I.J. Information Technology and Computer Science, **2016, 5, 72-80**
Published Online May 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2016.05.08

Usability and Security in User Interface Design: A Systematic Literature Review

Ugochi Oluwatosin Nwokedi
School of Computing and Technology
Asia Pacific University of Technology & Innovation (APU), Bukit Jalil, 57000, Kuala Lumpur, Malaysia
E-mail: ugobelle@gmail.com

Beverly Amunga Onyimbo and Babak Bashari Rad
School of Computing and Technology
Asia Pacific University of Technology & Innovation (APU), Bukit Jalil, 57000, Kuala Lumpur, Malaysia
E-mail: beverlyamunga@gmail.com, dr.babak.basharirad@apu.edu.my

***Abstract*—**Systems carry sensitive data where users are involved. There is need for security concern for the modern software applications. We can term them as 'untrusted clients'. Internet usage has rapidly grown over the years and, more users are opening their information system to their clientele, it is essential to understand users' data that need protecting and to control system access as well and the rights of users of the system. Because of today's increasingly nomadic lifestyle, where they allow users to connect to information systems from anywhere with all the devices in the market, the users need to carry part of the information system out of the secure infrastructure. Insecurity in user interfaces is caused by user ignoring functionalities in the system where some are not only a threat but can harm the system e.g. leaving network services active even though the user does not need them, or when a user is having little or no information of the available security measures. This research paper aims critically address through a review of existing literature, the importance of balance or trade-off between usability and the security of the system. Systematic review method involved a physical exploration of some conference proceedings and journals to conduct the literature review. Research questions relating to usability and security were asked and the criteria for usability and security evaluations were identified. This systematic literature review is valuable in closing the gap between usability and security in software development process, where usability and security engineering needs to be considered for a better quality end-user software.

***Index Terms*—**Usability, Security, Authentication, User Interface Design, Usability and Security engineering, Quality Criteria.

I. Introduction

Over the past few years, human interaction design had become a growing topic as users are being focused on in every application that is presently designed. Now, security issues are increasing with developers having to rework some of the programs, which have already been designed [1]. While using a particular system, users tend to ignore other activities that might be taking place until they are faced with one challenge or the other. An example, which has been reported, is that some applications, which contain multimedia features, have the ability to take snapshots or recordings of the user without his/her knowledge, thereby encroaching into user's privacy [2].

Now that the question of security in user interface has risen what should be the appropriate answer? This paper seeks to evaluate the adoption of security practices in user interface. It addresses both user interface and security issues together by talking about security mechanisms e.g. Firewall protecting computer, use of security protocols for a website and use of authentication mechanisms in protecting user data. More focus is on usability in a perspective concentrating on the achievement of specific user goals in regards to the environment [3]. Interface Usability is a requirement for security of the interface since it is the main platform that users use to interact with the system. As Cranor & Buchler [4] vivid explained, usability and security are expected to go "hand in hand". An analysis on the presently existing approach with research questions trying to find a balance between the usability and security, criterions used to evaluate system usability, the connection between security criteria and usability criteria in regard to quality. Several conditions were used as criteria for this research, they include: (1) the focus was usability and security of user interface and specifically in authentication mechanism and (2) analysis were focused on studies been done in journals or conference proceedings on the subject matter.

This paper is prepared with the following sections: The first section provides a brief introduction. The second section contains a literature review. The third section provides answers and discusses research questions presented. Finally, the fourth section provides a conclusion of the discussed subject and fifth suggests recommendation for future work.

II. Literature Review

This study examines the existing literature and adaptation of security practices in user interface design. There are two ways of looking at this issue; for the security perspective which involves securing the user interface using security mechanisms such as a firewall protecting computer, using security protocols for a website or providing authentication mechanisms such as passwords and PIN to protect user data. This concern with security seems to focus more data access such as using authentication or preventing malware from affecting user interface. However, there is the usability perspective, which is described “as the effectiveness, efficiency and satisfaction with which specified users can achieve specified goals in specified environment” [3]. Security and privacy supervision activities were previously left to system administrators who are experts and could devote time to studying the use of complex user interface, but currently, these responsibilities are progressively left to the end-users [1].

