U.S. DEPARTMENT OF ENERGY

PNNL-20201

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Situated Usability Testing for Security Systems

FL Greitzer

February 2011

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

This document was printed on recycled paper.
(9/2003)

PNNL-20201

Situated Usability Testing for Security Systems

FL Greitzer

February 2011

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Abstract

The purpose of this brief report is to document a research concept referred to as "situated usability testing" for application to evaluation of usability and utility of security systems. We suggest the application of a modified usability evaluation methodology referred to as ***situated usability testing*** in which the researcher studies the usability of the security tools (a secondary task) in the context of the users performing a primary task. This allows the researcher to evaluate the usability of security tools in a typical context – where use of the tool is not the primary task but rather is situated in the performance of a task whose goal is unrelated to security.

Acknowledgments

This work was carried out with financial support from the Pacific Northwest National Laboratory (PNNL) Information and Infrastructure Integrity Initiative (I4). PNNL is operated by Battelle Memorial Institute for the U.S. Department of Energy. The author wishes to express sincere thanks and gratitude to Deborah A. Frincke, I4 Initiative Lead, for her continuous support and advocacy for human-centric research and development to enhance effectiveness of cyber security systems. The author also thanks Dr. Barbara Endicott-Popovsky and Mr. Marc J. Dupuis for their comments and discussion about the ideas presented here. This report (May 2011) is slightly updated from the original work published in February 2011.

Contents

1.0 Introduction

1.1 Background

Usable security is a critical concept that has emerged in discussions aimed at ensuring the security and privacy of computer systems (National Research Council, 2010). In a broad sense, usability refers to how well a system supports the user's needs and ability to perform a desired task. The International Organization for Standardization (ISO) 9241-11 standard defines 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" (ISO 1998). Nielsen (1993; p. 26) and Shneiderman (1992) describe usability in terms of ease of learning, efficiency of use, memorability, reduced error rate and ease of recovery from errors, and (subjective) user satisfaction.

While usability testing is well established, assessing the usability of security software, tools, or methods deserves more careful consideration. It has been argued that dealing with security has become too difficult for individuals or organizations to manage effectively or to use conveniently (National Research Council, 2010). As difficult as it is for system administrators and developers to deal with, security is even more challenging for casual users. Indeed, it is much too easy for casual/home users to configure the security of their systems in non-optimal ways that leave their systems inadvertently insecure. This is exacerbated by the fact that casual users are focused on matters other than security, and likely would prefer not even to think about security. This brief report argues that when security and/or privacy are part of the equation, traditional methods for usability testing should be re-considered. The purpose of this brief report is to argue for and outline a method associated with a new approach to usability testing for examining usable security issues.

1.2 Rationale for Proposed Innovative Usability Testing Methodology

The questionable usability of security mechanisms is one of the reasons why casual users may lack confidence in the security of their systems or find ways to ignore security mechanisms. Traditionally, usability testing involves examining a user performing a task involving the specific tool under investigation in order to achieve a primary goal—we shall refer to this task as the *primary* task. The primary task supports the user's primary goal. In most application contexts, this is quite appropriate. For example, performing usability testing for a productivity tool such as a word processing program is rather straightforward as users use this tool to achieve a primary goal (e.g., write a report). However, when information security tools are used by casual users, it is often the case that the goals of the users are not directly related to the security software—thus, there may be a radically different context of use. In a real sense, in typical situations involving casual users of security software, it is most appropriate to consider the security task as a *secondary* task while the user focuses on the primary task. Indeed, a casual user may have a primary objective that is not heavily focused on computer security or that disregards computer security completely. The casual user may prefer not to think about computer security, even though this secondary task is an important requirement for reliably and safely accomplishing primary tasks. We suggest that when applying traditional usability testing methods in usable security research aimed at casual users, the appropriate context for the

participant is missing, which increases the likelihood that the researcher may draw incorrect conclusions.

This view is shared by recent usable security research. Birge (2009) observes it is possible some usable security usability tasks "force" participants to execute a security task, introducing bias (Wu et al., 2006) since the task may not be performed under normal circumstances: "The security issue being studied must be 'concealed' behind a different primary task that users will more readily accept." The mis-match between the testing environment and the real world may cause participants to provide different subjective usability ratings than in a realistic context. (Egelman et al. 2007). Birge argues, as we do, that "…new ideas for usability methods... [should be developed to] provide more reliability and ecological validity to studies of privacy and security (p. 223).

