Online Banking Security and Usability
Towards an Effective Evaluation Framework

Mansour Alsaleh[1], Abdulrahman Alarifi[1], Ziyad Alshaikh[1] and Mohammad Zarour[2]
[1]*King AbdulAziz City for Science and Technology, P.O. Box 6086, Riyadh 11442, Saudi Arabia*
[2]*Prince Sultan University, College of Computer Science and Information System, Rafha Street, P.O Box 66833, Riyadh 11586, Saudi Arabia*

Keywords: Security and Usability Evaluation, Online Banking, Online Consumers Trust.

Abstract: Convenience and the ability to perform advanced transactions encourage banks clients to use online banking. As security and usability are two growing concerns for online banking users, banks have invested heavily in improving their web portals security and user experience and trust in them. Despite considerable efforts to evaluate particular security and usability features in online banking, a dedicated security and usability evaluation framework that can be used as a guide in online banking development remains much less explored. In this work, we first extract security and usability evaluation metrics from the conducted literature review. We then include several other evaluation metrics that were not previously identified in the literature. We argue that the proposed online banking security and usability evaluation frameworks in the literature in addition to the existing standards of security best practices (e.g., NIST and ISO) are by no means comprehensive and lack some essential and key evaluation metrics that are of particular interest to online banking portals. In order to demonstrate the inadequacy of existing frameworks, we use some frameworks to evaluate five major banks. The evaluation reveals several shortcomings in identifying both missing or incorrectly implemented security and privacy features. Our goal is to encourage other researchers to build upon our work.

1 INTRODUCTION

Internet technologies have experienced a rapid growth over the last decades, as it became a major element in almost every business. One of the most important developments in this aspect is the banking industry. Online banking is a new business model and development direction in banking industry in which fixed operating costs are decreased by providing uninterrupted set of banking services (YeeLoong Chong et al., 2010). Online banking is expected to grow due to the dramatical increase in using e-commerce applications in businesses by Internet users (Laukkanen et al., 2008). Through online banking, banks compete to increase loyalty of customers, gain a bigger share of the market, improve services, provide value added services, increase efficiency and decrease operational cost (Lichtenstein and Williamson, 2006).

Most banks in the world provide online banking; providing their customers with the ability to access their bank accounts and make transactions anytime and anywhere. Banks have been able to reach out to millions of customers through online banking and offer more products and a relatively better, convenient and flexible banking experience relative to traditional, fixed-location branches. On the flip side, online banking has revealed a set of security threats and privacy concerns that can endanger the use of such financial services (Weir et al., 2010) (Mannan and van Oorschot, 2008). While most banks claim secure and easy access through their websites to clients' accounts where they can perform most of their daily transactions online, the balance between practical security and reasonable usability of online banking is considered to be a vital question (Casalo et al., 2007).

Sixty-eight percent of consumers with regular Internet access and a bank account used online banking in the year prior to March 2012. New figures released by Financial Fraud Action UK (FFA UK) show an increase by 3 percent in online banking fraud in the UK during 2013. Most online banking fraudsters are located overseas which even harden more the way of hold them accountable for their activities (Aladwani, 2001).

In this paper, we investigate existing frameworks for evaluating online banking security and usability.

Alsaleh M., Alarifi A., Alshaikh Z. and Zarour M..
Online Banking Security and Usability - Towards an Effective Evaluation Framework.
DOI: 10.5220/0005493901410149
In *Proceedings of the 11th International Conference on Web Information Systems and Technologies* (WEBIST-2015), pages 141-149
ISBN: 978-989-758-106-9

Table 1: Number of metrics for each security category.

	Category	Num. of Metrics
1	General online security and privacy information to the Internet banking customers	13
2	IT assistance, monitoring and support	4
3	Bank site authentication technology	3
4	User site authentication technology	29
5	Internet banking application security features	10
6	Software and system requirements and settings information	14

Table 2: Number of metrics for each usability category.