In user interface design, the usability of the interface is one of the main goals that needs to be achieved. This means that usability will also be a requirement for security of the interface that users utilize to communicate with the system. Therefore, major efforts need to be made in order to improve the design of the user interface by merging security with the usability principle which had been defined by Norman (1994). The topic of security in user interface has not been explored much and only a few studies have been carried out in order to improve the usability of user interface and protect the users [4]. The behavior or reaction of the users towards an interface is one of the key things which are studied in Human Computer Interactions (HCI). For example, when the user experiences any form of discomfort while using the interface, it tells a lot on the usability of that particular system [5]. Scenarios for both security and usability are widely used by experts for various purposes. From the perspective of usability, how users use software to carry out task so as to achieve their target goal or objective is the key concern while from the perspective of security how system can prevent an attacker from gaining access is the principal goal. Procedures from secure software engineering and usability engineering, respectively can influence qualifying risk or developing the effectiveness of user tasks. Developers have this belief that their understanding of user objective and expectations contradicts the necessity for interaction design or their understanding of the system’s risk and justifying controls contradicts the necessity for performing security study. Because of these seeming contradictions, developers may have the feeling that much as security and usability engineering methods are valuable, they do not carry a justifiable reward [6].

A. Usability Engineering

The term Usability engineering can be described as a method of how systems are developed and verified using experimental methods to accomplish efficiency, effectiveness and satisfaction for particular users that perform definite objective in a certain environment [7]. The definition of Usability Engineering connects a system’s usability to particular requirements, and users. It takes into consideration adding end user’s view with the developed product [32]. Usability experiments offer impartial and personal information for the design and engineering of technology clarifications that are appropriate for a given goal. The purpose is to establish suitable trade-offs between satisfaction and performance methods. The principles of usability engineering are becoming commonly used in developing security solutions and are appropriate for examining the possibilities of some certain types of authentication such as to factor in an e-Banking scenario.

Usability engineering highlights information acquired on the basis of hands-on involvement with substitute interface, concerning illustrative users carrying out normal functions in clear situations. The importance of a usability approach is to ask questions related to the perspective of usage, after undergoing the process directly [8].

B. Security Engineering

Security engineering is not restricted to just building secure software. It involves the proper integration of security activities and policies into software design. The term security engineering defines the several activities which can be based on the different phases of engineering and life-cycle. To integrate the security into software development process may seem not to be an easy job and the evaluation of security can be even viewed as such [33]. The essential universal opinion on security in engineering procedure has to study the complete dissimilar steps in the development of software. The phases of security engineering involve the identification of security requirements followed by software security design decisions. These choices are generally based on threat modeling and risk analysis and thereafter, security testing is carried out as well as maintenance so as to preserve security properties and security stages of a system [9].

C. Related Works

Usability-only evaluations approaches are not wholly suitable for assessing systems which are centered on security. As noted by Mihajlov, et al. [10], many studies lack the demonstration of negative properties assessment that arises when usability is initiated in security. They seem to focus more on the user experience and user interface, but additional studies into the behavior or reaction of the user toward an attack are necessary in order to come up with a way to understand and better develop secure interface. Some of these attacks include financial fraud, the internet, and other associated malicious occurrences. An example of systems that take this into consideration is an e-Banking system where a much-protected infrastructure is a very crucial issue that should not be taken for granted and at the same time has to deliver a high level of usability to its large number of incompetent users. Most research studies examine the relationship between usability and security as in the case of e-Banking which had depended upon old usability research approaches. The study of Mockel [11] argued that existing usability evaluation approaches do not fully justify the reason for the unique nature of protected applications and software. For this reason, the adaptation of usability approaches by researchers when applied to the field of human-computer interactions is debatable, taking into consideration only the stability and simplicity of the system while dwindling its security.

There has to be a trade-off between usability and security. According to Möller et al [3], the reason why users fail to use security systems as it best should be used is because security systems fail to incorporate usability in their design [3]. Sometimes users may not understand the seriousness of a threat and thereby downplay it because they would not want to be obstructed from what they were using the system for at the time. User interfaces should address security as well as usability as users have to, for example, balance functionality and the system security as well as privacy preferences by using the mechanisms already built into the system [12]. Inasmuch as security is meant for protecting people, if it de-emphasizes usability, harm may be done to user of the system as found in medical information systems which carry sensitive data [13] (check the correctness of this statement as there seem to be elements of contradiction unless you have to expound it). Hence, the balance between the two is very crucial considering the user safety.