2.0 Proposed Solution: A "Situated" Usability Testing Methodology

2.1 Situated Usability Testing

The foregoing discussion suggests that the typical usability testing approach may yield uncertain or misleading results for security software or tools used by casual users because of the different context of use for security tools versus productivity tools that are well-aligned with user goals and tasks. This situation threatens experimental validity when security tools are tested using traditional usability testing methods that are used for productivity tools. When traditional usability testing methods are applied with casual users of security systems, the study may miss an appropriate context for user performance—this increases the likelihood that the researcher may draw incorrect conclusions. Therefore, we suggest the application of a modified usability evaluation methodology that we refer to as ***situated usability testing***. The researcher studies the usability of the security tools (a secondary task) in the context of the users performing a primary task. This allows the researcher to evaluate the usability of security tools situated in the performance of another task with another goal.

When traditional usability testing methods are applied with casual users of security systems, the study may miss an appropriate context for user performance—this increases the likelihood that the researcher may draw incorrect conclusions.

This sort of arrangement in experimental psychology research is referred to as *dual-task* performance experiments. Dual-task experiments are used to study performance on two tasks that are usually performed simultaneously or in close temporal proximity. Typically the secondary task is used to manipulate the user's workload to determine the impact on performance of the primary task. However, in the present context, the focus of the study is on the secondary task (from the perspective of the user, the security task) rather than the primary task. A degree of deception is required to maintain a proper context of use.

2.2 Illustrative Example

An example is online banking transactions that require various security controls such as authentication. Various security applications are encountered by users prior to beginning an online transaction. These functions are not the user's concern; they are required in order to move the user closer to the primary task. While a secure experience is desired, security concerns may not be high in the user's consciousness while performing the primary task. At best, security is a secondary goal. Thus, online banking is a good example of a situation where there is a primary task (making a banking transaction) and a concomitant secondary task that aims to ensure the primary task is executed with an acceptable level of security or privacy.

In the usability study, a realistic mock-up of an online bank with various security tools is employed to allow the researcher to study the usability of these tools directly, despite them not

being the focus of the actual users. Thus, the users will perform a variety of primary tasks (e.g., withdrawal, transfer, checking balances, transferring funds) while encountering varying secondary tasks involving the specific security tools employed. In the typical dual-task experiment, the more difficult or labor intensive the secondary task, the less cognitive resources are available for the primary task. In the proposed situated usability testing approach for security tools, we vary parameters of the primary task to manipulate cognitive load or stress level of the participant. In this way, one can examine the usability of security software under varying workload and environmental conditions.

3.0 References

Birge, C. 2009. Enhancing research into usable privacy and security. SIGDOC'09, October 5–7, 2009, Bloomington, Indiana, USA.

Egelman, S, J King, RC Miller, N Ragouzis, and E Shehan. 2007. Security user studies: methodologies and best practices. *CHI '07 extended abstracts on Human factors in computing systems*. San Jose, CA: ACM, 2833-2836.

International Organization for Standardization (ISO). 1998. *Ergonomics of Human System Interactions: Guidance on Usability (Part 11).* Geneva: ISO.

Nielsen, J. 1993. *Usability Engineering*. San Diego, CA: Academic Press.

Shneiderman, B. 1992. *Designing the User Interface: Strategies for Effective Human-Computer-Interaction.* Reading, Mass.: Addison-Wesley.

Steering Committee on the Usability, Security, and Privacy of Computer Systems; National Research Council. 2010. *Toward Better Usability, Security, and Privacy of Information Technology: Report of a Workshop*. Washington, D.C.: The National Academies Press. Also available from http://www.nap.edu/catalog/12998.html

Wu, M, RC Miller, and S Garfinkle. 2006. Do security toolbars actually prevent phishing attacks? *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06),* Montréal, Québec, Canada.

Pacific Northwest
NATIONAL LABORATORY

U.S. DEPARTMENT OF
ENERGY

Proudly Operated by Battelle *Since 1965*

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)
www.pnl.gov