

Usability of Available Security Tools

Sponsoring faculty: Dr Rose Shumba (shumba@iup.edu)

Students: Sara Raffensperger, Louisa Ehinlaiye Ometere, Melissa A Karolewski
Computer Science Department
Indiana University of Pennsylvania

General Project Description

Designing security software that is usable enough to be effective is a specialized problem. Most available security tools are simply too difficult and confusing for the average computer user to manage correctly. User interface design strategies that are appropriate for traditional software do not seem to be sufficient enough to address the usability of security software. User interfaces for security software need to be improved. Improving user interfaces will help make security clear and intuitive so that most people can use the tools more effectively [15]. There are still no recognized exemplars of good interface design for security software. The result is that security issues are often ignored by users. The aim of this project is to initiate some groundwork on improving user interfaces for computer security software. This will be achieved through evaluation of user interfaces for commonly used security tools ¹against existing principles of good interface design for security software proposed by Whitten and Tygar [15] and Kerchhoff's laws [17]. The outcome from this project will be a collection of available principles for good user interface design for security software and a set of case studies on the usability of the tools.

Such work, if successful will extend the work that has been done before by the same group of female students. Through the ACM CREU 2004-2005 grant, a list of commonly used home security tools was identified [19]. The identified tools will form the basis for the formal evaluation to be carried out in this project. The formal evaluation used in the project is unique in that it integrates Human Computer Interaction (HCI) and security concepts. This is very important because, the development of security user interface design techniques requires expertise in security and HCI. This study is of interest not only because of the conclusions that we reach, but also because it can serve as an example of how to effectively evaluate the usability of computer security software. Ultimately, such work, if successful, will help find ways to make security sufficiently clear and intuitive that most people can use it effectively.

Specific questions/Hypothesis

1. What does the term usability for security mean?
2. Why is usability for security a special problem?
3. Why can't the traditional user interface techniques be used with security software?
4. How usable are available security tools?
5. What principles have been proposed to evaluate the usability of security software?

¹ Both home computer security tools and tools for teaching security courses will be considered

6. What does user interface design for effective security require?

Methods

Investigators will evaluate the usability of commonly used security tools against proposed general guidelines for evaluating the usability of computer security utilities and systems. The project will involve:

1. Carrying out some background research on:
 - a. HCI concepts:
 - i. Principles of good interface design as applied to traditional interfaces. Among other work [4], [5], [2], [6] and [7] will be studied.
 - ii. Usability testing. Different HCI usability testing methods will be studied; cognitive walkthrough and heuristic evaluation [11], [12], [13], [14].
 - b. Usability for security concepts. The focus will be on the following:
 - i. Why is usability for security a special problem?
 - ii. What does the term usability security mean?
 - iii. What are the characteristics of the usability problem for security? Some of the readings will include [3], [17], [20], [18].
 - iv. General principles for evaluating the usability of computer security utilities and systems. A number of principles have been proposed. Work by [15] and the Kerckhoffs' principles [17] will be studied.

The outcome from this part of the project will be a report comparing the traditional principles for good interface design with the principles for evaluating the usability of security software.

2. Identifying some commonly used security tools in the teaching of a security course. A questionnaire survey will be administered to the SIGSCE list. The aim of the questionnaire survey is to identify commonly used security tools for an information assurance course. A paper on the commonly used tools will be produced.
3. Evaluating the usability of security tools. Usability testing will be performed in a laboratory with participants selected to be representative of the general population of the security tool users. The tools identified in [19] and in 3 above will be evaluated. Morae, usability software, will be used to record the testing process. Morae is already installed in one of IUP laboratories. Users will be required to perform some task that involves the use of security. The aim of the usability testing is to identify security related problems that users of the tools might have. We anticipate at most 15 subjects will participate in the usability testing. Our lab
4. Developing case studies. Based on the results from the usability testing, case studies for each tool will be developed. The description of the participants, testing process, summaries of test session transcripts, and the most significant results observed from the test sessions will be the contents of the report.

Through a similar grant, all the investigators have worked on a security related project. One of the investigators has taken a Cybersecurity Basics course in the spring of 2005.

The sponsoring faculty has expertise in HCI. She currently teaches an HCI course at IUP. She therefore has the capability to supervise this work.

