Tradeoffs between Usability and Security

F. Sahar

***Abstract*—Usability and security become a core issue in the designing of modern computer software's. Nevertheless, there are studies have been conducted in different combinatorial ways of these subjects. However, still there is room to improve the relationship in sense of appropriate deployment of these features in software applications. In this paper we discuss the potential tradeoffs of usability and security in the software development process by proposing a guideline. The case studies are diligently carried out for qualitative approach.**

***Index Terms*—Guidelines, recommendation, security, security, Usability**

I. Introduction

Security issues are upraising its importance in many types of interactive systems due to change in user interface design strategies. Usability is also a vital aspect in such systems [1], [2]. It assumed that computer security and computer usability is inversely proportional to each other but with the advancement and contribution in this area this trend is starting to change [3]. Usability affects security in systems that aspire to protect data confidentiality [4].

The security and usability are not fundamentally at odds with each other. A system which is more secure is more reliable, more controllable, and hence more usable on the other side a more usable system reduces confusion and is thus more likely to be secure. In common, security aspects and usability aspects both want the computer to properly perform tasks what the user wants [5].

We have been concerned with the significant concern of how to make the relevant features of usability and security situations visible to users in order to allow them to make informed decisions concerning potential usability, and security problems. This directed towards the need for systems that are more secure and those that are more useful as well as trustable [6].

The usability of secure systems has to turn into a core subject in research on the efficiency and user acceptance of secure systems. In secure systems the authentication method is necessary for controlling the access. Even so, the design of usable yet secure user authentication methods raises critical questions regarding how to resolve conflicts between security and usability goals [7].

This report presents the issues concerning the usability of secure systems. It aims is to tackle the problems in minimizing the tradeoffs between usability and security. Moreover, contributing ideas about the problems and discussing the factors affecting the decision making process for usability of secure systems.

Manuscript received January 24, 2013; revised April 5, 2013.

The author is with Tampere University of Technology, Finland (e-mail: farrukhsahar@yahoo.com).

II. Background

Initially, the usability and security were treated as two different domains in computer systems. On account of their very different kind of nature these were used by the software developers and the researchers in a particular specified manner. Both have different meaning when asked in different contexts [8] e.g. security has different meaning when it is used in software applications, websites, and networks etc, whereas there are different implications of usability in different kinds of applications.

There are certain conflicts whether to make the design of software more usable or more secure. In order to hold both properties, there is a state of contention resolution in the form of tradeoffs. To perk up the usability of software for the facilitation of end user then worst situation can be happened in the form of low security and vice versa [9]. There are currently many obstructions in creating effective computer security which is usable. Defining the security strategies for software which usable and strategies for user interface design that are appropriate for that software is an indispensable concern [1]. The design of usable yet secure systems raises many considerable questions when it comes to balancing properly the properties of security and usability. Most of the properties of both the fields are hard to collaborate where usability and security are focused points. Finding the right tradeoffs between these two quality attributes is not an easy attempt according to following the standards as mentioned in ISO 9241, ISO 9241-11, ISO/IEC 9261-1 etc [10].

In the context of usability and security a lot of work has been done almost in every area. There are major categories like application interfaces usability, web interfaces usability, networks usability, hand-held devices usability and other hardware based interactive interfaces. If we see all these recognized classes in their domains, then there are certain specific issues has been discussed in their relevant sphere of influence.

III. Related Work

To the best of our knowledge, no such studies have been conducted in order to understand the relationship between usability and security in the form of providing guidelines. However, there are some studies on the relationship of usability and security in certain pointed areas of software's in very different context. For example, (Nathaniel Good et al) [11] did a user study of decision to install the applications that could affect their privacy and could be subject to ruin in consequence of inappropriate usability. Also, in this context (RachnaDhamija et al, 2006) [12] had discussed the security problems in usability as a result of phishing and proposed a security mechanism to interact with server's safely. In user authentication methods (Christina Braz *et al*.) [7] took a

DOI: 10.7763/IJET.2013.V5.591

comprehensive overview of security and usability.