Previous researches have been carried out using different approaches to assess the trade-off in usability and security. An experiment approach carried out by Gunson et al. [14] on automated telephone banking show that the perceptions of security was boosted when an extended authentication procedure was added, but at the expense of usability of the system. When carrying out the experiment on a number of participants, it was discovered that 90% of users successfully entered the access code when the authentication process required only one step but when the process required both secret number and access code users became confused causing a slight drop in the number of participants that successfully accomplished the task. Lightening the security of a system to require just one-way access could be a little bit risky but in order not to reduce the usability of the interface; it could be required [14]. Another research being carried out by Mihajlov, et al [15], used a quantification approach and quality criteria to come up with a conceptual framework which evaluated both security and usability characteristics of systems. The quality criteria for security and usability were quantified separately by determining the linear dependence between the different quality criteria. However, recommendation was suggested to develop the approach, as it didn't fully achieve the balance between the security and usability aspects of the system. Another research by Chiasson et al. [16] focused on the security aspect of user interface by looking at graphical passwords. It was discovered that users had the tendency to select predictable passwords and reuse them across their different accounts. This is because the design of user interfaces for systems authentication inspires users either by encouraging secure or insecure behavior. According to Cranor & Buchler [4] in order to achieve usability gains, researchers must go beyond adopting human-centered design principles and embrace user decision making. It is going beyond malware detection into providing a comfortable system for the users by studying their behavior and response to threats.

Researches that had been carried out establishing a trade-off seem to be farfetched. Some approaches seem to tilt towards usability or security without fully integrating the two to establish a better and more suitable way to address both in user interface. Inability to establish a trade-off between usability and security can affect the end-users of the system, who are the people for which the system is initially designed to assist. This is usually seen in systems where the identity of the users is very important. The issue of security cannot be compromised at the expense of the usability of the system as found in e-Banking services where the personal and private nature of the financial information makes the balance between usability and security a key concern. The next section will perform an analysis on the presently existing approaches by answering some research questions in order to establish a trade-off between usability and security.

III. Research Approaches and Discussion

This paper strives to address some problems recognized in the literature concerning usability and security by analyzing the existing approaches that had been used. For this reason, we are guided to use Systematic Literature Review (SLR) method which is commonly used for various examinations in the area of software engineering by Kitchenham and Charters [17]. This approach is a way of evaluating and reading completely existing research already carried out which are important in order to answer a particular research question in a specific topic [18]. Systematic reviews are intended to produce an unbiased assessment of a research topic by using a dependable, rigorous, and auditable procedure.

A. *Research Questions*

Some researches, which have been carried out on usability and security in user interface usually, discussed in terms of the integration of the two in a system. However, there seem to be more research studies which consider the security aspects as much as the usability perspective [19].

Based on the literature review presented in the second section we continue to plan and conduct a systematic literature review and answer some research questions that have been derived.

RQ1: How was information concerning secure user

interface obtained? [4]

In order to acquire as much information regarding the subject on usability and security in user interface design domain, the following databases were searched:

- IEEE Xplore
- ScienceDirect
- ACM Digital Library
- SpringerLink
- Google Scholar
- Modern Education & Computer Science Publisher (MECS)

Initial search string *"user interface security"* returned an overwhelming number of papers, many of which were not relevant to the subject. The revised search string *"usability and security"* yielded more positive results which were used in this research. After reviewing a number of these papers, the list of applicable usability and security papers were used. For the paper selection on the search strategy, suitable inclusion and exclusion criteria for selecting primary studies were used as shown in Table 1 with the items extracted from the papers in Table 2. Table 3 describes the papers which were found to be exceptional in their portrayal of either usability or security, or both perspective(s) of a system and used mostly to answer the research questions asked.

RQ2: What criteria can be used to evaluate the usability of a system? [11]

When considering usability, it essentially encompasses user interface as well as operations and performance of a system. So to examine security characteristics from user perspective, the following will likely be considered [15, 19]:

1) Convenience

The security of a system ought not to be time-consuming or prominent because this causes inconvenience to the user, who will likely switch the feature off to prevent disturbance [19]. It is noted that user's submission to a security feature is extremely narrow because they respond negatively to systems that waste their time.

Considering the convenience for an authentication system, it measures the time consumed in performing an authentication, or replacement and enrollment [15]. Authentication time refers to the time that elapses as the user is trying to enter their personal information in order to gain access into a system. Time spent on replacement is that of retrieving the authentication information about a user when it is no more usable. Finally, enrollment time is the time that elapses when authentication password has been newly assigned for the first time. Out of these three, time spent on authentication is the most significant because it affects the shortage of this quality criterion.

