Recommendations for a Graduate Seminar in Usable Security

Kent Seamons
Internet Security Research Lab
Brigham Young University
Provo, Utah, USA

1. INTRODUCTION

In the spring of 2006, I taught a graduate student research seminar on usable security at Brigham Young University (BYU). It was likely one of the first graduate seminars devoted exclusively to the nascent field of usable security. The course consisted primarily of readings from *Security and Usability*, a collection of papers in the field that had recently been edited by Cranor and Garfinkel [2]. Seven graduate students participated in the course. Students took turns presenting the papers, and all students brought a written critique to class that analyzed the papers scheduled for discussion. As a final project, each student designed a usability study related to a system or topic that interested them.

This seminar was instrumental in launching usable security as an emphasis in my research lab at BYU. Some recent lab projects included user studies in the areas of secure email [7] and secure web authentication [8]. My annual graduate security seminars since that time have continued to include several papers in the area of usable security. Next year, I plan to teach another graduate seminar devoted to usable security. This position paper outlines the student learning objectives for the seminar based on my nearly 10 years of experience in usable security research and education. It contains several recommendations for the usable security community to create resources that will assist educators and students in this field.

2. LEARNING OBJECTIVES

The course is intended for MS and PhD students and assumes no prior expertise in usability or security. The following are the learning objectives for a graduate seminar in usable security.

1. Learn by weekly practice to evaluate a research paper in the field of usable security.
2. Understand the common research methods for usability studies.
3. Understand standard usability metrics.
4. Understand standard statistical measures for analyzing user study data.
5. Complete training in ethical practices of experiments involving humans and how to obtain IRB approval.
6. Design a usability study by identifying an appropriate methodology for a problem and identifying the appropriate statistical methods to analyze the resulting data.
7. Be able to report the results from a user study in a way that is easy to understand.

The course is based on active learning principles where students present papers from the field, bring written critiques to class for papers that will be discussed, and conclude the course by designing a usability study for a problem that interests them.

3. RESEARCH METHODS

A core component to learning about the field of usable security is to read from the published research literature in the field. As I selected papers to study in my graduate seminars over the years, I made an effort to select a set that illustrates the common research methods in the field. For example, I've included papers that illustrate cognitive walkthroughs, laboratory user studies, Amazon Mechanical Turks surveys, and the use of grounded theory to analyze qualitative data gathered through in-depth interviews. As part of the course design process, I plan to create an annotated bibliography that organizes example papers according to the various research methods employed in the field for the purpose of educating new researchers.

An important area related to research methods is what kind of analytical techniques are appropriate for measuring and presenting research results. Another annotated bibliography that I envision is a taxonomy of papers in the field organized by the statistical methods they employ to analyze the results. This would be a detailed extension to the kind of advice contained in the paper by Stewart Schechter that warns authors of the pitfalls in submitting usability research to the SOUPS conference [10]. This paper provides excellent advice that would be valuable to students.

4. STANDARD METRICS

There are standard usability metrics that have been applied in usable security research. The most common metric is the System Usability Scale (SUS) [1], which I have used extensively in my own research. It is important to educate students on these standard metrics so that results can be compared to prior research. There is no reason to reinvent the wheel when suitable metrics have already been developed.

5. ETHICS

A usable security course must include a discussion of the ethical issues surrounding human subject experiments. The discussion can include an overview of the role if the Institutional Review Board (IRB) in approving usability studies. At BYU, the IRB requires all personnel in usability studies to complete on-line training provided by CITI [1]. I will have student in the course complete training that takes approximately two hours since I feel it provides useful background on the human issues to consider when designing user studies, including the gathering and protection of personally identifying information. There are several prior articles from the usable security community on the need for IRB approval that I believe are useful resources for students [4, 5].

6. TEXTBOOKS

I have not required a textbook in any of my prior graduate seminars. Instead, I rely on readings from the literature. However, there are several candidate textbooks that I believe will be of benefit to new students in the area and contribute to the learning objectives.

Garfinkel and Lipford/ [3] recently published *Usable Security: History, Themes, and Challenges*. It has valuable information for students learning about the area this is not conveniently contained in a single research paper. Some examples include definitions, a summary of why usability research is challenging, lessons learned, and a listing of significant open questions.

There are several recent books that provide information on conducting usability studies and analyzing the results. The first is *Handbook of Usability Testing: How to Plan, Design, and Conduct Effective Tests* by Rubin and Chisnell [6]. The three parts to the book are (1) Usability Testing: An Overview; (2) The Process for Conducting a Test; and (3) Advanced Techniques.

The second is *Quantifying the User Experience: Practical Statistics for User Research* by Sauro and Lewis [9]. It contains an in-depth introduction to the analytics that are relevant to usability testing, a description of some standard questionnaires for usability testing that includes the SUS metric that I have made extensive use of in my own usability research, and an appendix with a crash course in fundamental statistics concepts.

These last two books seem especially relevant if a course will include the students designing and conducting their own usability experiments. All of these books are available for new in the $30–40 range at Amazon, so they are affordable options for students.

7. CONCLUSIONS

This paper presents learning objectives for my next graduate seminar on usable security. The following are my recommendations to the community to develop resources to benefit usable security education.

1. Research methods: Create a taxonomy or annotated bibliography that categorizes papers according to the research methods employed in the analysis. A papers reading course should include a variety of papers that expose students to the various research methods in the field.

2. Analytics: Create a taxonomy of papers in the field that categorize papers according to the statistical methods used to analyze the data. This will help students be able to find strong and weak examples of data analysis in the field.

The Computer Science Department at BYU does not currently offer a graduate course in usability. In the long run, I may be able to attract more students to a general usability course. Broadening the scope may be a necessary step in making usability a permanent part of the curriculum. Most of the learning objectives and recommendations in this paper apply to usability in general, and not just usable security specifically. In order to generalize the course, I will use papers in usable security as examples of the general usability principles.

8. REFERENCES

[1] J. Brooke. SUS — a quick and dirty usability scale. In *Usability Evaluation in Industry*. CRC Press, 1996.

[2] L. F. Cranor and S. Garfinkel. *Security and usability: designing secure systems that people can use.* " O'Reilly Media, Inc.", 2005.

[3] S. Garfinkel and H. R. Lipford. *Usable Security: History, Themes, and Challenges*, volume 5. Morgan & Claypool Publishers, 2014.

[4] S. L. Garfinkel. Irbs and security research: myths, facts and mission creep. *Usabilty, Psychology, and Security (UPSEC'08)*, 8:1–5, 2008.

[5] S. L. Garfinkel and L. F. Cranor. Viewpoint: Institutional review boards and your research. *Communications of the ACM*, 53, june 2010.

[6] J. Rubin and D. Chisnell. *Handbook of Usability Testing, 2nd edition.* Wiley Publishing, Inc., 2008.

[7] S. Ruoti, N. Kim, B. Burgon, T. van der Horst, and K. Seamons. Confused Johnny: when automatic encryption leads to confusion and mistakes. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, page 5. ACM, 2013.

[8] S. Ruoti, B. Roberts, and K. Seamons. Authentication melee: A usability analysis of seven web authentication systems. In *Proceedings of the 24th international conference on World wide web.* International World Wide Web Conferences Steering Committee, 2015.

[9] J. Sauro and J. Lewis. *Handbook of Usability Testing, 2nd edition.* Morgan Kaufmann, 2012.

[10] S. Schechter. Common pitfalls in writing about security and privacy human subjects experiments, and how to avoid them. 2010.

[1] http://orca.byu.edu/IRB/irbtutorial.php