In addition, (Benjamin J. Halpert) [13] made the evaluation authentication interface and design for mobile devices. Moreover, in the background of networking environment there is a case study in the university made by (Douglas E Ennis) [14] which describes how user can communicate in a secure way with wireless networks. Furthermore, in the perspective of hardware interaction systems (Rajah James et al) [15] proposed a laboratory case study of user interaction with heartbeat systems that describes how a user can monitor the data in a usable and secure way. All above mentioned categories with few others proposed a certain issues which discussed their usability and security in a specific domain, but we found no any general guidelines to make our decisions for the creation of an optimal, secure and user-friendly system.

IV. Design Principles or Guidelines

The following section will presents a selective set of guidelines for secure interface design. Apply them in practical will show their effectiveness, it may not be completely effective but will demonstrate the optimal solutions for the success of a user interface. For the development of these guidelines we took a critical overview of literature consists on different set of standard's features. The design standards listed here are picked from ISO/IEC, IEEE and Jakob Nielsen reported literature. Due to time constraints we have select only a few important standard features for our study assessment [5].

The suggested Guidelines are the general concepts of right tradeoffs, so these could be equally useful for the application interface designs and the users of those systems. In case of designers it is pointed to the application interface developers like software application designers, web site designers and mobile interface designers etc. While the users are the persons who interact with some interface devices such as keyboard, mouse and displays.

A. Problems Types and Design Recommendations

This action illustrates the selective set of standard features with their various problems along with examples which were observed by different researchers. In this part we will explain the causes of problems and will provide observed appropriate design recommendations in terms of guidelines. These related guidelines will provide the fine line between tradeoffs of usability and security. The selected set of features from those standards are; effectiveness, efficiency, satisfaction and learnability.

1) *Effectiveness and Security:* The author says [16]", the accuracy and completeness with which users achieve specified goals", along with providing good security. As author says [12], in case of password's protection, the password protection mechanisms are very inconvenient to the users to enhance their security. So these users possibly face new security threats. As a result due to lack of effective usability the strong security policies turn into weak security. Moreover, another researcher says that [17]"users errors cause are contributed to most computers tend to be clumsy, confusing are near nonexistent." For the effect security different software requires different standards. So these are different acceptance levels of usability and security effectiveness.

2) *Recommendations:* For the right tradeoffs between usability and security is that designers must provide an easy to use interface with less hindrance and provide the better understanding of security in that environment in terms of warning messages, wizards and interacting tools [18].in order to develop usable security designers must incorporate security from early stages of software development by giving the high priority to security.

3) *Guideline:* In order to develop usable security designers must incorporate security from early stages of software development by giving the high priority to security.

4) *Satisfaction and Security:* According to [19] satisfaction means trust in concern of the issues such as security, honesty and dependability when dealing with any interface. Moreover as proposed in [20] as a design analyst point of view trust meet when it is satisfy the user in providing the expected working environment and it also fulfills the security requirements. Furthermore as [21] defines in user centered context the security meets with usability when we deal with the usability of security tools with the satisfaction of its users. The most important concept where satisfaction meets with security is [22] dealing with the digital products and the services such as information content, transaction and payments. The main issue is not to adopt the online services but the main concern is the satisfaction on the services with security policies. He posted an example of banking systems where the key targets that companies want to achieve are the internet security, building customer trust and ensuring privacy of the customer trust.

5) *Recommendations:* When dealing with the context such as banking systems we have to satisfy the customer needs and making customer trust on the security without compromising the security policies of our system. A small mistake in security point of view could become a reason of a disaster. When dealing with satisfactory and secure environment user feel comfortable in proceeding of their tasks.

Security and satisfaction both can work together as by giving user satisfaction in security aspects as well as in pleasant use aspects.

6) *Guidelines:* In order to achieve satisfaction and security it has to support the trusts on the services in both points of views first is the ease of use, and second the security of information contents specially when dealing with transactions and payments.

7) *Efficiency and Security:* [23] Explore his ideas that how security and efficiency tradeoffs arise when dealing with content distribution and to prove this he gave an example when small amounts of the video are selected for encryption and watermarking, the security of the scheme decreases. On the other side when bigger percentages of the video are

chosen to be watermarked, encrypted and unicast security increases but it will also affect the efficiency. Furthermore [24] illustrated their findings about security and satisfaction for multicast key management in the case of rekeying. The combination of security with efficiency sometimes reaches at a compromising state because we have to implement security efficiently with all respect in concern of speed and accuracy.