2) Understandable

The ability of the users of a system to be able to understand security features shows the extent of the usability of that system [19]. This can also be known as meaningful retrieval which is the amount of effort that is put in by the user to retrieve and understand an authentication password [15]. One of the principles of designing a user interface is that the user should be able to recognize rather than having to recall the property of a particular function.

3) Inclusivity

Since the use of technology is not optional but rather something, which people need to use, designing user interface should be able to cut across different types of users [23]. This ensures that every user irrespective of their level of intuition, mobility, and cognitive skills can make use of a system with authentication features. This criterion is quantified by computing the addition of users in disability classifications [24]. The users should receive a clear indication of what to do at any level.

Table 1. Criteria for Paper selection [34]

Inclusion Criteria	Exclusion Criteria
Paper must be on usability, security or both perspective	Papers not in English
It must be in software domain	Papers that do not make claims about usability and security topics
Studies on usability and security engineering	Studies not focused on end-user perspective of usability and security

Table 2. Items Extracted for Papers [34]

Data Items	Description
Identifier	Unique identifier of the paper
Reference	The author's name, date published, title, source
Domain	The domain in which the paper is focused on
Perspective	The perspective of the topic
Research Questions	Questions in relation to the literature on the topic

Table 3. Discussions of Usability and Security in different articles [20]

Article	Perspective		Emphasis	Objectives	Journal/ Conference
	Security	Usability			
Bourimi, et al (2011)[12]	✓	✓	Security in social media	▪ To address privacy and security issues in multi-model user interfaces for social applications	Privacy, Security, Risk, and Trust (PASSAT)
Cranor, & Buchler, (2014)	✓	✓	Usability and Security Go Hand in Hand	▪ Introducing approaches taken by researchers to address usable security challenge	Security & Privacy, IEEE
Furnell, (2010)[19]		✓	Usability and complexity	▪ To examine usability and security as it affects the complexity of systems	Security and Privacy in Dynamic Environments
Ibrahim, et al., (2010)[21]	✓	✓	Assessing the Usability of End-User Security Software	▪ To reveal user's absence of security knowledge, which influence their decision-making process. ▪ To address for criteria for security measures	Trust, Privacy and Security in Digital Business
Mihajlov, M., Jerman-Blazic, B. and Josimovski, S. (2011)[15]		✓	Conceptual framework from usability perspective	▪ Framework for assessing stable security and security evaluation process by balancing quality metrics	Network and System Security (NSS), IEEE
Mihajlov, M., Blazic, B. J. & Josimovski, S., (2011)[10]	✓	✓	Usability and security evaluation	▪ Using Quantification approach to direct the evaluation process of authentication mechanisms	Computer Software and Applications Conference (COMPSAC), IEEE
Minami, et al., (2011)[13]	✓	✓	Trade-off between security and usability	▪ Addressing the balance between security and usability in systems ▪ Demonstrating through a case of computer scientists and care providers taking into consideration high security with better usability in systems	Consumer Communications and Networking Conference (CCNC), IEEE
Mockel, (2011)[11]	✓	✓	Integration of usability and security in e-banking systems	▪ Aligning of usability and security criteria to develop an evaluation framework specific to e-banking	Applications and the Internet (SAINT)
Weir, et al., (2009)[7]	✓	✓	Perception of security, convenience, and usability	▪ Comparing two-factor methods of e-banking authentication to illustrate the trade-off between usability and security	Computers & Security
Yoshimoto, et al., (2007)[22]		✓	Development and Evaluation User Interface for Security Scanner with Usability	▪ Using security scanners to develop an interface for users with high usability to evaluate the usability of user interface	Network-Based Information Systems

4) *Requirement*

Requirement calculates the properties required for hardware, technical and software support of the authentication feature of the system [25]. For instance, for a system with voice recognition security feature, there is a need for it to be a self-support software application.

The ability to access a system is hinged on the level of technical skill and knowledge as well as the value of the user's kit. Consequently, the authentication systems which need distinct hardware, software or technical know-how may also ignore users and encroach upon the common standard of accessibility and unrestrained situation. Therefore, in order to measure requirement, it is necessary to introduce a minute hardware and software system configuration which will require no technical expertise for the part of the user.

