Computing (2017) 99:519–535
DOI 10.1007/s00607-017-0546-9

A model for evaluating the security and usability of e-banking platforms

Abdulrahman Alarifi[1] · **Mansour Alsaleh**[1] · **Noura Alomar**[2]

Received: 13 February 2016 / Accepted: 22 February 2017 / Published online: 9 March 2017

Abstract Convenience and the ability to perform advanced transactions encourage banks clients to use e-banking systems. As security and usability are two growing concerns for e-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 e-banking systems, a dedicated security and usability evaluation model that can be used as a guide in the development of e-banking assets remains much less explored. To build a comprehensive security and usability evaluation framework, we first extract security and usability evaluation metrics from the conducted literature review and then include several other evaluation metrics that were not previously identified in the literature. We then propose a structured inspection model for thoroughly evaluating the usability and security of internal and external e-banking assets. We argue that the proposed e-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

This work extends a preliminary version presented at the 11th International Conference on Web Information Systems and Technologies (WEBIST 2015).

Electronic supplementary material The online version of this article (doi:10.1007/s00607-017-0546-9) contains supplementary material, which is available to authorized users.

✉ Noura Alomar
nnalomar@ksu.edu.sa

Abdulrahman Alarifi
aarifi@kacst.edu.sa

Mansour Alsaleh
maalsaleh@kacst.edu.sa

[1] King AbdulAziz City for Science and Technology, P.O. Box 6086, Riyadh 11442, Saudi Arabia

[2] College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia

and lack some essential and key evaluation metrics that are of particular interest to e-banking portals. In order to demonstrate the inadequacy of existing models, we use the proposed framework 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.

Keywords Security · Usability evaluation · E-banking · Online consumers trust

Mathematics Subject Classification 68N01 · 68N99 · 68N30

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. E-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 [1]. E-banking is expected to grow due to the dramatical increase in using e-commerce applications in businesses by Internet users [2]. Through e-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 [3].

Most banks in the world provide e-banking services that give customers the ability to know the details of their bank accounts and perform a variety of financial transactions irrespective of time and place boundaries. Banks have been able to reach out to millions of customers through e-banking and offer more products and a relatively better, convenient and flexible banking experience relative to traditional, fixed-location branches. On the flip side, a set of security and privacy issues have shown to endanger the utilization of such e-banking services [4,5]. While security and convenient access to bank accounts through online banking portals are claimed by most bank organizations which allows their customers to commit financial transactions online, achieving an acceptable balance between usability and security of banking software systems remains an open question [6,7].

Sixty-eight percent of consumers with regular Internet access and a bank account used e-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 [8].

In this paper, we investigate existing frameworks and models for evaluating e-banking security and usability. 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 e-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 e-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 interfaces of the e-banking portals 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 e-banking portals, but also during the design and development phases. We anticipate that, should it be built particularly for e-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. We also propose a structured evaluation model that utilizes a number of subjective and objective evaluation approaches for systematically addressing the trade-offs between security and usability considerations.

Contributions. The contributions of this work can be summarized as follows.

1. E- Banking Security and Usability Evaluation Framework (EBSUEF). Built on top of existing frameworks and for the purpose of evaluating the publicly accessible assets of e-banks, we propose a framework that covers 13 different security and usability categories and more than 160 metrics.
2. Case study on the utilization of EBSUEF. We utilize the EBSUEF for comparatively evaluating the publicly accessible e-banking systems of five banks in the MENA region from usability and security perspectives.
3. Hybrid security and usability evaluation model. We propose a systematic evaluation model that could be utilized for regularly assessing the security and usability of internal and external e-banking assets, streamlining the identification of security and usability shortcomings and assisting decision makers in resolving usability and security conflicts.

Organization. The remainder of the paper is organized as follows. In the next section, we present an e-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. We then propose a model for managing the usability-security conflicts and discuss the usability and security considerations of e-banking systems in Sects. 4 and 5, respectively. The related literature is then summarized in Sect. 6. Section 7 concludes.

2 EBSUEF: e-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 [9]. We have also included key usability features from MoBEF, a banking portal evaluation framework [10]. The resulted framework includes the most essential features that should be considered when assessing the security and usability of e-banking systems. It takes into consideration all the main security and usability factors from the first visits of customers to e-banking portals and up to the successful completion of financial transactions.