	Category	Num. of Metrics
1	Interface	22
2	Navigation	23
3	Content	22
4	Services Offered	11
5	Reliability	8
6	Technical Aspects	2
7	Multi-factor Authentication Methods	9

We combine a set of frameworks that examine the related security properties in the following: (1) losses compensation; (2) security monitoring, support, and awareness; (3) authentication and encryption mechanisms; and (4) Internet banking application security features. We also include those that examine the related usability properties including: (1) interface; (2) navigation; (3) content; (4) offered services; (5) registration and transaction procedure; and (6) multi-factor authentication methods. We argue that the proposed online banking security and usability evaluation frameworks in the literature in addition to the existing standards of security best practices (e.g., NIST and ISO) are by no means comprehensive and lack some essential and key evaluation metrics that are of particular interest to online banking portals. We demonstrate the inadequacy of existing frameworks through evaluating five large international banks using a combination of some of these frameworks. Our examination of the security properties is limited to only the front-end interface of the online banking portal as we do not have access to the back-end security mechanisms. The evaluation reveals several shortcomings in these frameworks in identifying both missing or incorrectly implemented security and privacy features.

We hope to inspire additional research efforts addressing the difficult problem of how to establish and maintain a comprehensive security and privacy framework that can be used not just for the evaluation of existing online banking portals, but also during the design and development phases. We anticipate that, should it be built particularly for online banking, a carefully thought-out security and privacy framework will not just enhance usability and security and eliminate many forms of fraud but it will also help online clients to trust with confidence these services.

The remainder of the paper is organized as follows. In the next section, we present an online banking security and usability evaluation framework extracted from state-of-the-art evaluation metrics in the literature. Section 3 provides an illustrative example that first shows a comparative analysis of the security and usability of the five examined banks using our framework and then identifies the framework shortcomings. Section 4 provides further discussion and concludes.

2 ONLINE BANKING SECURITY AND USABILITY EVALUATION FRAMEWORK

Including several evaluation metrics that were not previously identified in the literature, we built our framework on top of the Internet banking security checklist proposed by Subsorn and Limwiriyakul (Subsorn and Limwiriyakul, 2011). We have also included key usability features from MoBEF, a banking portal evaluation framework (Zarifopoulos and Economides, 2009). The resulted framework captures the most important features for secure yet usable online banking. It considers all the important factors from the first visit to the site, to the registration process, authentications methods and up to the completion of the transaction.

The framework consists of two large sets of metrics for (1) security evaluation; and (2) usability evaluation. The metrics are extracted and derived from the literature as well as several new ones. While we tried to collect the best available evaluation approaches, we believe that the resulted framework is by no means comprehensive and lacks some essential and key evaluation metrics that are of particular interest to online banking portals.

2.1 Security Evaluation Metrics

The security evaluation part of the framework consists of 73 metrics which are categorized into 6 main categories (see Table 1). The framework examines the current confidentiality policy that banks provide to their clients. The provided information to the Internet banking customers to increase their awareness of the possible cyber attacks are evaluated in the framework. It also examines the bank current guarantee policy in which the bank is obliged to cover any losses in case of unauthorized transactions committed by someone

other than the customer, using the customer's online banking account. Furthermore, the security evaluation part of the framework verifies the availability of IT hotline and helpdesk services. Ideally, the banks must provide various modes of communication with their online banking clients.

The framework involves the identification of the deployed authentication technology in the web portal (i.e., login mechanism, login requirements, login failure limitation, and transaction verification) and the characteristics of the secure connection between a client's host and the bank server. The framework also inspects whether the bank supports multi-factor authentication and their ability to guarantee high level of identity confirmation.

Internet banking applications are also examined against a set of metrics that are intended to mitigate the risk of security breaching and remote malicious attacks, such as worms and viruses. For example, automatic timeout for inactivity is one of the examined security features that sets a default inactivity period after which the online client is logged off. Session management is also evaluated from the perspective of securing transactions execution during online banking sessions (e.g., session tokens, page tokens technologies, and deleting the corresponding cookie information in the user browser after the client logs off or closes the Internet browser). In order to mitigate the risk of impersonation attacks, the default allowable transfer amount should be limited and tied with an additional factor authentication (e.g., PIN verification through SMS).

In addition, the framework also examines the bank portal support for various Internet browsers, the provided OS and browser settings by the banks for optimum and safe usage, and if there is any provided Internet security software to the bank clients in order to protect their machines. A summary of the metrics used in the security evaluation part of the framework is given in Table 1. Detailed description of the used metrics is given in Table 5 in Appendix A.

2.2 Usability Evaluation Metrics

The usability of security features in online banking is a key factor for their effectiveness in performing the intended objectives. Unfortunately, many security solutions place usability considerations as a second priority as developers might not recognize the tight relationship between them (Gutmann and Grigg, 2005) (Seffah et al., 2006) (Braz et al., 2007).