8) *Recommendation:* When dealing with security and efficiency in interfaces we have to strongly consider the efficiency attributes that speed and accuracy and security attributes such as privacy, authentication and so on in specified context. We also have to get knowledge about the compromising states because sometimes it is hard to implement security in all respect with the speed and accuracy attributes.

9) *Guidelines:* Efficiency meets security when we are able to achieve security attributes such as authentication, privacy and so on with speed and accuracy in a specified context.

10) *Learnability and Security:* Learnability is concern with how the system is easy to learn and easy to use-in literature there is a discussion has been done on it as according to [18] the learnability is more crucial because in some cases more secure system or software's may not be used due to there difficult to learn and users just skip the security limitations for the task completion.

11) *Recommendations:* The most often objection faced to usability is learnability. There should be proper balance between security and learnability. But in some cases learnability is take edge over security.

12) *Guidelines:* For the right tradeoffs between learnability and security the system should be more learnable in order to incorporate proper security.

B. Procedures

The research performs with qualitative approach in which we conduct two cases different case studies in two different organizations. For the evaluation of recommended guidelines in order to understand at what extent these features are implicated in application designing processes. These case studies have been conducted to get a broader view of different aspects of designing interfaces process. For the date collection of each case study, we will examine the relevant application developing representatives. Furthermore, we will collect the useful data especially for our concerning problems.

1) *Data Collection:* Data collection procedure in each case will consist on interviews, direct observations and documentation of the products. The interview session will conduct with the interface design team and application programming team. The interviews intended to gather information about organizations such as its projects length and size, project types (desktop applications, web sites application, mobile application, etc.), number of projects, etc. The interview part will consist on structured and unstructured questions from both teams pertinent to our research scenario. The data collection from these case studies will assess to test the influence of suggested guidelines.

In observation session three members of interface designing and three from coding team will be observed during application development practices. These sessions will be conducted on both teams in same organization, i.e. one session for interface designing and one for code development.

During the observation session researcher participation is there, they will promote the session. In which they will provide the tradeoffs answers during the developing process of applications. During the observation session researchers will take to notice the techniques to develop the applications. In the way the researchers can assist them by suggesting the better approach for the right tradeoffs of usability and security.

In the document session, the documents of requirement specification, application design documents and coding documents will be analyzed to get insight of the intended levels of tradeoffs.

2) *Data Analysis Procedure:* In order to analyze the conducted case studies, transcript data will be read and re-read in order to code for adopted practices for development. This will help to examine different organization to observe similar factors that effecting their application development in proposed features view. Regardless of whether the similar features are identified, they will also be evaluating with respect to the both development teams information, collected through interviews. Furthermore, during the observation session judgment will be made whether the developing teams are intended to complete their tasks or follow the precise standards. This part will show their dedication to analyze whether they practices the best possible tradeoffs or not.

3) *Validity of Study:* The validity of this study is more apparent from its way of conduct. As the different data collection sessions will help to provide the variety of information from each team's perspectives. As the interview and observation sessions with three respective persons shows the span of study coverage.

To make the validity of collective data more robust, the final report prepared by researchers will be given to the interviewed and observing teams, with highlights of their interviews and observations during study. They can better authenticate the study that will be helpful for further proceedings. The investigated material will provide to the users of those applications they can analyze as well and proposed their interpretation of findings that will also validate the accuracy of the study.

V. Conclusion

It is concluded that there is a need of experiment to understand the relationship among guidelines, usability attributes and security attributes. It supposed that once experiment data has gone through from analyzing phase then it reveals a good understanding of the relationship among guidelines, usability attributes and security attributes. It is expected the experiment will confirm that the tradeoffs between usability and security can be identified and

minimize when appropriate guidelines are used. If everything will be up to expected results, then we could say that the result can be generalize-able in the form of general guidelines to an industry setting.

REFERENCES

[1] A. Whitten and J. D. Tygar, "Usability of security: A case study," CMU-CS-98-155, December 18, 1998.

[2] D. G. Marks and M. Stinson, "Security trumps efficiency: Putting it into the curriculum," *J. Comput. Small Coll,* vol. 22, no. 4, pp. 162-169, 2007.

[3] K. Rozinov, "Are usability and security two opposite directions in computer systems?" Department of Computer and Information Science, Polytechnic University, Brooklyn, NY 11201.