The framework consists of two main 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 e-banking portals.

2.1 Security evaluation metrics

The security evaluation part of the framework consists of 72 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

Table 1 Number of metrics for each security and usability categories of the EBSUEF

Security categories	# of metrics	Usability categories	# of metrics
1. General online security and privacy information to the Internet banking customers	13	1. Interface	22
2. IT assistance, monitoring and support	3	2. Navigation	23
3. Bank site authentication technology	3	3. Content	22
4. User site authentication technology	29	4. Services offered	11
5. Internet banking application security features	10	5. Reliability	8
6. Software and system requirements and settings information	14	6. Technical Aspects and multi-factor authentication methods	11

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 1 in Appendix A.[1]

2.2 Usability evaluation metrics

The usability of security features in e-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 [11–13].

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 1 for a summary of the used usability metrics; detailed description of the used metrics is shown in Table 2 in “Appendix A). The interface is evaluated against several design principles in order to maximize user task completion and minimize interfering. Also, we expect the usability evaluation criteria presented in the EBSUEF to help in examining the presentation of visual interface elements (e.g., graphics and colors). Furthermore, the correct presentation of the text and language, and the adjustment of web pages according to various user browsing scenarios can be examined using the proposed framework. Using the EBSUEF, the ability of e-banking users to navigate through the e-banking application can also evaluated from convenience and easiness perspectives. For example, the structure and organization of menus, the effectiveness of search features and the visibility of navigation options are all essential usability factors that could have positive or negative effects on user experience.

When accounting for usability in e-banking systems, the clarity, structure and comprehensiveness of information available in these systems are also of the important considerations. Providing up-to-date information that sufficiently explain how to use e-banking systems and how to take advantage of the offered investment, accounting and

[1] Appendix 1 can be found in the supplementary material of this paper.

financial services is of extreme importance. 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 e-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 Sects. 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 in Appendix A 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 compare 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 [2] 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

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

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 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 banks included in our evaluation have followed acceptable design principles in implementing their web portals and have made a good utilization of colors, white space and images. Graphics and rich media content are used moderately to make their websites easier to navigate and more attractive without having negative impact on loading time. Furthermore, the banks have shown a consistent use of text and page format as well as the use of language that can be understood by users of e-banking systems. Among the web portals of the five banks, we also noticed variations in the capability of web pages to fit browser windows; 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 people with disabilities, nor provided options for clients with various levels of skill and technical knowledge. The web portals of the five banks can be easily 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 provides guidance on how to effectively utilize e-banking services and navigate

through the banks' web portals; however, we noticed that the evaluated systems are built on the assumption that users have to read various documents to obtain all required information. Also, the five banks utilized their e-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 A hybrid model for evaluating the security and usability of e-banking systems

Due to the importance of maintaining highly secure yet usable e-banking systems, we propose a lightweight model that utilizes the EBSUEF (see Sect. 2) for addressing the interplay between security and usability related considerations during or after