The usability evaluation part of the framework inspects various key usability aspects of the online banking web portal including interface, navigation, content, service offered, reliability, authentication methods and others (see Table 2 for a summary of the used usability metrics; detailed description of the used metrics is given in Table 6 in Appendix A). The interface is evaluated against several design principles in order to maximize user task completion and minimize interfering. Also, the framework examines criteria related to the effective use of color, graphics, and multimedia. Furthermore, it examines the right use of the text and language, and the web pages' adjustment to various situations. Navigation through the online banking application is also evaluated from convenience and easiness perspectives. For example, the site organization, menus, site map and effective search engine are all important factors as users should easily navigate the site and find exactly what they are looking for.

The content of banking web applications play an important role in respect to usability. Information about available banking services must be comprehensive and clear. The web application should provide sufficient recent information not only about financial, accounting, and investment issues but also about technical requirements in accessing and using the site. Finally, the system must provide detailed technical help for both expert and novice users. Beside the content, it is important that the bank web application provides multiple services and transactions types.

In general, the framework focuses on the usability of security features such as the usability of the deployed authentication and verification mechanisms. While we include mainly security and usability metrics, the framework also examines: (1) the reliability of the registration process and the transaction procedure; and (2) the continuous availability of the online banking services.

3 CASE STUDY: RESULTS, ANALYSIS, AND IDENTIFIED SHORTCOMINGS IN THE FRAMEWORK

In this section, we apply the modified version of the framework (see Sections 2.1 and 2.2) to evaluate the security and usability of online banking for five large banks in the MENA region (see Tables 3 and 4 for the results of evaluating the five banks using our framework, for the security and usability parts, respectively). We start by opening chequing accounts in these selected banks and then collect the related user guides and information from the banks' web portals. We evaluate each bank against these metrics and com-

Table 3: The results of evaluating the five banks using the security part of the framework, where ni=no information, y=yes, and n=no; Table 5 in Appendix A explains the corresponding metrics in each category

Banks	Categories																			
	1														2				3		
	1.1	2.1	2.2	2.3	2.4	2.5	3.1	3.2	3.3	3.4	3.5	3.6	3.7	1.1	1.2	1.3	1.4	1.1	1.2	1.3
A	y	n	y	n	n	n	n	1	1	0	5	3	5	y	n	y	0	y	y	y
B	y	n	ni	n	n	n	y	5	5	0	5	5	5	y	n	n	2	y	y	y
C	y	n	y	n	n	n	y	5	5	0	5	5	5	n	y	y	5	y	y	y
D	y	y	n	n	n	n	ni	4	5	0	5	4	5	y	n	y	4	y	y	y
E	y	n	y	n	n	n	y	3	3	0	5	5	3	y	n	y	3	y	y	y

Banks	Categories																												
	4																												
	1.1	1.2	1.3	1.4	2.1	2.2	2.3	2.4	2.5	2.6	3.1	3.2	4.1	4.2	4.3	4.4	4.5	4.6	4.7	5.1	5.2	5.3	5.4	5.5	5.6	5.7	6.1	6.2	6.3
A	y	y	y	n	n	y	n	y	n	y	y	n	y	y	y	n	n	n	y	y	y	n	n	n	n	n	y	y	y
B	y	y	n	n	n	y	n	y	y	y	y	n	y	y	y	y	n	n	y	y	y	n	y	n	n	n	y	y	y
C	y	y	n	n	n	y	n	y	y	y	y	n	y	y	y	n	n	n	y	y	n	y	y	n	n	n	n	y	n
D	y	y	n	n	n	y	n	y	y	y	y	y	y	y	y	y	n	ni	n	y	ni	n	ni	n	n	n	ni	y	ni
E	y	y	n	n	n	y	n	y	y	y	y	y	y	y	y	n	n	n	n	y	y	n	n	y	n	y	y	y	n

Banks	Categories																							
	5										6													
	1.1	1.2	2.1	2.2	2.3	3.1	3.2	3.3	3.4	3.5	1.1	1.2	1.3	1.4	1.5	1.6	2.1	2.2	2.3	2.4	3.1	3.2	3.3	3.4
A	y	y	ni	ni	y	n	y	y	n	n	ni	ni	y	ni	ni	ni	n	y	y	n	n	n	n	n
B	y	y	ni	ni	y	n	y	n	n	ni	ni	ni	ni	ni	ni	ni	n	ni	n	n	n	n	n	n
C	y	n	ni	ni	y	n	y	n	y	y	y	ni	y	ni	ni	y	n	y	n	n	y	n	n	n
D	y	y	ni	ni	y	n	y	n	ni	ni	y	y	y	ni	y	y	y	y	n	n	n	y	n	y
E	y	y	ni	ni	y	n	y	y	y	n	y	ni	y	ni	ni	y	n	ni	n	n	y	n	n	y

pare the banks against each other.

