj48ZG12IGNsYXNzPSd0ZXdzSGVhZGVyJz50b3cgeW91IGNhbiBpbnZlc3Qgaw4gbXV0dWFsIGZ1bmRz
IE9ubG1uZTwwZG12PjxkaXYgY2xhc3M9J05ld3NUaXR5ZSc%2BWW91IGNhbiBhcnJhbmdb1IGZpcnN0LX

```

```

2015-09-27 05:40:11,324 SECURE POST Data ( [REDACTED] ):
LOGIN=[REDACTED]SPASSWD=[REDACTED]&lgin.x=31&lgin.y=4
2015-09-27 05:40:12,157 SECURE POST Data ( [REDACTED] ):
SESSIONEASY=07085573657269643D3039303132303135303335377C53636F64653D585230326633
394A3669747472785058674756566F73766C465850366B6E426A7035316878520503
2015-09-27 05:41:00,872 SECURE POST Data ( [REDACTED] ):
SESSIONEASY=07085573657269643D3039303132303135303335377C53636F64653D585230326633
394A3669747472785058674756566F73766C465850366B6E426A7035316878520503&undefined=u
ndefined
root@kali:~#

```



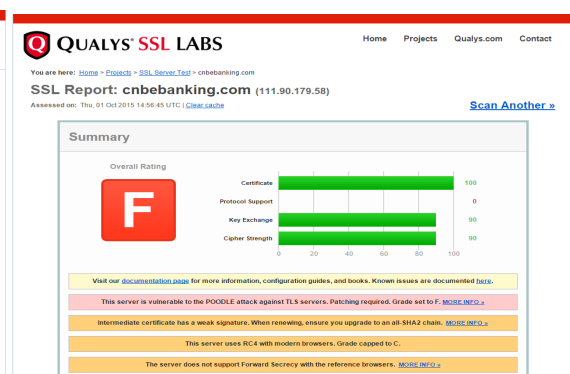
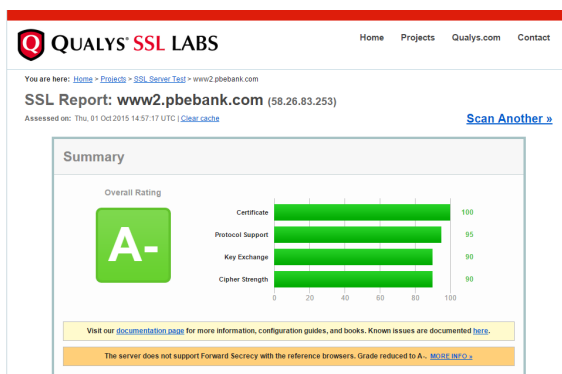

```

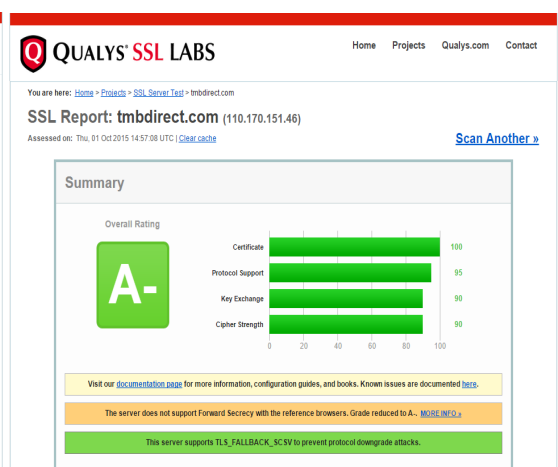
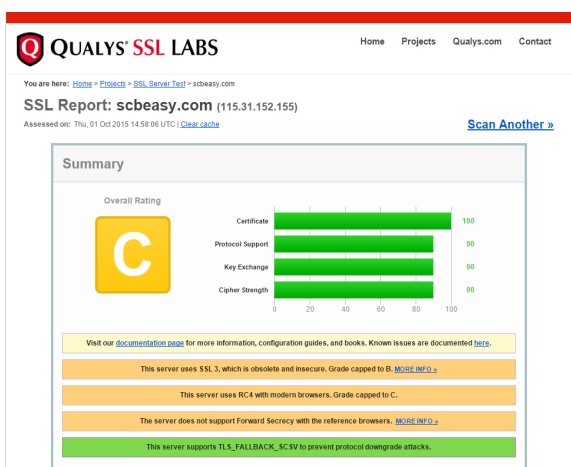
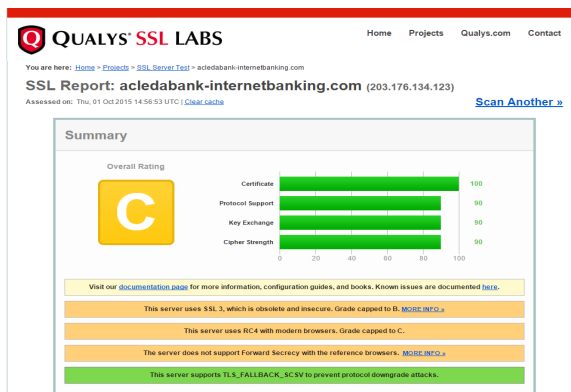
root@kali: ~
File Edit View Search Terminal Help