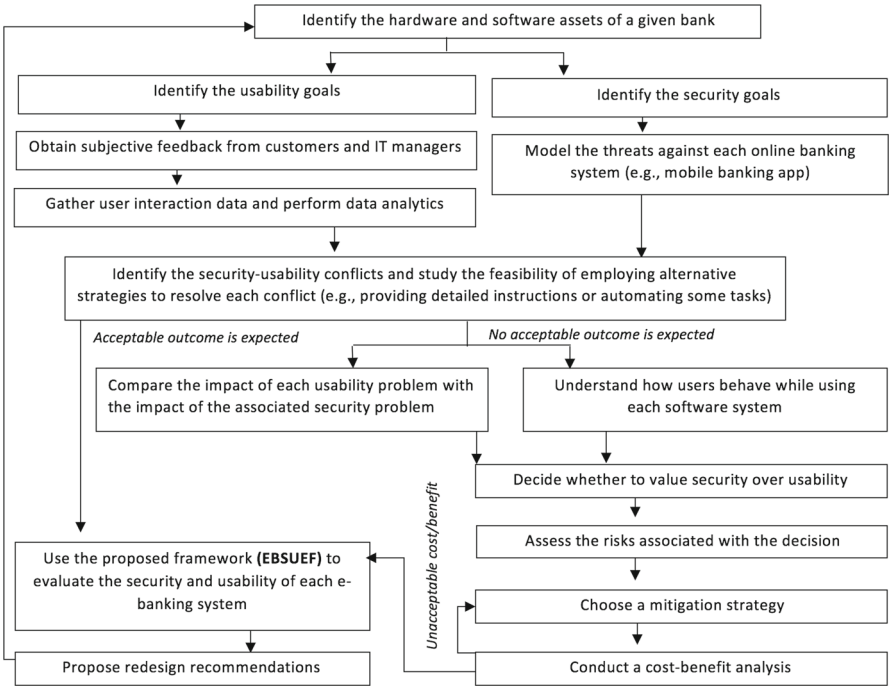

Fig. 1 The proposed security and usability evaluation model

releasing e-banking software systems (see Fig. 1). The proposed model is derived based on a careful study of the approaches that could facilitate addressing the trade-offs between security- and usability-related considerations in e-banking systems. As usability and security changes in e-banking contexts could result in undesirable effects to many business activities in bank organizations, the phases of the proposed model were designed on the basis of helping decision makers in assessing the impact of all foreseeable risks and weighing the costs and benefits of all usability or security related changes before investing considerable resources on changes that could result in costly errors for the banks in question. Contrary to other previous proposals in the literature, our model focuses on encompassing all necessary usability and security-related considerations from the very early stages of the software development lifecycle rather than dealing with them as add-ons at the later development stages. To minimize the effects of any negative consequences of any planned conflict-resolution strategy and ensure that usability and security considerations are fully integrated into the development and maintenance processes, the proposed model also encourages making continuous assessment of the usability and security of e-banking systems and iteratively resolving any potential conflicts as efficiently and effectively as possible. The proposed model is also expected to help decision makers build thorough understanding of the current usability and security situations of e-banking systems and implement appropriate conflict resolution strategies accordingly while ensuring that appropriate resources are invested for each selected security or usability-related software change.

The structure of the proposed model encourages its incorporation with other security or usability evaluation frameworks. Because e-banking systems vary in the features that they provide and due to the fact that thoroughly evaluating the security and usability of e-banking systems requires taking into consideration many internal and external factors and studying the correlations between these factors [14,15], we believe that following our model would help in thoroughly evaluating the usability and security of publicly accessible assets as well as the internal hardware and software assets of online banks. Our model focuses on strengthening the security and usability of e-banking systems by incorporating a number of security and usability assessment methods into one systematic evaluation model. By considering the organizational and external factors that might impact the usability and security levels of e-banking software solutions, we believe that applying our model in a regular basis would help in iteratively enhancing the security of the evaluated systems without sacrificing their usability. It is also worth noting that the structure of the proposed model allows tailoring it to work as a change management process as utilizing it is expected to facilitate recognizing the usability and security shortcomings of e-banking systems and aligning them with the inter-organizational factors of the banks in question. We also expect applying the proposed model to simplify the administration of usability- or security-related changes in e-banking systems, assist in identifying the risks, costs and benefits associated with implementing these changes and inspire the design of appropriate strategies for minimizing the negative impact of change failures in the banks in question. We also believe that following the steps of the proposed model would contribute to detecting the usability and security problems early and addressing the discovered issues in efficient and cost-effective ways. This is because our model encourages the utilization of any usability or security evaluation method and at the same time helps decision makers in systematically assessing the costs, benefits, risks and consequences of their choices. In this paper, due to the difficulty of accessing all the hardware and software assets of banking organizations and the sensitivity of information processed in these systems, evaluating the effectiveness of the proposed model is only restricted to some publicly accessible e-banking assets (see Sect. 3).