Although, the five banks have shown compliance with the national privacy principles and laws as well as the customer protection code; all the five banks are not liable for any claim, loss, expense, delay, cost or damage arising from or in connection with any instruction, request, inquiry or transaction made or affected where any user identification or password has been or is purported to have been used by unauthorized persons. An exception is when the bank website has been hacked or has been accessed by an unauthorized access, in which the bank will be obligated to compensate the clients after investigating the corresponding attack. We notice that only some banks provide sufficient necessary information about threats, attacks, general online security guidelines, security alert issues, and password security tips. However, there are some technical terms in the webpages that are intended for expert users only. Also, all banks did not provide information about key logger for their clients that can be used to steal user identification and password.

All banks employed SSL protocol with extended SSL validation certificate. The results show that all five banks offer tokens or SMS for two-factor authentication for signing in, where the user chooses the preferred way. However, no banks uses SiteKey [1] which is mainly used to detect phishing attacks. The banks apply restriction rules on the number of failed logins to prevent unauthorized users from attempting online password guessing attacks. In order to strengthen the password strength in terms of length, complexity, and unpredictability against online password guessing attacks, all banks request that the users must choose a minimum of 8 digits that include both characters and numbers. However, strict password composition polices on users were not applied (e.g., using combination of lower and upper case and forcing users to change the password periodically).

When a user loses or forgets her password, the banks vary slightly in their password recovery methods. Although most of the banks require the user to use ATM card number, ATM PIN number, and/or their national ID number to reset their passwords online, some banks require more rigorous verification steps for the password recovery (e.g., accessing an ATM machine to reset the online banking password). One bank sends an automatic generated verification code to the user's registered mobile number through an SMS and then the user types this verification code in the password reset form in the online banking site.

The banks provide additional security features to mitigate the risk of unwanted transactions. For example, all banks have an automatic timeout feature for inactivity that ranges from 2 minutes to 15 minutes for others. In terms of session management, all banks do clear the cookie information after logging off or closing the Internet browser. Also, all banks have a limited daily transfer amount to third party accounts to reduce the impact of unauthorized transactions. Furthermore, the international transfer limit is much less than the national transfer limit in some banks.

Banks are expected to provide their clients with detailed information about the required software settings and how to use the online banking portal in

[1] A web-based security mechanism that provides one type of mutual authentication between end-users and web servers

Table 4: The results of evaluating the five banks using the usability part of the framework, where ni=no information, y=yes, and n=no; Table 6 in Appendix A explains the corresponding metrics in each category

Banks	Categories 1																					
	1.1	1.2	1.3	1.4	1.5	2.1	2.2	2.3	2.4	2.5	3.1	3.2	3.3	3.4	3.5	3.6	4.1	4.2	4.3	4.4	4.5	4.6
A	5	5	5	5	5	4	5	y	y	y	y	y	y	y	5	5	y	y	n	y	n	n
B	5	5	5	4	5	4	3	y	y	y	y	y	y	y	5	4	y	y	ni	y	n	n
C	4	5	5	4	5	3	4	y	n	y	y	y	y	y	5	4	n	y	y	y	n	n
D	5	5	5	4	4	3	4	y	y	y	y	y	y	y	5	5	y	y	ni	y	n	n
E	4	4	5	4	4	4	4	y	n	n	y	y	y	y	5	4	n	y	ni	y	n	n

Banks	Categories 2																						
	1.1	1.2	1.3	1.4	1.5	1.6	2.1	2.2	2.3	2.4	2.5	3.1	3.2	3.3	4.1	4.2	4.3	4.4	5.1	5.2	5.3	5.4	5.5
A	4	4	y	y	y	y	5	4	5	y	4	4	y	y	4	3	3	3	5	5	5	5	4
B	4	4	y	y	y	y	5	4	5	y	3	4	y	y	5	5	4	4	5	5	4	5	3
C	4	3	y	y	y	y	5	3	5	y	5	4	y	y	na	na	na	na	5	5	5	5	3
D	4	4	y	y	y	y	5	5	5	y	4	4	n	y	na	na	na	na	5	5	5	5	3
E	4	3	y	y	y	y	5	3	5	y	4	4	n	y	5	0	0	0	5	5	4	5	3