RQ3: What criteria can be used to evaluate the security of a system? [10]

According to Mihajlov, et al. [10] security criteria of a system are based on the quality standards of security measurement which shows different features. These features include the following: revelation, secrecy, privacy, breakability and abundance. The parameters for security evaluation are shown in Table 4.

Table 4. Quality standards for security evaluation [10]

Security Criteria	Description
Revelation	Revealing of the authentication password is hinged on factors of system and its user
Secrecy	The authentication password certainty depends on system and human factors
Privacy	Protecting user's personal details from being compromised
Breakability	The weakness of systems authentication part of the system
Abundance	The quality of accessible authentication passwords

1) *Revelation*

Revelation considers the access level of an authentication password from a user and system viewpoint. To quantify this quality criterion both points of authentication key exposure have to be considered, as they are separated into system and user revelation respectively [30]. There are certain ways in which the user of a system might reveal his/her authentication key. One of these ways is through frequent popups warning; out of frustration to get rid of such notifications the user might consent to the release of certain information that should have been kept private [26].

2) Secrecy

The ability to predict an authentication key is confirmed to be a huge concern. The effort of deliberate unpredictability arises from the reduced perception of randomness that users pose. To decide the order of arranging the authentication being selected at random, it is important to spot these things: *distinctness*, the absence of association with previous or subsequent words, *even distribution*, the same likelihood of distribution over the whole words, and *uniquenes*s, the failure to casually produce a similar order of words. The main aspect of this security criterion is to find how several people can discover a password as predictable [27].

3) Privacy

Privacy refers to the number of reserved details necessary for the authentication part of the system [28]. A compromised password can violate the confidentiality of user and cause their identity to be stolen. Determining who to trust with private information is a difficult decision which involve the use of risk management process. Unfortunately, users are not good at risk assessment, particularly where privacy decisions are concerned.

4) Breakability

This refers to the effort put in by an attacker to navigate around security part of the system and have access to either the system or the codes that generate the authentication password. Based on how the system is built, the attacker may use any of the following four techniques to determine the user's key: keylogging, brute-force, research and dictionary [29].

5) Abundance

This criterion calculates the authentication password space or, in other words, the set of possible passwords that can be used to generate a password, in two aspects: the amount of existing passwords offset by the amount of passwords regularly used in practice. This has an obvious influence on the penetration level of the authentication password, providing more likelihoods of increasing the time needed to compromise it [31].

RQ4: What is the connection between security criteria and usability criteria in influencing quality? [11]

The exact usability and security criteria for the system have to be resolved, assessed and then measured to decide on the total quality of the system. Security and usability quality criteria can individually display properties which are not aligned. For simplification, it is important to consider the different quality criteria as equally independent variables. The quality criteria earlier mentioned did not have anything to do with the quality metrics, but emphases on the quality of the system in terms of it being suitable for the task in a particular domain [15]. The criteria for usability and security can affect the quality of the system produced because the quality criteria mentioned have a direct impact on any system and point to important aspects that a system should consider when being developed.

A more dynamic dimension can be delivered upon supplementary research. In addition, some quality criteria used to determine the presence of security and usability are interdependent and require dissimilar quantification method. Howbeit, the reliance exhibited between specific criteria has to be investigated in order to improve the quantification method for each value.

From the research questions which have been answered above, the essential question is whether the trade-off between usability and security is necessary. A prevalent understanding is that usability criteria must be sacrificed to achieve meaningful security criteria, and vice versa [4]. Our contention is that to achieve usability of a user interface without sacrificing security, it is important to go beyond adopting usability principles. These quality criteria as earlier mentioned can be quantified to establish a balance between the usability and security. Weir, et al., [7] delivered a broad study on usability for most frequently used authentication method. Mihajlov, et al., in two of their papers [10, 15] also carried out extensive study on authentication mechanisms and tried to quantify them in one paper and then went further in a bid to develop a framework that can be used to establish a trade-off between usability and security. None of these quality criteria can be discussed without the other. Each of these quality criteria cannot be discussed without the other. Users usually don't want to actively manage the minutiae of security features. So developers have the attitude of creating a "smart defaults" in which users adopt. On the other hand, users must be able to easily manage and effectively understand system security features.