5 Discussion

By comprehensively evaluating the direct and indirect factors that might influence the security of e-banking systems or affect the end user experience, we believe that the proposed model would help decision makers in gaining a comprehensive view of the security and usability states of the evaluated systems and identifying the conflicts that should be addressed. Our model also emphasizes on the importance of involving usability engineering experts and using a combination of usability evaluation methods to clearly understand the usability flaws of the evaluated systems. The detected usability shortcomings can be then classified according to their severity levels in order to start by addressing the ones that would highly impact convenience of target users [16]. For e-banking systems, evaluating the usability of authentication methods is also essential because they are considered as entry points to these systems and the usability of these methods directly impacts the security of the systems in question [17–19]. Decision makers can utilize a number of usability evaluation methods to analyze users' interac-

tions with their systems, measure the task completion rates, assess the complexity of the functionality provided by their systems and understand the factors that might degrade the usability levels of the evaluated systems (e.g., the visibility and readability of user interface elements [16,20]). For instance, eye tracking techniques can be employed for analyzing the navigation behaviors of end users and extracting data related to the their viewing patterns [16]. Usability engineers could also take advantage of the think-aloud protocols to elicit users' feedback while they are interacting with the evaluated systems and gain sufficient understanding of the cognitive effort that is consumed for making payments, withdrawing or depositing funds or performing any other e-banking transactions [16,21]. Established heuristics evaluation approaches could also be utilized for finding usability problems in the evaluated user interfaces and deciding on the number of usability engineering experts who should be involved and the number of subjective ratings that should be collected from end users (e.g., [22–24]).

From a security perspective, modeling the threats against each e-banking system, the employed user authentication methods, the reused software components and the external systems that interact with the evaluated banking solutions at early stages would also play a major role in discovering the security vulnerabilities that might be exploited by attackers. Exploring the socio-cultural factors of target users and understanding the reasons behind adopting insecure e-banking behaviors is also important. Further, studying the cultural factors by taking advantage of well-known theories (e.g., Hofstede's theory of cultural dimensions [25]) and conducting user studies would also help in understanding whether target users perceive security as more important than usability or vise versa [26,27]. For example, a number of researchers have found that Australian users value convenience over security [3,28]. Further, after investigating the usability characteristics of e-banking systems provided by three banks in the Arab region, Alhmoud et.al have also recommended implementing culturally-oriented design approaches that can be followed through all the phases of the software development life cycle [29]. The essential role of human factors in designing usable software systems is also emphasized in [30] and the authors have suggested considering the cognitive abilities of target users in order to improve the effectiveness of the evaluated systems.

It has been suggested to treat usability and security as complementary to each other and tie them together from the early phases of the development process [31–34]. Three approaches are suggested in [35] for balancing the security and usability trade-offs. Designers of e-banking software solutions can instruct the users how to complete tasks, simplify some tasks by automating them or improve users' awareness of the security consequences of their actions [35]. It is also recommended to minimize users' mental overhead by reducing the number of instances in which a user is required to take security related decisions and increase the transparency of e-banking systems by allowing users to visualize their security states in user-friendly ways [31,36]. The design principles presented in [33] have also highlighted the importance of clarifying the consequences of any security related decision, maximizing the security of input and output communication mediums and ensuring that system elements, services and actors can be easily identified. In our model, in case of the infeasibility of resolving the conflicts by employing any of the above mentioned strategies, we encourage designers to assess the risks associated with each security or usability problem by measuring their severity levels and probabilities of occurrences. We also suggest listing all the

possible mitigation strategies of the expected risks and evaluating the costs and benefits of adopting each one.

Architectural Considerations. Before taking any security or usability related decisions, it is also essential to identity the changes that demand architectural support and determine whether the software architectures of the evaluated e-banking systems can accommodate these changes in cost-effective ways. As usability and security are of the most important attributes that reflect the quality of e-banking software solutions, software architectures of e-banking systems should be quantitatively and qualitatively analyzed for their support of usability and security to avoid making extensive refactoring work at the late stages of the development life cycle or after deployment. In multi-layered software architectures, some usability or security related decisions require major software restructuring work whereas others could be addressed by making simple modification to user interface elements [37]. To fulfill the security requirements of e-banking systems, multiple layers of security could be architected which might be comprised of authentication mechanisms, firewalls, encryption methods, etc [38]. Because of the size of e-banking systems, we believe that taking late security or usability related decisions would mostly be constrained by the complexity of the corresponding software architecture and which could be costly to refactor. Researchers found that more than 60% of software maintenance costs are often spent on fixing usability issues [39,40]. Thus, instead of appending usability or security related evaluations after deploying e-banking software systems, the proposed model encourages following a forward-engineering approach in that software architectures should be constantly assessed for their support of usability and security from the early stages of the software development life cycle [41,42].