[4] R. Dingledine and N. Mathewson, "Anonymity loves company: Usability and the network effect," in *Proceedings of the Fifth Workshop on the Economics of Information Security (WEIS 2006)*.

[5] K. P. Yee, "User interaction design for secure systems," in *Proc. 4th International Conference on Information and Communications Security (ICICS 2002)*, pp. 278-290, January 01, 2002.

[6] R. de Paula *et al.*, "Two experiences designing for effective security," in *Proceedings of the 2005 Symposium on Usable Privacy and Security*, pp. 25 - 34, 2005, vol. 93, ACM, New York, NY, 25-34. DOI= http://doi.acm.org/10.1145/1073001.1073004

[7] C. Braz and J. Robert, "Security and usability: the case of the user authentication methods," *IHM '06*, vol. 133. ACM, New York, NY, 199-203. DOI= http://doi.acm.org/10.1145/1132736.1132768

[8] E. P. Rozanski and A. R. Haake, "The many facets of HCI," in *Proc. 4th Conference on Information Technology Curriculum, CITC4 '03*, ACM, New York, NY, pp. 180-185, 2003.

[9] E. Schultz, "Research on usability in information security," *Computer Fraud & Security*, pp. 8-10, June 2007.

[10] C. Braz *et al.*, "Designing a trade-off between usability and security: A metrics based-model," *Human-Computer Interaction – INTERACT 2007*, pp. 114-126, 2007.

[11] N. Good *et al*., "Stopping Spyware at the gate: A user study of privacy, notice and spyware". in *Proceedings of the 2005 Symposium on Usable Privacy and Security*, pp. 43 - 52, 2005.

[12] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," *CHI'06*, ACM, April 22-27, 2006.

[13] B. J. Halpert, "Authentication interface evaluation and design for mobile devices," *InfoSecCD '05*, ACM, New York, NY, pp. 112-117, 2005.

[14] D. E. Ennis, "The wireless tightrope: an economical, secure, and user friendly approach for the wireless," *SIGUCCS*, 2005. ACM, pp. 62-67.

[15] James *et al*., "A usability evaluation of a home monitoring system," in *Proceedings of the 3rd Symposium on Usable Privacy and Security*, SOUPS '07, vol. 229. ACM, New York, NY, pp. 143-144.

[16] N. Bevan, "International standards for HCI and usability," *J. Human-Computer Studies,* vol. 55, issue 4, October 2001, pp. 533-552.

[17] A. Whitten and J. D. Tygar, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0," in *Proc. the 8th USENIX Security Symposium*, August 23-36, 1999, Washington, D.C., pp. 169-184.

[18] K. P. Yee, "Aligning security and usability," *Security & Privacy*, vol. 2, issue 5, pp.48 – 55, 2004.

[19] T. Grandison and M. Sloman, "Trust management tools for internet applications," in *Proc. the 1st International Conference on Trust Management*, pp. 91-107, Crete, Greece: Springer Verlag, 28-30 May 2003.

[20] C. B. Haley, R. C. Laney, B. Nuseibeh, and J. D. Moffett, "Using trust assumptions in security requirements engineering," *Second Internal iTrust Workshop On Trust Management In Dynamic Open Systems*, 2003.

[21] D. G. tom Markotten, "User-Centered security engineering," Albert-Ludwigs-University of Freiburg, Friedrichstrasse 50, D-79098 Freiburg, Germany.

[22] I. Brown and M. Buys, "A cross-cultural investigation into customer satisfaction with internet banking security," (White River, South Africa, September 20 - 22, 2005). ACM, vol. 150, pp. 200-207, 2005.

[23] P. Judge and M. Ammar, "Security issues and solutions in multicast content distribution: A survey," *Network*, vol. 17, Issue 1, 2003.

[24] C. Duma *et al*., "A hybrid key tree scheme for multicast to balance security and efficiency requirements," in *Proc. Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, 2003, WET ICE 2003, June 2003, pp. 208-213.

Farrukh Sahar was born in Quetta, Pakistan in 1980.

He got his M.S.degree in Computer Science from Blekinge Tekniska Högskola, Sweden. He is a PhD Student at Tampere University of Technology, Finland.

His Research interests are Remote methods for long-term UX evaluation, Long-term UX evaluation of multi-component products.