IV. Conclusion

It is evident that quality criteria of usability and security cannot be discussed independently; they must go together while user interface is being designed. This will prevent the developers from creating or coming up with system adoption where users don't have to validate and understand their security features. A better solution would be making users aware of the things they do and their implications. An organization that is storing any type of sensitive information/data is required by law to have a technology-based deterrent in place, a diligent monitoring and review method, and a process to mitigate the breach. Security policies are a necessary measure in the current enterprise networks, otherwise, users will be open to attacks. Though most of the breaches in security are caused by weak passwords, encrypted files left unprotected on computers and successful social engineering could be a source of attack on users. It is, therefore, important that programs interface to enhance security by making it easy for user to make secure choice and thereby helping in avoiding a costly mistake. Secure human interface design is a complex topic affecting the different operating systems. There is the common belief that security and usability are incompatible when it comes to design that involves users but this does not have to be so. In many cases, a simple interface considered is more secure because they don't require a severe authentication mechanism to be put in place [26]. Security in systems is an assurance to the user, gives them a right to a system's access to information by putting up authentication and control mechanisms making sure the users of these systems are the only ones that have been granted acceptable rights. Although security mechanisms might make it hard for users to access systems, instructions are becoming more complicated as the networks expand. Thus, usability and security must be considered in a manner which allows users to make suggestions to the developers on interface design they find comfortable so that they can enjoy the user interfaces and securely use the information systems.

With the advent of the use of internet services which makes life much easier and convenient for users, a question is being placed on the usability and security of the system they use. The question of usability seems to be more emphasized with new ways coming up on improving human interaction design with little spoken of security. Nowadays, the issue of security is on the increase and responses have been slow in eliminating the risk users are faced with when confronted with such situations. If security and usability were taken into consideration during the design of software system, it would have helped to reduce the number of security cases which are affecting users. Now researchers and developers are beginning to go back to the drawing board in order to address these issues and tackle them before any software system is rolled out.

V. Future Recommendations

The outcome of any software system that implements the balance of both security and user interface design will be of great benefit although little has been done to address these areas. Most of the works that have been performed on the balance between usability and security seems to focus more on the authentication methods but it has to go beyond just this part of a system to take into consideration the integration into every part of the user interface design. For example, the authentication interface of e-Banking software should not be the only part that considers security and usability, but also the other interfaces after that.

We, therefore, recommend that this research can be further done with real-life cases properly, using another research method such as questionnaire and interview. For the future research requirement collection phase in the software development life circle (SDLC) can be taken into consideration as it is important to collect not just the usability requirement alone but also that of the security requirement of the system in question. This will help to prevent rework which is a humongous issue that no developer is willing to face because it reduces the quality and affects the overall performance of the software. The quantification of the evaluation carried out on usability and security can help to determine the quality criteria that will also be used to decide the total quality of the system [10]. Based on the questions which have been answered in this review, it is expected that more development should be done to come up with a strategy that integrates the two aspects. Researchers that are working on this field should try out their ideas in some real-life software development so that they can gain a deeper understanding into how users behave and interrelate with security features that are found in their system. The study will help to increase the confidence of users while using the system, therefore increasing the usability as well as the security. Nevertheless, it is important to note that one of the things to avoid while establishing a trade-off between usability and security is complexity [19]. The outcomes from these researches will help to provide information on design of substitute methods which will also be assessed and conveyed as part of future work.

References

[1] R. W. Reeder, C.-M. Karat, J. Karat, and C. Brodie, Usability challenges in security and privacy policy-authoring interfaces, in *Human-Computer Interaction– INTERACT 2007*. 2007, Springer. p. 141-155. doi:10.1007/978-3-540-74800-7_11

[2] T. Fischer, A.-R. Sadeghi, and M. Winandy, "A pattern for secure graphical user interface systems," vol. pp. 186-190, 2009. doi:10.1109/DEXA.2009.76

[3] S. Möller, N. Ben-Asher, K.-P. Engelbrecht, R. Englert, and J. Meyer, "Modeling the behavior of users who are confronted with security mechanisms," Computers & Security, vol. 30, pp. 242-256, 2011. doi: http://dx.doi.org/10.1016/j.cose.2011.01.001

[4] L. F. Cranor and N. Buchler, "Better together: Usability and security go hand in hand," IEEE Security & Privacy, pp. 89-93, 2014.