Banks	Categories 3																					
	1.1	1.2	1.3	1.4	1.5	2.1	2.2	2.3	2.4	3.1	3.2	3.3	3.4	4.1	4.2	4.3	4.4	4.5	5.1	5.2	5.3	5.4
A	3	5	2	3	y	y	y	y	y	4	y	5	5	y	y	y	n	5	4	3	4	4
B	3	5	5	4	y	y	y	y	y	3	y	3	4	n	y	y	n	4	2	4	3	5
C	5	5	5	4	y	y	y	y	y	3	y	4	5	y	y	n	y	4	4	3	4	4
D	3	5	5	5	y	y	y	y	y	4	y	5	4	y	y	y	y	4	3	4	3	3
E	5	5	5	4	y	y	y	y	y	4	y	4	4	y	y	y	y	4	3	4	4	4

Banks	Categories 4											5								6		7								
	1.1	1.2	1.3	1.4	1.5	1.6	2.1	2.2	2.3	3.1	3.2	1.1	1.2	1.3	1.4	1.5	2.1	2.2	2.3	1.1	1.2	1.1	1.2	1.3	1.4	1.5	1.6	1.7	2.1	3.1
A	5	5	4	ni	y	n	y	y	n	y	y	4	5	5	0	5	y	y	y	5	4	n	y	y	y	2	5	y	n	5
B	4	4	4	ni	y	y	y	y	y	y	y	4	5	5	0	5	y	y	y	5	2	n	y	y	y	3	5	y	n	na
C	5	5	5	y	y	y	y	y	n	y	y	3	5	5	3	5	y	y	y	5	3	y	n	y	y	2	5	y	y	na
D	5	5	5	ni	y	y	y	y	y	y	y	5	5	5	5	4	y	ni	y	5	2	y	n	y	y	2	5	y	n	2
E	5	5	4	y	y	y	y	y	n	y	y	4	5	5	5	5	y	y	y	5	4	y	n	y	y	2	5	y	n	na

order to have a pleasant experience and to harden their machines to become less vulnerable to security breaches. Though, all the evaluated five banks did not provide any information about operating system requirements, security settings, and browser settings, other than internet connection, and browser type with the implicit assumption that the user knows how to access and use the online banking safely. Some banks offer their clients with links to download free/paid antivirus and antimalware software.

From a usability perspective, the five banks have followed good design principles in implementing their we portals and have made an effective use of white space, color, and graphics. Graphics and multimedia are used moderately to make their websites easier to navigate and more attractive without having negative impact on loading time. Furthermore, the banks show a consistent use of text and page format as well as the use of plain language that users can understand. The pages capability to fit the browser window vary from one bank website to another; however, printable versions of pages are available. Although the banks offer their websites in two languages based on the spoken languages in the corresponding hosted country, unfortunately, their websites have not shown any accommodation for users with special needs, nor provided options for users with diverse levels of skill and experience. The five banks' websites can be intuitively used by average users (e.g., the site map and navigation bar). We also notice that some banks separate online banking pages from other bank informative (or non-functional) pages to simplify navigation. Although the banks portals provide no broken links or under-construction pages, good link labeling, clear indicators of current position and an effective use of frames, they either have failed to provide an effective search feature or have no search feature at all.

The five banks have shown excellent scores in providing information about their online services and their charges, terms and conditions, and demo of online services that shows how to use the bank's site; however, the user must go through various documents to get all information. Also, the banks utilized their online banking portals to effectively present advertisements of their services and a controlled amount of advertisements of other third-parties.

All the five banks have fairly simple registration process and easy to use banking services as well as excellent profile/account management. They provide helpful tools and some extra services such as shop-online and charities support. One of the banks requires new users to visit an ATM machine or any branch to verify her identity which negatively affects the usability (although it increases the security of the registration process). This is an example of the trade-off between security and usability in which the evaluation metrics in different frameworks may have negative relationship with each other. The five banks provide action history to view all the transactions.

Although several metrics have been evolved to deal effectively with existing limitations in our proposed framework, our study shows that the framework needs further improvements. The framework must reflect a sound trade-off of having a secure and yet a usable portal. The existing framework does not provide any prioritization for a long list of metrics in which all of them are treated equally. Prioritization is essential for the decision makers to take the right steps to improve their web services, find suitable remedies to handle their weaknesses, and utilize their strengths.

