Evaluating and Improving the User Interface for Password Management Software – A Case Study

Rob Tannen
Electronic Ink
One South Broad Street
Philadelphia, PA 19119
+1 215 922 3800
rtannen@electronicink.com

Kris Jackson
Wyeth
31 Morehall Road
Frazer, PA 19355
+1 484 563 3028
jacksok3@wyeth.com

James Temple
Electronic Ink
One South Broad Street
Philadelphia, PA 19119
+1 215 922 3800
jtemple@electronicink.com

ABSTRACT

This presentation discusses a real-world approach to applying usability to a password management solution. Usability was a primary driver in the selection and customization of an enterprise-wide password management and synchronization application. Analysis of the usability characteristics of four prospective applications contributed to the selection of one of the applications for proof of concept testing. During the proof of concept, the usability of the "out of the box" user interface was tested by having representative end users carry out core tasks with the application. The results of this testing were a set of usability issues to address in the customization phase. During this phase, prototype screens were designed to address problems related to terminology, workflow, navigation, password guidelines and authentication questions. Usability testing of the prototype led to further refinement. While this focus on usability led to an improved user interface, issues of security, and the impact of usability recommendations on security had to be balanced with ease of use.

1. INTRODUCTION

In many information technology driven organizations, a large amount of internal customer-support focuses on addressing password-related problems. In the current environment, user research discovered the potential users of this application had, on average, six separate passwords to maintain. Moreover, half of the participants reported they write down their passwords and call the help desk with password-related questions at least three times per year.

Password synchronization enables an end-user to apply a single password for multiple systems and applications, thereby minimizing the number of passwords that an individual needs to remember. Previous research and analyses on creating usable security applications have identified key points that make this such a challenge [1, 2, 3, 4, 5].

2. PHASE 1 - SOFTWARE SELECTION

At the project start, analyses of a number of available password management solutions determined the subset that met business and technical requirements.

Following this, four selected vendors presented their password management applications for review. The usability characteristics for each product were assessed via product demos and detailed vendor questionnaires and interviews. These characteristics were grouped around each applications software development process and the user interface itself. Criteria analyzed in scoring each application included visibility of secure status, clarity of terminology, user recovery from errors, availability of contextual user assistance, and the ability to customize the user interface.

The responses and data provided by each of the four vendors were combined with expert usability analysis of the product demos. Each application was rated on thirteen different usability-related criteria. The usability ratings for each vendor, weighted along with business and technical ratings provided a scorecard to guide the selection of the most suitable password management application among the four vendors.

3. PHASE 2 - PROOF OF CONCEPT USABILITY TESTING

The project team conducted usability testing with the selected application's default user interface to identify and prioritize issues that would affect user acceptance and effective usage of the application. The testing sessions provided an overview of the password management application's purpose and capabilities, including the ability to synchronize multiple passwords for different systems into one or more passwords, and for users to self-reset passwords without having to call the helpdesk.

Participants then attempted to complete key tasks including login, password change, setting up challenge questions and adding an application for password synchronization.

Objective and subjective measures were collected, including task completion success, errors and participant ratings and comments.

The usability testing resulted in the recommendation of over 25 user interface changes to the default version of the password management application. These recommendations related to labeling, navigation and task workflow. The pattern of findings suggested that cognitive complexity may have a greater impact on the usability than the number of steps to complete the task.

Among the numerous usability findings and associated recommendations, some were specific to the overall application design, while others were specific to the password management process. For example:

- When users are creating passwords, dynamically display the total number of characters entered to assist

users in meeting minimum password number-of - character requirements. Following this recommendation would not have a negative impact on security – rather it would ensure that system users are setting appropriate passwords, and minimize the need to re-enter non-conforming passwords.

- Eliminate case-sensitivity. When not feasible, always indicate if data entry fields are case-sensitive for both creating and authenticating passwords. While this recommendation reduces password complexity (by reducing the possible number of password variations) it was seen as a worthwhile tradeoff since it is expected to reduce the rates of forgotten and mis-entered passwords. High rates of these types of password failures lead to users writing down passwords and high customer support.

4. PHASE 3 – USER INTERFACE CUSTOMIZATION

4.1 Design

Paper prototype screens, or Wireframes, were created to document the initial redesign of the layout, content and workflow for the password management application. The Wireframes served as a reference to verify the redesigned user interface would be compatible with the underlying technology and security rules. Moreover, the Wireframes served as a tool to solicit stakeholder and user feedback to refine the interface prior to development. Several iterations of screens were paper-prototyped.

4.2 Prototype Usability Testing

Emphasis was placed on getting specific user input and feedback on authentication challenge questions. A set of open-response authentication questions were included for user feedback. The questions were drawn from vendor recommendations and project team expertise, and were specific for users within the United States. Just's guidelines for challege-question selection [6] were incorporated into the selection process. While previous work ascertained feedback on authentication questions [6], the current effort was conducted within the context of using the application. Measures on question response rate and memorability were collected.

The findings were consistent enough to rule-out several of the questions simply because a majority of participants could not effectively answer those questions.

- In some cases, participants were unable to answer certain authentication questions because they did not have an example in memory to draw from (e.g. high school mascot).
- Other questions were too difficult to remember for most participants (e.g. first grade teacher). Only one question was easily memorable by all participants (mother's maiden name), but risked being observed or measured.
- It was also determined that some questions could be answered if they were modified – for example, many participants could remember a childhood pet, but not necessarily their *first* pet.

These findings were taken into account to determine the final set of authentication questions for implementation.

5. CONCLUSIONS

By including comparative usability ratings as part of the selection of the application, the strengths and weaknesses of the user interface were recognized at the onset and could be proactively addressed prior to the rollout of the application.

While the implementation of the password management application is ongoing, the usability-focused approach has pro-actively addressed and improved the application's ease of use, while attempting to balance security concerns. In some cases, such as eliminating case-sensitive passwords, ease of use was considered to be significant enough to outweigh the increase in password complexity and security. This is because case-sensitive data entry can fail both due to cognitive and mechanical (e.g. Caps Lock key enabled) factors. Other potential recommendations, such as eliminating the requirement for a numeric character, were not applied because the tradeoff in ease of use was seen as less than the potential loss to security. In that instance, the cognitive workload alone was not sufficient to mandate reducing the security of the application.

6. REFERENCES

[1] Whitten, A. and Tygar, J.D. Usability of Security: A Case Study. *Carnegie Mellon University School of Computer Science Technical Report CMU-CS-98-155*, December 1998.

[2] Cranor, L.F. & Garfinkel, S. Secure or Usable?. *IEEE Security & Privacy, 2*, 5, (September-October 2004), 16-18.

[3] Yee, K Aligning Security and Usability. *IEEE Security & Privacy, 2*, 5, (September-October 2004), 48-55.

[4] Yee, K. User Interaction Design for Secure Systems. In *Proceedings of the International Conference on Information and Communications Security, 2002.*

[5] Nielsen, J. *Security and Human Factors.* Retrieved February 1, 2004, from http://www.useit.com/alertbox/20001126.html.

[6] Just, M. Designing and Evaluating Challenge-Question Systems. *IEEE Security & Privacy, 2*, 5, (September-October 2004), 32-39.