[5] Y. Fujihara, H. Oikawa, and Y. Murayama, "Towards an interface causing discomfort for security: A user survey on the factors of discomfort," vol. pp. 173-174, 2008. doi: 10.1109/SSIRI.2008.44

[6] S. Faily and I. Fléchais, "Finding and resolving security misusability with misusability cases," Requirements Engineering, pp. 1-15, 2014. doi:10.1007/s00766-014-0217-8

[7] C. S. Weir, G. Douglas, M. Carruthers, and M. Jack, "User perceptions of security, convenience and usability for ebanking authentication tokens," Computers & Security, vol. 28, pp. 47-62, 2009. doi: 10.1016/j.cose.2008.09.008

[8] L. B. Ammar, A. Trabelsi, and A. Mahfoudhi, "A model-driven approach for usability engineering of interactive systems," Software Quality Journal, pp. 1-35. doi: 10.1007/s11219-014-9266-y

[9] C. Rudolph and A. Fuchs, "Redefining Security Engineering," vol. pp. 1-6, 2012. doi: 10.1109/NTMS.2012.6208773

[10] M. Mihajlov, B. J. Blažič, and S. Josimovski, "Quantifying Usability and Security in Authentication," vol. pp. 626-629, 2011. doi: 10.1109/COMPSAC.2011.87.

[11] C. Möckel, "Usability and Security in EU E-Banking Systems-Towards an Integrated Evaluation Framework," vol. pp. 230-233, 2011. doi: 10.1109/SAINT.2011.42

[12] M. Bourimi, R. Tesoriero, P. G. Villanueva, F. Karatas, and P. Schwarte, "Privacy and security in multi-modal user interface modeling for social media," vol. pp. 1364-1371, 2011. doi: 10.1109/PASSAT/SocialCom.2011.49

[13] M. Minami, K. Suzaki, and T. Okumura, "Security considered harmful a case study of tradeoff between security and usability," vol. pp. 523-524, 2011. doi: 10.1109/CCNC.2011.5766529

[14] N. Gunson, D. Marshall, H. Morton, and M. Jack, "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking," Computers & Security, vol. 30, pp. 208-220, 2011. doi: 10.1016/j.cose.2010.12.001

[15] M. Mihajlov, B. Jerman-Blazic, and S. Josimovski, "A conceptual framework for evaluating usable security in authentication mechanisms-usability perspectives," pp. 332-336, 2011. doi: 10.1109/ICNSS.2011.6060025

[16] S. Chiasson, A. Forget, R. Biddle, and P. C. Van Oorschot, "User interface design affects security: Patterns in click-based graphical passwords," International Journal of Information Security, vol. 8, pp. 387-398, 2009. doi: 10.1007/s10207-009-0080-7

[17] B. A. Kitchenham and S. Charters, Guidelines for performing systematic literature reviews in software engineering, in Technical report, Ver. 2.3 EBSE Technical Report. EBSE. 2007, School of Computer Science and Mathematics, Keele University.

[18] L. García-Borgoñon, M. Barcelona, J. García-García, M. Alba, and M. J. Escalona, "Software process modeling languages: A systematic literature review," Information and Software Technology, vol. 56, pp. 103-116, 2014.

[19] S. Furnell, "Usability versus complexity–striking the balance in end-user security," Network Security, vol. 2010, pp. 13-17, 2010. doi: 10.1007/0-387-33406-8_26

[20] P. Savolainen, J. J. Ahonen, and I. Richardson, "Software development project success and failure from the supplier's perspective: A systematic literature review," International Journal of Project Management, vol. 30, pp. 458-469, 2012. doi: 10.1016/j.ijproman.2011.07.002

[21] T. Ibrahim, S. Furnell, M. Papadaki, and N. L. Clarke, "Assessing the Usability of End-User Security Software," vol. pp. 177-189, 2010. doi: 10.1007/978-3-642-15152-1_16

[22] M. Yoshimoto, T. Katoh, B. B. Bista, and T. Takata, Development and evaluation of new user interface for security scanner with usability in human interface study, in Network-Based Information Systems. 2007, Springer. p. 127-136. doi: 10.1007/978-3-540-74573-0_14

[23] D. Reed and A. Monk, "Inclusive design: beyond capabilities towards context of use," Universal Access in the Information Society, vol. 10, pp. 295-305, 2011. doi: 10.1007/s10209-010-0206-8

[24] A. Mieczakowski, P. Langdon, and P. J. Clarkson, "Investigating designers' and users' cognitive representations of products to assist inclusive interaction design," Universal access in the information society, vol. 12, pp. 279-296, 2013. doi: 10.1007/s10209-012-0278-8

[25] B. Akhgar, A. Staniforth, and F. Bosco, Cyber Crime and Cyber Terrorism Investigator's Handbook. Syngress, 2014.