Prioritization also helps in establishing ranking levels or classes of satisfaction levels that helps not just in understanding the bank web portal current status relative to other portals but also in encouraging the bank to elevate to a more mature level through a set of well-defined steps. The evaluation will be used as an integral part of planning and hence should serve their stakeholders. The evaluation framework should be tailored to the evaluation purpose and stakeholders intended objectives that include banks, customers, and regulators. In fact, each evaluation framework must have an associated set of well designed steps to guide evaluation processes and activities.

Unfortunately, the current security and usability framework neglects the web portal back-end solutions which might play a key role in securing the online banking services. The back-end solutions include the adopted database servers, DMZ architecture, and core network infrastructure components (e.g., firewall and routers). All these solutions are integrated to form the final system that provides the online banking services to the customers. Furthermore, the used processes during product and service development and through service establishment, management, and delivery are not considered in the evaluation although they are de facto components that affect the security and usability of the final product or service. In short, the framework is oriented towards the final product rather than the used processes.

4 FURTHER DISCUSSION AND FUTURE WORK

It is important to realize that the security and usability are correlated and that it is preferable to evaluate them as one block rather than separately in order to capture their effects on each other. The evaluation framework must be tailored to serve the needs of the stakeholders without strong bias towards one over the other. The stakeholders should be involve in all evaluation phases and should be part of any resolution. Although such evaluations are considered milestones for any quality improvement process, they should be designed and tested within the quality improvement process in order to ensure their coherence with other parts in the process. With the online banking portals evolving as an essential source for banking services that are used by a majority of people, a more mature security and usability evaluation framework is indeed a necessity. In fact, in order to obtain an effective online banking security and usability evaluation framework, we need to leverage not just the existing frameworks in the literature and the existing standards of security best practices (such as NIST and ISO), but also the feedback gathered by engaging the online banking development and operational entities and the corresponding stakeholders. Driven by the existing needs and lessons learned from the conducted experiment and the literature, we are looking to develop a new effective and comprehensive framework that encompasses both essential and key evaluation security and usability metrics.

ACKNOWLEDGEMENTS

We thank Mashael Almeatani, Nouf Alnufaie, Mona Alsemayen, Njoud Alshehri, and Nora Alswailem for helping in conducting the evaluation. We also thank the anonymous reviewers for their comments which helped improve this paper to its present form. This work was supported in part by KACST.

REFERENCES

Aladwani, A. M. (2001). Online banking: a field study of drivers, development challenges, and expectations. *International Journal of Information Management*, 21(3):213–225.

Braz, C., Seffah, A., and M'Raihi, D. (2007). Designing a trade-off between usability and security: A metrics based-model. In *Proceedings of the INTERACT07*, pages 114–126. Springer.

Casalo, L. V., Flavián, C., and Guinalíu, M. (2007). The role of security, privacy, usability and reputation in the development of online banking. *Online Information Review*, 31(5):583–603.

Gutmann, P. and Grigg, I. (2005). Security usability. *Security Privacy, IEEE*, 3(4):56–58.

Laukkanen, P., Sinkkonen, S., and Laukkanen, T. (2008). Consumer resistance to internet banking: postponers, opponents and rejectors. *International Journal of Bank Marketing*, 26(6):440–455.

Lichtenstein, S. and Williamson, K. (2006). Understanding consumer adoption of internet banking: an interpretive study in the australian banking context. *Journal of Electronic Commerce Research*, 7(2):50–66.

Mannan, M. and van Oorschot, P. C. (2008). Security and usability: the gap in real-world online banking. In *Proceedings of the 2007 Workshop on New Security Paradigms*, pages 1–14. ACM.

Seffah, A., Donyaee, M., Kline, R., and Padda, H. (2006). Usability metrics: A roadmap for a consolidated model. *Journal of Software Quality*, 14(2).

Subsorn, P. and Limwiriyakul, S. (2011). A comparative analysis of the security of internet banking in australia: A customer perspective.

Weir, C. S., Douglas, G., Richardson, T., and Jack, M. (2010). Usable security: User preferences for authentication methods in ebanking and the effects of experience. *Interacting with Computers*, 22(3):153–164.

YeeLoong Chong, A., Ooi, K., Lin, B., and Tan, B. (2010). Online banking adoption: an empirical analysis. *International Journal of Bank Marketing*, 28(4):267–287.

Zarifopoulos, M. and Economides, A. A. (2009). Evaluating mobile banking portals. *International Journal of Mobile Communications*, 7(1):66–90.