05727922067c8f6f98af185&sessionId=p7vPW7KmNJS58DqpQh3pfTM66kSgp0GN1wn1XXsl3c3C6
5wJr48%212036392842%21778071599%211443331018578&authenticateToken=true
2015-09-27 05:27:02,121 SECURE POST Data (www.tmbdirect.com):
timestamp=&localeId=en_US&platform=0&appID=TMB&appver=1.0.12.25&serviceID=getPh
rases&locale=en_US&channel=wap&platform=thinclient&cacheid=&tknid=&rcid=spadeskt
opweb&
2015-09-27 05:27:03,324 SECURE POST Data (www.tmbdirect.com):
widgetName=segCampaignImage&formName=frmIBPreLogin&appChannel=I&prelogin=Y&appID
=TMB&appver=1.0.12.25&serviceID=GetCampaign&locale=en_US&channel=wap&platform=th
inclient&cacheid=&tknid=&rcid=spadesktopweb&
2015-09-27 05:27:55,747 SECURE POST Data (www.tmbdirect.com):
loginId= &userid= &password= &appID=TMB&a
ppver=1.0.12.25&serviceID=IBVerifyLoginEligibility&locale=th_TH&channel=wap&plat
form=thinclient&cacheid=&tknid=1185E45766BB99E2C2D0E938CE58978B8FF309D35E7E9DFDC
684FF44F5D0841B&konyreportingparams=%7B%22plat%22%3A%22windows%22%2C%22aid%22%3A
%22TMB%22%2C%22aver%22%3A%221.0.12.25%22%2C%22aname%22%3A%22vit_1.0.12.25_build8
3%22%2C%22did%22%3A%221443331675909-0fd5-3376-650f%22%2C%22os%22%3A%2245%22%2C%2
2stype%22%3A%22b2c%22%2C%22dm%22%3A%22%22%2C%22ua%22%3A%22Mozilla%2F5.0%20(Windo
ws%20NT%206.3)%20AppleWebKit%2F537.36%20(KHTML%2C%20like%20Gecko)%20Chrome%2F45.
0.2454.101%20Safari%2F537.36%22%2C%22chnl%22%3A%22desktop%22%2C%22atype%22%3A%22
spa%22%2C%22fid%22%3A%22frmIBPreLogin%22%2C%22kuid%22%3A%22%22%2C%22rsid%22%3A%2
21443331675910-949a-11f9-f7e0%22%2C%22metrics%22%3A%5B%5D%7D&rcid=spadesktopweb&
2015-09-27 05:27:56,957 SECURE POST Data (www.tmbdirect.com):
rqUUID=&LoginInd=login&TriggerEmail=yes&activationCompleteFlag=Login&appID=TMB&a

```

3, Scanning Results





BIOGRAPHY



BIOGRAPHY

Name Mr. Sok Rachana

Date of Birth 23 October 1990

Place of Birth Sangkat Beoung Keng Korng II, Khan Chamkamorn,
Phnom Penh, Cambodia

Institution Attended

2008	Zaman International School, Phnom Penh
2012	Royal University of Phnom Penh, Phnom Penh, Cambodia Bachelor Degree of Computer Science and Engineering
2016	Faculty of Informatics, Mahasarakham University, Thailand Master Degree of Computer Science

Position and Work Place

Teller at Cambodian Public Bank PLC.

Contact Address

No. 1, Street 2, Borey Phnom Penh Thmey, Sangkat Phnom Penh
Thmey, Khan Sen Sok, Phnom Penh, Cambodia
Tel: (+66) 087 641 0391, (+855) 070 711 526
Email: rachanase7en08@gmail.com