[26] R. Dhamija and L. Dusseault, "The seven flaws of identity management: Usability and security challenges," Security & Privacy, IEEE, vol. 6, pp. 24-29, 2008. doi: 10.1109/MSP.2008.49

[27] P. N. Son and H. Y. Kong, "An Integration of Source and Jammer for a Decode-and-Forward Two-way Scheme Under Physical Layer Security," Wireless Personal Communications, vol. 79, pp. 1741-1764, 2014. doi: 10.1007/s11277-014-1956-z

[28] U. Habiba, R. Masood, M. A. Shibli, and M. A. Niazi, "Cloud identity management security issues & solutions: a taxonomy," Complex Adaptive Systems Modeling, vol. 2, pp. 1-37, 2014. doi: 10.1186/s40294-014-0005-9

[29] K. Renaud, Evaluating authentication mechanisms, in Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, Editors. 2005, O'Reilly Media: Stebastopol, C.A. p. 103-128.

[30] N. Anciaux, M. Benzine, L. Bouganim, P. Pucheral, and D. Shasha, Revelation on demand. Distributed and Parallel Databases, vol. 25(1-2), pp. 5-28, 2009 doi: 10.1007/s11219-014-9266-y

[31] P. Mayer, M. Volkamer, and M. Kauer, Authentication Schemes - Comparison and Effective Password Spaces in Information Security, A. Prakash and R. Shyamasundar, Editors. 2014 Springer International Publishing: Hyderabad, India. p. 204-225. doi: 10.1007/978-3-319-13841-1_12

[32] H. Iqbal and M. F. Khan, "Assimilation of Usability Engineering and User-Centered Design using Agile Software Development Approach" I.J Modern Education and Computer, vol.6(10), pp. 23-28, 2014.

[33] I. Ahmad Mir and S.M.K. Quadri, "Analysis and Evaluating Security of Component-Based Software Development: A Security Metrics Framework", IJCNIS, vol.4 (11), 2012 pp. 21-31

[34] D. Heaton & J.C. Carver, Claims about the use of software engineering practices in science: A systematic literature review, Information and Software Technology, vol. 67, pp. 207-219, 2015

Authors' Profiles

Ugochi Oluwatosin Nwokedi received her B.Sc. Degree from Crawford University, Nigeria in 2012 and currently pursuing her M.Sc. degree in Software Engineering at Asia Pacific of Technology and Innovation under Staffordshire University franchised program. Her research interests include software security, requirement engineering, software development process modeling, software modeling, Identity management, Security policies and standards, and software project management.

Beverly Amunga Onyimbo awarded Bachelor Degree from Kabarak University, Kenya in 2012. Currently, she is pursuing her M.Sc. Degree in Software Engineering at Asia Pacific of Technology and Innovation under Staffordshire University franchised program. Her research interests include User Experience and User Interface (UX & UI) Design, Human-Computer Interaction, Computer Communication Networks, Artificial Intelligence, Internet of things and Information Security.

Babak Bashari Rad received his B.Sc. of Computer Engineering (Software) in 1996 and M.Sc. of Computer Engineering (Artificial Intelligence and Robotics) in 2001 from University of Shiraz; and Ph.D. of Computer Science (Information Security) in 2013, from University Technology of Malaysia. Currently, He is Program Leader of Postgraduate Studies and Senior Lecturer in School of Computing and Technology, Asia Pacific University of Technology and Innovation (APU), Kuala Lumpur. His main research interests cover a broad range of various areas in computer science and information technology including Information Security, Malware Detection, Machine Learning, Artificial Intelligence, Image Processing, Robotics, and other relevant fields.

How to cite this paper: Ugochi Oluwatosin Nwokedi, Beverly Amunga Onyimbo, Babak Bashari Rad,"Usability and Security in User Interface Design: A Systematic Literature Review", International Journal of Information Technology and Computer Science(IJITCS), Vol.8, No.5, pp.72-80, 2016. DOI: 10.5815/ijitcs.2016.05.08