APPENDIX A

In this appendix, we give a detailed description of the used security evaluation metrics (Table 5) and usability evaluation metrics (Table 6).

Table 5: The security evaluation part of the framework (most of the metrics are extracted from (Subsorn and Limwiriyakul, 2011))

Subcategory	Metric
Category 1: General online security and privacy information to the Internet banking customers	
1. Account aggregation or privacy and confidentiality	1.1. Complied with the national privacy principles and privacy law
2. Losses compensation guarantee	2.1. Liability for any claim where the user identification or password used by unauthorized persons 2.2. Compensate client when bank website get hacked/unauthorized access 2.3. Compensate client when client computer get hacked/unauthorized access 2.4. Responsibility for losses or damages or expense incurred by the customer as a result of his violation of the terms and conditions 2.5. Responsibility for all telecommunications expenses (internet services)
3. Online/Internet banking security information that the banks provide	3.1. "Customer Protection Code" document by the country's responsible authority 3.2. Threats: Hoax email, scam, phishing, spyware, virus and Trojan 3.3. Fraud Awareness 3.4. Key logger 3.5. General online security guidelines 3.6. Security alert/up-to-date issue 3.7. Provides Password security tips
Category 2: IT assistance, monitoring and support	
1. Hotline/helpdesk service availability	1.1. 24/7 customer contact center by phone 1.2. Not 24/7 customer contact center by phone 1.3. Messaging system (similar to an email) 1.4. FAQ/online support form
Category 3: Bank site authentication technology	
1. Employed encryption and digital certificate technologies	1.1. SSL encryption 1.2. Extended validation SSL certificates 1.3. Signing CA
Category 4: User site authentication technology	
1. Two-factor authentication for logon and/or for transaction verification available	1.1. Tokens 1.2. SMS 1.3. SiteKey 1.4. Not in use
2. Logon requirements	2.1. Bank credit cards number 2.2. Bank register/customer ID 2.3. Email address 2.4. Password 2.5. Other (e.g. personal code or security number) 2.6. Two-factor authentication
3. Logon failure limitation	3.1. Max. (times) 3.2. In use but does not specific maximum number of failure allowed
4. Password restriction/ requirement	4.1. Enforce good Password practice 4.2. Password length restriction (characters) 4.3. Combination of numbers and letters 4.4. Combination of upper and lower cases 4.5. Special characters 4.6. Different passwords as compared to any of previous used passwords 4.7. Automatically check password strength when creating or changing password
5. Password Recovery Method (Using ATM card number and PIN/username)	5.1. User ID, Card Number and PIN Number 5.2. Users can reset password online 5.3. Restore via ATM 5.4. SMS code 5.5. Answer Security Question 5.6. Restore via E-mail 5.7. Call customer service to complete this action
6. Transaction verification	6.1. All transactions required token/SMS 6.2. All external transactions required token/SMS 6.3. Other method e.g. password
Category 5: Internet banking application security features	
1. Automatic timeout feature for inactivity	1.1. Expiration time limit (Maximum minutes) 1.2. In use but does not specific maximum number of failure allowed
2. Session management	2.1. Session tokens 2.2. Page tokens 2.3. Clear session Cookie information after logoff or shut down the Internet browser
3. Limited default daily transfer amount to third party account/BPAY/ international transactions	3.1. Less or up to 5,000 USD 3.2. More than 5,000 USD 3.3. The default maximum daily limit transfer is vary depend on the type of the Internet banking customer 3.4. The maximum daily limit transfer may be increased with the approval by the banks 3.5. International transfer limit is different from the national transfer limit
Category 6: Software and system requirements and settings information	
1. Compatibility best with the popular Internet browsers (based on the banks information provided)	1.1. Chrome 1.2. FireFox 1.3. Internet Explorer 1.4. Netscape 1.5. Opera 1.6. Safari
2. Internet banking user device system and browser setting requirement	2.1. Operating System 2.2. Type of browser 2.3. Browser setting 2.4. Screen resolution
3. Free/paid security software/tool available to the Internet banking customers	3.1. Antivirus/anti-spyware 3.2. Internet security suite 3.3. Browser setting 3.4. Provides Internet links to security software vendor(s)

Table 6: The usability evaluation part of the framework (most of the metrics are extracted from (Zarifopoulos and Economides, 2009))

