Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2007 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2007

Aligning Information Systems Security and Usability Requirements for Computer-Based Information Systems

Santa Susarapu
Virigina Commonwealth University

ALIGNING INFORMATION SYSTEMS SECURITY AND USABILITY REQUIREMENTS FOR COMPUTER BASED INFORMATION SYSTEMS

by

SANTA RAM SUSARAPU
M.B.A., University of Nebraska, 2003
B.Com., Andhra University, India, 1995

Dissertation Chair: DR. GURPREET DHILLON
PROFESSOR, DEPARTMENT OF INFORMATION SYSTEMS

Dissertation Co-Chair: DR. H. ROLAND WEISTROFFER
ASSOCIATE PROFESSOR, DEPARTMENT OF INFORMATION SYSTEMS

Virginia Commonwealth University
Richmond, Virginia

Abstract

* * * * * * *

Key words: Information Systems, Security, Usability, Rep Grids, Personal Construct Theory

* * * * * * *

With extensive usage of information systems in the day-to-day business operations, organizations have been encountering several security and usability challenges. One such challenge is the alignment of information systems security and usability requirements while developing computer based information systems.

Information systems security and usability have been dominating several aspects of information systems research including systems development. Moreover, in the information systems development processes, information systems security and usability have traditionally been considered as add-on features and are not integrated into the systems development process. Yee (2004), argues that "security and usability elements cannot be sprinkled on a product like pixie due." Highlighting the current research gaps, Yee (2004) also emphasizes the compelling need for aligning information systems security and usability by incorporating both security principles and usability principles throughout the information systems development and design process.

Since the information systems security and usability aspects have not been integrated into the systems development process, the end users have to make certain choices between information systems security and usability features, which would result in unwarranted trade-offs between information systems security and usability. It is well known that if computer-based information systems are made more secure, they are less usable and if the systems are less secure, they are more usable (Cranor and Garfinkel 2005). Though the users choose between information systems security and usability by maximizing one component and compromising the other, there will certainly be a point where either information systems security or usability cannot be compromised any more than what they already are. Such a trade-off depends on information systems security and usability as dependent on individual users' values and cognitive beliefs, which in turn influence the security objectives and usability objectives. The current state of information systems literature and research has little focus on the user trade-offs between information systems security and usability. The basic premise for the proposed research is that

computer based information systems are get abandoned because fundamental usability criterion have not been met. Furthermore, such systems are weak in security and therefore pose a number of risks to the organization. Alignment of the information security and usability of information systems is critical for efficient and effective usage of the information system.

There are two informing pieces of literature that explain the current state of affairs. One body of literature can broadly be classified as 'information systems security research' which includes various sub-streams of literature including access controls, data security, behavioral aspects of security, etc. The second body of literature can be classified as 'usability research' which includes various sub-streams of literature, including, usability engineering, human computer interaction, etc. Both bodies of literature have their own assumptions and beliefs about the nature of knowledge and how information security and usability can or cannot be aligned all the way through the systems development life cycle. For the purposes of this dissertation, we adopt the definition of information security as defined within the ISO/IEC 17799 standard in the context of the C-I-A triad. The ISO/IEC 17799 defines information security as "the preservation of confidentiality (ensuring that information is accessible only to those authorized to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorized users have access to information and associated assets when required)." For the purposes of usability, we adoption the definition based on part 11 of ISO 9241 Standard (1998) which defines the word usability as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use." Though the above ISO standard is set forth for "evaluating the usability of a visual display terminal in terms of measures of user performance and satisfaction (ISO 9241)" and hence the definition is very specific to such circumstances, we believe that the basic concept of usability as the "extent to which an information system is used to achieve specific goals" fits very well with the overall theme of the current dissertation.

In this dissertation, we argue that there is an urgent need to align security and usability requirements for computer based information systems. We further argue that, in order to align information systems security and usability, understanding the objectives of information systems security and usability is critical. Such an understanding is necessary to effectively align the information systems security and usability requirements—or as we call them "usable security measures"—which need to be well integrated into the initial stages of information systems development life cycle. An integrated systems

development process with "usable security requirements" would not only secure the information systems efficiently and effectively but also enhance the overall usability of the information systems.

The primary objective of this research is to explore the issue of aligning the information systems security and usability requirements. To be more elaborate, within a specific information system instantiation, we would like to investigate the following:

- Based on the individual values and cognitive beliefs of the users of a specific instantiation of an information system, what are the initial security and usability objectives?
- Which of the above identified security and usability objectives are conflicting with each other and to what extent? How can we categorize and prioritize these objectives?
- Based on the conflicting nature of security and usability objectives, how these conflicting objectives can be aligned?

The main idea of this research is to understand the security and usability factors within a computer-based information system and present them as design guidance for the software developers and engineers. Such design development guidance will be developed at various levels of systems development which will be helpful for the software developers and engineers (Karat and Karat 2003).

Since the goal of the research is to understand the users' individual values and cognitive beliefs about information security and usability, we intend to use the "personal construct theory" and "repertory grid techniques" (Keeney 1996; Tan and Hunter 2002) to elicit such values and beliefs. With a careful selection of a specific business context and a particular information system user group, the planned research methods/techniques will enable the proposed research to be designed and conducted either as a single or as multiple case studies using case study design principles proposed by Yin (2003).

The primary outcome of this research will be the security and usability objectives that will help design a secure and usable computer based information systems. As Karat and Karat (2003, p. 537) argue that "progress in usability of systems for particular contexts is much more likely when the features of that context are brought into focus than when they are left in the background or ignored." The proposed research with the repertory grid techniques will provide insight into the ways in which information systems security and usability requirements can be aligned. Finding an alignment between the these security and usability requirements would enhance not only information systems development practices, but also enable organizations to better manage conflicting security and usability requirements.

References:

Cranor, L. F. and S. Garfinkel (2005). Security and usability: designing secure systems that people can use. Beijing Sebastopol, CA, O'Reilly.

ISO 9241 Standard (1998). Ergonomic Requirements for Office Work with Video Display Terminals. ISO 9241 Standard. Geneva, International Organization for Standardization.

Karat, J. and C. M. Karat (2003). "The evolution of user-centered focus in the human-computer interaction field." IBM Systems Journal **42**(4): 532-541.

Keeney, R. L. (1996). Value-Focused Thinking: A Path to Creative Decision-making.

Tan, F. B. and G. M. Hunter (2002). "THE REPERTORY GRID TECHNIQUE: A METHOD FOR THE STUDY OF COGNITION IN INFORMATION SYSTEMS." MIS Quarterly **26**(1): 39-57.

Yee, K.-P. (2004). "Aligning Security and Usability." IEEE Security & Privacy **5**(2): 48-55.

Yin, R. K. (2003). Case study research: design and methods. Thousand Oaks, Calif., Sage Publications.