Computers in Human Behavior 61 (2016) 656–666

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Full length article

Deciding between information security and usability: Developing value based objectives

Gurpreet Dhillon [a], Tiago Oliveira [b, *], Santa Susarapu [c], Mario Caldeira [d]

[a] School of Business, Virginia Commonwealth University, 301 West Main Street, Richmond, VA, 23284-4000, USA
[b] NOVA, Information Management School, Campus de Campolide, 1070-312, Lisboa, Portugal
[c] KPMG, USA
[d] ISEG, University of Lisbon, Rua Miguel Lupi, 20, 1249-078, Lisboa, Portugal

ARTICLE INFO

Article history:
Received 29 June 2015
Received in revised form
17 March 2016
Accepted 21 March 2016

Keywords:
Security values
Usability values
Value focused-thinking
Qualitative methods
Instrument development
Quantitative methods

ABSTRACT

Deciding between security and usability of systems remains an important topic among managers and academics. One of the fundamental problems is to balance the conflicting requirements of security and usability. We argue that definition of objectives for security and usability allows for deciding about the right balance between security and usability. To this effect we propose two instruments for assessing security and usability of systems, and develop them in three phases. In Phase 1 we identified 16 clusters of *means* and 8 clusters of *fundamental* objectives using the value-focused thinking approach and interviews with 35 experts. Based on phase 1, in the second phase we collected a sample of 201 users to purify, and ensure reliability and unidimensionality of the two instruments. In the third phase, based on a sample of 418 users we confirmed and validated the two instruments found in Phase 2. This resulted in 14 means objectives organized into four categories (*minimize system interruptions and licensing restrictions*, *maximize information retrieval*, *maximize system aesthetics*, and *maximize data quality*), and 10 fundamental objectives grouped into four categories (*maximize standardization and integration*, *maximize ease of use, enhance system related communication, and maximize system capability*). The objectives offer a useful basis for assessing the extent to which security and usability has been achieved in systems. The objectives also provide a decision basis for balancing security and usability.

1. Introduction

Bruce Schneier's cynical slogan, “The more secure you make something, the less usable it becomes” sums up the current state of security and usability. As we make systems more secure, genuine users try and find hacks and work around, which result in compromising security. Research in information security and usability has recognized this problem, however not much has been accomplished, largely because of two reasons. First, the requirement for security and usability of systems has always been considered as an afterthought (see, Baskerville, 1988). Two, security and usability issues have not been considered strategically and integrated into the strategic plans for developing systems. These two reason have resulted in systems that are often not aligned in terms of security and usability. Therefore the need is to identify objectives for both security and usability, collectively, that will help with proactively balancing security and usability.

In the literature the value of strategic objectives in guiding decision-making has been well researched. Keeney (1992) for instance argues that objectives and their corresponding attributes guide decision-making. And they are important for developing the overall strategy of an organization. In our case when an enterprise decides that it should strategically focus on aligning security and usability in systems, a decision context gets defined. The task then is to systematically define the objectives such that proper strategic planning can be accomplished. In terms of security and usability it is important to engage in such an exercise since both security and usability, which are two distinct quality dimensions (Kim & Park, 2012), have often been considered as after-thoughts.

In this paper we present such objectives through a detailed two-step process. First, using Keeney (1992), and Gregory and Keeney (1994) we define policy alternatives for ensuring alignment between security and usability of systems. Second, we undertake a

* Corresponding author.
E-mail addresses: gdhillon@vcu.edu (G. Dhillon), toliveira@novaims.unl.pt (T. Oliveira), susarapusr@gmail.com (S. Susarapu), caldeira@iseg.utl.pt (M. Caldeira).

http://dx.doi.org/10.1016/j.chb.2016.03.068
0747-5632/

detailed quantitative analysis to present a parsimonious set of security and usability objectives. These objectives form the basis for any alignment and balancing security and usability.

2. Literature review

Typically, in any discussion of security and usability issues, users are the first to be blamed for being the weakest link and less motivated to adopt any stringent security measures. On the contrary, Adams and Sasse (1999) recognized the importance of challenging the view that "users are never motivated to behave in a secure manner." Adams and Sasse (1999) affirm that user apathy toward not behaving in a secure manner is due to lack of user-centered design in security mechanisms. In spite for the recognition that usability of systems needs to be balanced with the security requirements, not much progress has been made within the researcher and practitioner communities. Chen, Wong, Zhang, and Techonlogies (2015), for instance note, "security for every service and application we depend on and use every day is turning into a major challenge for all of us, not just the designers, the architects, the developers, and implementers alike, but especially so for the users". Indeed security and usability are at odds with each other. Yee (2004) notes that the conflict is because implementers treat security or usability as an add-on to a system. As a result in the literature several calls have been made to consider usability and security considerations coherently.