Software architects could employ scenario-based assessments, take advantage of architecture simulation and prototyping tools or develop mathematical models to assess the extent to which the evaluated architectures satisfy the required usability and security considerations [42,43]. At the architectural design stage and by considering the trade-offs between security and usability, decision makers could identify the required usability attributes and link them to the design solutions and architectural patterns that could help in addressing the usability requirements early in the development process (e.g., using the Software Architecture Usability (SAU) framework [44,45]). Beside the usability considerations, the choice of proper architectural styles for e-banking systems should be based on the assumption that multiple layers of security must be implemented for protecting critical e-banking assets [46]. Thus, when deciding on the ways to organize software components and model the interfacing between these components and external systems, careful attention should be paid to taking architectural decisions that would help in maintaining highly confidential communications and preventing any form of unauthorized access to e-banking assets [46]. As architectural design patterns vary in their support for security and usability, software architects could prioritize their security and usability requirements and apply some modifications to their chosen patterns to support the desired quality attributes. These changes might include adding new software components, replicating existing ones, dividing large components into smaller ones, or modifying the structures of the chosen architectural patterns [47]. However, since some usability considerations might degrade

the security of some e-banking systems and vice versa, a careful analysis of security-usability trade-offs should be conducted before applying any architectural changes. For instance, although keeping redundant copies of system data might significantly affect the responsiveness of e-banking systems, this would increase the risk of exposing protected data and thus degrading the security of the corresponding systems [47,48]. To build maintainable e-banking systems and reduce the number of software components that could be affected once a security or usability related decision is taken, architectural designers are also encouraged to choose architectural design patterns that could assist in reducing the level of coupling between software components and use software quality metrics for measuring the overall complexity of these systems [42]. Software architects could also analyze the data flow between software and hardware components of e-banking systems, the flow of control between these components and the context in which the designed systems operate in order to determine the architectural implications of each usability or security related decision [49]. To build software architectures that support usability and security, it has also been suggested to consult HCI experts and information security professionals and to consider stakeholders perspectives early in the architectural design process [50].

6 Related work

Prior research efforts have addressed the factors that affect the usability or security of software systems deployed in many contexts (e.g., financial institutions and educational settings [51–53]). Other studies have emphasized on aligning the usability and security considerations by either following user-centered design approaches that tailor the functionality of software solutions to match the demands of target users, attempting to integrate both of them into the software development life cycle or proposing theoretical guidelines for addressing the conflicts [31,33,34,54,55]. The evaluation model proposed in this paper (see Sect. 4) encourages the incorporation of security and usability aspects from the early stages of the software development life cycle and motivates system designers to regularly perform security-usability analyses to constantly improve the usability and security sides of their e-banking systems. The model also stresses the importance of considering the human, social and cultural factors in cases where designers should decide whether to weigh convenience or security over the other. Thus, we believe that the results presented in previous studies complement our work and might help in understanding the specific usability or security properties that should be given more attention by designers of e-banking systems.

Some researchers have focused on investigating the usability and security of user authentication methods employed in banking organizations [7,17,18,56,57]. For instance, Mihajlov et. al proposed a framework for quantitatively examining a number of security and usability dimensions of authentication schemes [57]. Although the evaluation approach presented in [57] might help in comparing the effectiveness of authentication methods, its underlying assessment criteria ignores the interrelationships between security and usability elements. From the perspectives of e-banking customers, Althobaiti and Mayhew have studied the security and usability related perceptions of more than 300 users and found that tokens were perceived as secure

whereas passwords were perceived as difficult to remember [17]. Focusing on the security-usability trade-offs related to two factor authentication, the experimental results presented in [56] show that the surveyed participants were mostly prepared to value convenience over security. Mairiza and Zowghi have also proposed to address the usability-security conflicts by utilizing ontologies to model the relationships between security and usability requirements and thus simplifying the identification of potential conflicts and proposing the appropriate mitigation strategies accordingly [55]. Other studies have proposed frameworks for addressing the security or usability considerations without comprehensively studying the effects of integrating both of them into one e-banking system [51,58–61]. Clearly, previous research attempts have either explored individuals' online banking attitudes, combined usability and security metrics into one evaluation framework or studied the possible ways of implementing usable and secure systems. However, there is clearly a lack of a comprehensive model that can be used as a basis for identifying the usability and security drawbacks of e-banking systems and determining the considerations that should be augmented into the analysis, design and evaluation phases of these systems.