Subcategory	Metric
Category 1: Interface	
1. Design Principles	1.1. Home page is concise and clear 1.2. Effective use of white space 1.3. Effective and consistent use of color, color combination and backgrounds 1.4. Effective graphics 1.5. Aesthetics and Minimalist Design - apply appropriate visual representation of security elements and not provide irrelevant security information
2. Graphics and Multimedia	2.1. Site is visually attractive 2.2. Graphics and multimedia help the navigation 2.3. Icons are easy to understand 2.4. Not excessively used 2.5. No negative impact on loading times
3. Style and Text	3.1. Consistent use of pages style and format 3.2. Consistent use and easy to read fonts 3.3. Correct spelling and grammar 3.4. Text is concise and relevant 3.5. Purpose of site is made clear on home page 3.6. User Language - the use of plain language that users can understand with regard to security
4. Flexibility and Compatibility	4.1. Pages sized to fit in browser window 4.2. Printable versions of pages are available 4.3. Text-only version is available 4.4. Options of many available languages 4.5. Accommodation made for users with special needs 4.6. User Suitability - provide options for users with diverse levels of skill and experience in security
Category 2: Navigation	
1. Logical Structure	1.1. Intuitively progressing (proceeding) 1.2. Rational design of the content 1.3. Menus are understandable and straightforward 1.4. Sitemap is available 1.5. Consistent navigation throughout the site 1.6. Navigation bar is available
2. Ease Use of the Site	2.1. Easy to find the site 2.2. Easy to learn and navigate the site 2.3. Easy to use the navigation bar 2.4. Easy to return to main page 2.5. Easy to modify users settings
3. Ease Use of the Online Banking Pages	3.1. Easy to access complete online banking range 3.2. Separation of online banking pages from the rest pages 3.3. Separation between individual and business customers, as well among various channels
4. Search Feature	4.1. Easy to use search engine 4.2. Search engine provides accurate and useful results 4.3. Good description of search engine findings 4.4. No search engine errors
5. Navigational Necessities	5.1. No broken links 5.2. No under-construction pages 5.3. Links are clearly discernible, well labeled and defined 5.4. Clear label of current position on the site 5.5. Effective use of frames, non-frames version is available
Category 3: Content	
1. Online Banking Information	1.1. Full information about the purpose of each service 1.2. Full information about the charges 1.3. Terms and conditions are easily accessed 1.4. Full information about Technical Requirements 1.5. Familiarity programs and demo are available
2. Bank Information and Communications	2.1. Full bank information is available 2.2. Different ways for communication with the banks employees are available 2.3. Telephone and fax numbers are available 2.4. Postal and physical addresses are available
3. Advertisement	3.1. Adequate advertisement of banks services 3.2. Controlled amount of advertisements by other companies 3.3. Careful advertisement use 3.4. Effective use of advertisement techniques
4. Website Users Support	4.1. Feedback forms are available 4.2. Telephone and e-mail numbers for providing help 4.3. Round the clock support 4.4. Free or toll free telephone assistance 4.5. Security help are relevant and apparent to users
5. Competency of the Provided Assistance	5.1. Detailed information about every step 5.2. Easily understandable assistance for amateur users 5.3. Assistance regarding settings is provided 5.4. Transaction guide is provided
Category 4: Services Offered	
1. General Services	1.1. Information about banks announcements 1.2. Profile/ username/ password management 1.3. Ease use of services 1.4. Revocability - allow users to revoke security actions where appropriate 1.5. Tools such as organizer and calculator are available 1.6. Extra services such as ticket booking, shop on line, charity
2. Financial Services	2.1. Account and loan information 2.2. Credit card and check information 2.3. Loan request
3. Provided Transactions	3.1. Bill payments 3.2. Mobile phone bill or card recharge
Category 5: Reliability	
1. Registration	1.1. Easy to register 1.2. Easy to log on to the site 1.3. Adjustable customer profile is stored 1.4. E-mail request for receiving offers or information 1.5. Easy modification of users profile
2. Transaction Procedure	2.1. Foreign language support is available 2.2. Disconnection management 2.3. Actions history is available
Category 6: Technical Aspects	
1. Loading Speed	1.1. Fast loading speed of the home page as well the rest pages 1.2. Consideration of non-broadband users
Category 7: Multi-factor Authentication Methods	
1. Tokens	1.1. Hardware Tokens 1.2. Software Tokens 1.3. Easy to get the code from the device 1.4. Security and Stability 1.5. User Adoption 1.6. Total Cost of Ownership (TCO) 1.7. Replacement of the token in the event of defects
2. SMS	2.1. Multiple mobile numbers allowed (maximum)
3. Tokens	3.1. Effective use of Sitekey