References

- 1) Norman, D; The Design of Everyday Things (Excerpt pp. 5-22); 1988.
- 2) National Cancer Institute. **Research-Based Web Design and Usability Guidelines**; <http://usability.gov/guidelines/>; 2000.
- 3) Garfinkel Simson; Keep It Simple; www.csconline.com
- 4) Jacob Nielson; **Information Pollution**; <http://www.useit.com>; 2003
- 5) Tufte, E; Graphics and Web Design Based on Edward Tufte's principles; <http://www.washington.edu/computing/training/560/zz-tufte.html>.
- 6) Ben Schneiderman; Designing User interfaces; Addison Wesley; 2000
- 7) John Carroll; Human Computer Interaction in the new Millennium; Addison Wesley; 2001.
- 8) Deborah Hix, Rex Hartson; Human Computer Interaction; Developing User Interface; Elements of user interface design; John Wiley; 2000.
- 9) Preece, Rogers and Sharp; Interaction Design: beyond human-computer interaction;; John Wiley, 2002.
- 10) Rubin Jeffrey: Handbook of Usability Testing; How to plan, design and conduct effective tests. John Wiley; 1994.
- 11) C. Wharton et. al. "The cognitive walkthrough method: a practitioner's guide" in J. Nielsen & R. Mack "**Usability Inspection Methods**" pp. 105-140.
- 12) Polson, P.G., Lewis, C., Rieman, J., and Wharton, C. (1992). Cognitive walkthroughs: A method for theory- based evaluation of user interfaces. International Journal of Man-Machine Studies 36, 741-773.
- 13) Wharton, C., Rieman, J., Lewis, C., and Polson, P. (1994). The Cognitive Walkthrough Method: A Practitioner's Guide. In Usability Inspection Methods, J. Nielsen and R.L. Mack (Eds.), New York: John Wiley & Sons, pp.105-141.
- 14) Wharton, C., Bradford, J., Jeffries, R., and Franzke, M. (1992). Applying cognitive walkthroughs to more complex user interfaces: Experiences, issues, and recommendations. Proceedings CHI92 (Monterey, CA, 3-7 May, 1992).
- 15) Whitten, A, Tygar, J. Usability of Security; Carnegie Mellon University Computer Science Technical Report CMU-CS-98-155, Dec 1998.
- 16) Clarke, V., Teague, G. (1994). Encouraging girls to study computer science - Should we even try? Australian Educational Computing. www.schools.ash.org.au/litweb/gender.html
- 17) Ross S, Security through Usability; www.securius.com.
- 18) Jacob N, Security and Human Factors, Useit.com, Alertbox, Nov 2000.
- 19) Raffensperger. S, Ometere L, Karolewski M, Coon A, Shumba R; Home Computer Security: A Survey; submitted for consideration for the CSSNE conference, 2005.
- 20) www.Suramya.com

Impact on the goal of CREU

The successful completion of this project will:

1. Provide a positive research experience for a team of undergraduate female students majoring in computer science.
2. Advance the knowledge and understanding of the relationship between information security issues and HCI issues by investigators through the stated background research and evaluation of security tools.
3. Provide an environment for exchange and dialog among the participating female investigators and the faculty. This will give value to girls' learning styles, skills and strengths. Many research studies report that boys often prefer to work alone on a computer problem, whereas girls prefer to work collaboratively in groups where they can explore the problem verbally [16].
4. Encourage participation by female students in a very unique computer application area, information assurance and Human Computer Interaction. It is believed that an exposure to a wide range of computer applications can help develop an appreciation of the uses of computers by female students.
5. Increase level of confidence by the workshop participants through hands-on exercises.

All the above will contribute towards the generation of interest and enthusiasm among the investigators and workshop participants hence motivate them into considering further studies in computer science. This is in line with the goal of CREU, to increase the number of women who continue on to graduate school in computer science.

Finally, the sponsoring faculty is a female whose research interests are in information assurance and gender and computer science. The faculty acting as a mentor will encourage the investigators to seriously consider pursuing graduate studies in computer science.

Student Activity and Responsibility

All the students will be involved with all the activities; however one student will be responsible for the successful completion of the activity.

Time	Student Activity	Student responsible
Fall 2005 (September 2005)	Background research report	Louisa Ometere
	Identification of security tools for teaching	Sarah Raffensperger
	Usability testing	Melissa
Spring 2006	Development of the case studies	ALL

Faculty Activity and Responsibility

1. Read and comment on the background research report.
2. Help with the design and administration of the questionnaire.
3. Chair weekly meeting with the female students.
4. Help with the usability testing
5. Supervise the production of the case studies.

Budget

Budget item	Cost
Copying of readings	\$ 20.00
Cost of usability testing subjects (15 @\$10)	\$ 150.00
Duplication cost (questionnaires)	\$ 50.00
Duplication of announcements	\$ 10.00
Travel to regional conferences	\$270.00

Informational Pages

Faculty pages

Name: Rose Shumba, Department of Computer Science, Indiana University of PA, Stright Hall, Indiana, PA 1570, shumba@iup.edu

Relevant background in the area:

Dr Rose Shumba has been teaching the Cybersecurity Basics course, Human Computer interaction and the Software Engineering course at IUP for the past 3 years. In 2003, she received a Senate Fellowship to improve and augment the teaching of the Cybersecurity Basics course at IUP. She developed tool-based instructional materials for the Cybersecurity Basics course. A poster presentation was accepted for the 2004 SIGSCE conference. In June 2003, Dr Shumba, Dr Oblitey and Dr. Micco received a CISCO equipment grant for \$88 000. The equipment, which included 15 PIX firewalls and 15 Cisco 2600 series routers, has been added to the existing 22-Linux server security laboratory. In summer of 2003, Dr Shumba worked on a project to incorporate information assurance issues into the software engineering curriculum. She is currently working on the development of standards for the network security program. In 2004, she developed an HCI course.