The impact of modeling the threats against e-banking applications on discovering the security vulnerabilities at very early stages and addressing the security complexities of e-banking systems has also been highlighted in prior work [54]. Uusitalo and Catot have also pointed out that estimating the direct and indirect costs of security attacks would significantly help in discovering the areas that should be improved and thus simplifying the process of regularly updating e-banking systems to address these threats [53]. Further, Ramzan and Pervais have suggested assessing and prioritizing the risks against online banks from multiple perspectives including the types of transactions, the sensitively of information and the potential effects on the hardware and software resources of the corresponding banks [7]. Furthermore, Braz et. al have also proposed a model called Security Usability Symmetry (SUS) for addressing the correlations between security and usability factors by comparing the severity levels of the examined factors [13]. Although the effectiveness of SUS has been demonstrated in [13], solely relying on the ratings obtained from usability or security experts might not necessary lead to taking correct decisions to address the usability-security conflicts. In our usability-security inspection model (see Sect. 4), we propose to regularly analyze users' interactions with e-banking systems and evaluate these systems based on a comprehensive set of subjective and objective measures using the EBSUEF framework (see Sect. 2). Similar to our hybrid evaluation model, Flechais et. al have proposed a structured model called AEGIS that gives a significant attention to assessing the costs, benefits and risks of security or usability related decisions at every stage of the SDLC [62]; however, we believe that specifying the metrics that should be considered at each stage is necessary for ensuring the comprehensiveness of a security-usability evaluation model.

7 Concluding remarks

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

model is indeed a necessity. Because security and usability 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. This paper proposes a structured usability and security evaluation model that takes into consideration the architectural, functional and business sides of e-banking software solutions. While focusing on iteratively enhancing the quality of e-banking systems, our model is expected to assist decision makers in resolving security-usability conflicts early in the development process. Structuring e-banking systems, deciding how software components should communicate and exchange data and choosing which architecture evaluation approaches to use are all essential for designing software architectures for usability and security. The proposed model encourages early identification of security or usability requirements that would demand architectural support while developing or refactoring e-banking software systems. This would significantly help in analyzing the trade-offs between these two important software quality attributes early in the development process which would therefore lead to reducing subsequent maintenance and refactoring costs. 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. For e-banking systems, we also believe that there is still a demand for researching how to align software architectural design considerations with usability and security requirements.

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

1. YeeLoong Chong A, Ooi K, Lin B, Tan B (2010) Online banking adoption: an empirical analysis. Int J Bank Mark 28(4):267–287
2. Laukkanen P, Sinkkonen S, Laukkanen T (2008) Consumer resistance to internet banking: postponers, opponents and rejectors. Int J Bank Mark 26(6):440–455
3. Lichtenstein S, Williamson K (2006) Understanding consumer adoption of internet banking: an interpretive study in the Australian banking context. J Electron Commer Res 7(2):50–66
4. Weir CS, Douglas G, Richardson T, Jack M (2010) Usable security: user preferences for authentication methods in ebanking and the effects of experience. Interact Comput 22(3):153–164
5. Mannan M, van Oorschot PC (2008) Security and usability: the gap in real-world online banking. In: Proceedings of the 2007 workshop on new security paradigms. ACM, pp 1–14
6. Casalo LV, Flavián C, Guinalíu M (2007) The role of security, privacy, usability and reputation in the development of online banking. Online Inf Rev 31(5):583–603
7. Pervaiz FRT. Online banking security
8. Aladwani AM (2001) Online banking: a field study of drivers, development challenges, and expectations. Int J Inf Manag 21(3):213–225
9. Subsorn P, Limwiriyakul S (2011) A comparative analysis of the security of internet banking in Australia: a customer perspective. In: Proceedings of the 2nd international cyber resilience conference, pp 70–83
10. Zarifopoulos M, Economides AA (2009) Evaluating mobile banking portals. Int J Mobile Commun 7(1):66–90
11. Gutmann P, Grigg I (2005) Security usability. Secur Priv IEEE 3:56–58