Hoffman, Grivel, and Battle (2005) argue that "some architecture decisions may unknowingly limit the ability to implement usability requirements" (Hoffman et al., 2005, p. 469). Therefore, it is clear that security is one of the information systems architectural decisions that IT executives focus leaving critical system usability decisions unaddressed. Al Abdulwahid, Clarke, Stengel, Furnell, and Reich (2015) undertook a survey of users where they found that users systematically did not adequately protect themselves, perhaps because of the inconvenience of the technology.

Liimatainen (2005), in a study to search for usability problems of decentralized authorization systems, identifies various usability problems within systems security context and they include "authorization of entities, definition of a security policy for a resource, revocation of rights, checking validity of a set of credentials, privacy of users, and distinguishing trusted channels. Whitten and Tygar (1999) present that a security system is usable if, apart from other aspects, its users are aware of the security risks and know how to perform the necessary tasks. Additionally Al Abdulwahid et al. (2015) found that while users may be aware of the risks, yet they may not use some of the security mechanisms because of usability issues. Johnston, Eloff, and Labuschagne (2003) highlight the seemingly diverse goals of information security and human computer interaction. For example, the implementation of the most common security mechanism, such as passwords, needs to consider appropriately between security and usability. Otherwise, end-users tend to write down the passwords on notes, which completely make all the organizational policies and procedures null and void. Johnston et al. (2003) also point out that "even the most user-friendly interface could be avoided by users unless there are policies in place which enforce the use of security programs" (Johnston et al., 2003, p. 684). Some progress has been made where security and usability are being considered simultaneously. Kainda, Flechais, and Roscoe (2010), report the development of a proposed security-usability threat model, which help "understand and identify both system and external elements that are threats to a system's usability, security, or both". However, further research is required to assess when a user compromises security over usability and vice versa.

As noted, system security and system usability are core elements in the development of computer based information systems. For example, the security and usability are drives of mobile learning application and stakeholder satisfaction (Sarrab, Elbasir, & Alnaeli, 2016); web site security and usability have a significant effect on consumer trust in a financial services web site (Casalo, Flavián, & Guinalíu, 2007). In their detailed analysis of existing information systems and security research, Dhillon and Backhouse (2001) conclude that the overall security can be achieved by analyzing the behavior of constituent elements of the system. We extend this argument to postulate the core argument for this research that understanding the security and usability collectively is critical for the successful development, implementation and usage of computer based information systems. Findings of Andriotis, Oikonomou, Mylonas, and Tryfonas (2016) also support this contention. In their study Andriotis et al. found that most users prefer usability than security, particularly in the context of graphical passwords. Similarly Ruoti et al. (2016), while studying usability of secure emails, found that users prefer integrated solutions, where neither security nor usability is compromised. They also found that clarity of security procedures leads helps in building trust in the system.

As such, Dhillon and Torkzadeh (2006) used the Value Focused Thinking approach to explore and understand information system security in terms of the values of the people such as security professionals. Dhillon and Torkzadeh (2006) proposed a set of information system security objectives. Similarly, understanding the information systems usability from the perspective of the information system users and developing information system usability objectives is critical to align the security and usability objectives.

System security and system usability of computer based information systems can be immensely improved by defining the usability objectives and leveraging the existing security objectives developed by Dhillon and Torkzadeh (2006). Casting choices made by the IT stakeholders during the course of systems development process for information system security and usability as the decision making choices and defining and aligning the security and usability objectives paves the way for better development of computer based information systems.

In addition, the system security depends on the actions undertaken by the users and system administrators. Studying the existing security and usability objectives and their implementation will reveal the existing gaps and deficiencies for better security and usability. The main idea of this research is to understand the security and usability objectives within an information system and present them as design guidance for the software developers and engineers. Such design development guidance may be developed at various levels which will be helpful for the software developers and engineers (Faily, Lyle, Fléchais, & Simpson, 2015; Karat & Karat, 2003).

3. Value focused security and usability objectives

As mentioned above, methodologically this research builds on Keeney (1992) 'value focused thinking' approach. Keeney suggests that most decision-making methods are based on alternative thinking practices. He advocates that choices are made from available alternatives that are not numerous, and that are further constrained by the impositions of decision-makers. Individuals thereby tend to lose sight of what it is that they really hope to achieve. Since reaching a goal is the principal driver for being involved in any decision situation, Keeney argues that one should remain focused on the bottom-line objectives, and make decisions that are focused on meaning and value, instead of choosing only from among the alternatives found at hand. Value focused thinking is proposed as a method by Keeney, to address the most