12. Seffah A, Donyaee M, Kline R, Padda H (2006) Usability metrics: a roadmap for a consolidated model. J Softw Qual 14(2):159–178
13. Braz C, Seffah A, M'Raihi D (2007) Designing a trade-off between usability and security: a metrics based-model. In: Proceedings of the INTERACT07. Springer, NewYork, pp 114–126
14. Möckel C (2011) Usability and security in eu e-banking systems-towards an integrated evaluation framework. In: Applications and the internet (SAINT), 2011 IEEE/IPSJ 11th international symposium on IEEE, pp 230–233
15. Just M, Aspinall, D (2012) On the security and usability of dual credential authentication in UK online banking. In: Internet technology and secured transactions, 2012 international conference for IEEE, pp 259–264
16. Al-Wabil A, Al-Khalifa H (2009) A framework for integrating usability evaluations methods: the mawhiba web portal case study. In: Current trends in information technology (CTIT), 2009 international conference on the IEEE, pp 1–6
17. Althobaiti MM, Mayhew P (2014) Security and usability of authenticating process of online banking: user experience study. In: Security technology (ICCST), 2014 international carnahan conference on IEEE, pp 1–6
18. Weir CS, Douglas G, Carruthers M, Jack M (2009) User perceptions of security, convenience and usability for ebanking authentication tokens. Comput Secur 28(1):47–62
19. Alomar N, Alsaleh M, Alarifi A (2017) Social authentication applications, attacks, defense strategies and future research directions: a systematic review. IEEE Commun Surv Tutor. http://ieeexplore.ieee.org/abstract/document/7814222/
20. Becker S, Mottay FE et al (2001) A global perspective on web site usability. IEEE Softw 18(1):54–61
21. Jääskeläinen R (2010) Think-aloud protocol. Handb Transl Stud 1:371–373
22. Nielsen J, Landauer TK (1993) A mathematical model of the finding of usability problems. In: Proceedings of the INTERACT'93 and CHI'93 conference on human factors in computing systems. ACM, pp 206–213
23. Nielsen J (1994) Estimating the number of subjects needed for a thinking aloud test. Int J Hum Comput Stud 41(3):385–397
24. Nielsen J (1994) Enhancing the explanatory power of usability heuristics. In: Proceedings of the SIGCHI conference on human factors in computing systems. ACM, pp 152–158
25. Hofstede G (1993) Cultural constraints in management theories. Acad Manag Exec 7(1):81–94
26. Yoon HS, Steege LMB (2013) Development of a quantitative model of the impact of customers personality and perceptions on internet banking use. Comput Hum Behav 29(3):1133–1141
27. Alsaleh M, Alomar N, Alarifi A (2017) Smartphone users: understanding how security mechanisms are perceived and new persuasive methods. PloS One
28. Nielsen A (2005) Online banking continues despite security concerns. ACNielsen, NewYork
29. Alhumoud S, Alabdulkarim L, Almobarak N, Al-Wabil A (2015) Socio-cultural aspects in the design of multilingual banking interfaces in the arab region. In: Human–computer interaction: users and contexts. Springer, NewYork, pp 269–280
30. Al-Ageel N, Al-Wabil A, Badr G, AlOmar N (2015) Human factors in the design and evaluation of bioinformatics tools. Proc Manuf 3:2003–2010
31. DeWitt AJ, Kuljis J (2006) Aligning usability and security: a usability study of polaris. In: Proceedings of the second symposium on usable privacy and security. ACM, pp 1–7
32. Boehm BW (1988) A spiral model of software development and enhancement. Computer 21(5):61–72
33. Yee K-P (2002) User interaction design for secure systems. Springer, NewYork
34. Kainda R, Flechais I, Roscoe A (2010) Security and usability: analysis and evaluation. In: Availability, reliability, and security, 2010. ARES'10 international conference on IEEE, pp 275–282
35. Hertzum M, Jørgensen N, Nørgaard M (2004) Usable security and e-banking: ease of use vis-a-vis security. Aust J Inf Syst 11(2):52–65
36. Dourish P, Redmiles D (2002) An approach to usable security based on event monitoring and visualization. In: Proceedings of the 2002 workshop on new security paradigms, ACM, pp 75–81
37. John BE, Bass L (2001) Usability and software architecture. Behav Inf Technol 20(5):329–338
38. Vrancianu M, Popa LA et al (2010) Considerations regarding the security and protection of e-banking services consumers interests. Amfiteatru Econ J 12(28):388–403
39. Landauer TK (1995) The trouble with computers: usefulness, usability, and productivity, vol 21. Taylor & Francis, Milton Park

40. Folmer E, Van Gurp J, Bosch J (2003) A framework for capturing the relationship between usability and software architecture. Softw Process Improv Pract 8(2):67–87
41. Juristo N, Lopez M, Moreno AM, Sánchez MI (2003) Improving software usability through architectural patterns. In: ICSE workshop on SE-HCI. Citeseer, pp 12–19
42. Abowd G, Bass L, Clements P, Kazman R, Northrop L (1997) Recommended best industrial practice for software architecture evaluation. Technical report, DTIC document
43. Folmer E, van Gurp J, Bosch J (2003) Scenario-based assessment of software architecture usability. In: ICSE workshop on SE-HCI, Citeseer, pp 61–68
44. Folmer E, Gurp JV, Bosch J (2003) Investigating the relationship between usability and software architecture. Software process improvement and practice. Wiley, Colorado
45. Folmer E, Bosch J (2010) Experiences with software architecture analysis of usability. Web engineering advancements and trends: building new dimensions of information technology: building new dimensions of information technology, p 177
46. Sommerville I (2011) Software engineering. Addison-Wesley, Boston
47. Kassab M, El-Boussaidi G, Mili H (2012) A quantitative evaluation of the impact of architectural patterns on quality requirements. In: Software engineering research, management and applications 2011, Springer, NewYork, pp 173–184
48. Bass L, Clements P, Kazman R (2003) Software architecture in practice. Addison Wesley, Boston
49. Barbacci MR, Klein MH, Weinstock CB (1997) Principles for evaluating the quality attributes of a software architecture, Technical report, DTIC document
50. Raza A, Capretz LF (2015) Usability as a dominant quality attribute. arXiv preprint arXiv:1508.06195
51. Jeng J (2005) Usability assessment of academic digital libraries: effectiveness, efficiency, satisfaction, and learnability. Libri 55(2–3):96–121
52. Diniz E, Porto RM, Adachi T (2005) Internet banking in Brazil: evaluation of functionality, reliability and usability. Electron J Inf Syst Eval 8(1):41–50
53. Uusitalo I, Catot JM, Loureiro R (2009) Phishing and countermeasures in spanish online banking. In: Emerging security information, systems and technologies, 2009. SECURWARE'09. Third international conference on IEEE, pp 167–172
54. Möckel C, Abdallah AE (2010) Threat modeling approaches and tools for securing architectural designs of an e-banking application. In: Information assurance and security (IAS), 2010 sixth international conference on IEEE, pp 149–154
55. Mairiza D, Zowghi D (2010) An ontological framework to manage the relative conflicts between security and usability requirements. In: Managing requirements knowledge (MARK), 2010 third international workshop on IEEE, pp 1–6
56. Gunson N, Marshall D, Morton H, Jack M (2011) User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. Comput Secur 30(4):208–220
57. Mihajlov M, Jerman-Blazic B, Josimovski S (2011) A conceptual framework for evaluating usable security in authentication mechanisms-usability perspectives. In: Network and system security (NSS), 2011 5th international conference on IEEE, pp 332–336
58. Nayebi F, Desharnais J-M, Abran A (2013) An expert-based framework for evaluating ios application usability. In: Software measurement and the 2013 eighth international conference on software process and product measurement (IWSM-MENSURA), 2013 joint conference of the 23rd international workshop on IEEE, pp 147–155
59. Hutchinson D, Warren M (2003) Security for internet banking: a framework. Logist Inf Manag 16(1):64–73
60. Sivaji A, Abdullah MR, Downe AG, Ahmad WFW (2013) Hybrid usability methodology: integrating heuristic evaluation with laboratory testing across the software development lifecycle. In: Information technology: new generations (ITNG), 2013 tenth international conference on IEEE, pp 375–383
61. Alomar N et al (2016) Usability engineering of agile software project management tools. In: International conference of design, user experience, and usability. Springer, Cham. http://link.springer.com/chapter/10.1007/978-3-319-40409-7_20
62. Flechais I, Sasse MA, Hailes S (2003) Bringing security home: a process for developing secure and usable systems. In: Proceedings of the 2003 workshop on new security paradigms. ACM, pp 49–57