Usable Privacy and Security

Maritza Johnson, UC Berkeley School of Information
Serge Egelman, UC Berkeley and International Computer Science Institute

Course Description

When computers first came into prominence, security problems were mostly thought of as technical ones: vulnerabilities were exploited due to technical errors—software bugs that needed to be patched. However, as is demonstrated over and over again, the vast majority of modern software security issues stem from human factors. For instance, most software vulnerabilities are exploited because *humans* fail to apply patches in a timely manner; authentication systems that are difficult to use result in *humans* choosing weaker passwords (or bypassing security measures altogether); *humans* are tricked into downloading malware or divulging credentials via phishing; and Internet traffic is easily intercepted because *humans* fail to properly use encryption technologies.

As you will learn in this course, despite the fact that many security problems are caused by human error, in most cases, the users aren't to blame. Many security problems exist because software is simply *unusable*; when software engineers fail to account for the abilities and expectations of their users, those users will make preventable errors. Security and privacy systems can be made more usable by designing them with the user in mind, from the ground up. In this course, you will learn many of the common pitfalls of designing usable privacy and security systems, techniques for designing more usable systems, and how to evaluate privacy and security systems for usability. Through this course you will learn methods for designing software systems that are more secure because they minimize the potential for human error.

Prerequisites

Completion of at least one of the three core courses for the MICS degree program or permission of the instructor.

Course Objectives

1. Students will develop an appreciation for the importance of usability to security and privacy.
2. Students will learn how to evaluate the usability of a system in the context of security and privacy.
3. Students will learn how to assess the validity and strength of usability evaluations for privacy and security systems and features.
4. Students will learn about current research findings and methods in usable security and privacy.

Course Evaluation

- Async responses and reflections (10%)
- Live session participation (10%)
- Assignments (20%)
- Midterm (20%)
- Final project (40%)

Collaboration Policy

We encourage studying in groups of two to four people. This applies to working on homework, discussing material, and studying for the exam. However, students must always adhere to the UC Berkeley Code of Conduct (http://sa.berkeley.edu/code-of-conduct) and the UC Berkeley Honor Code (https://teaching.berkeley.edu/berkeley-honor-code). In particular, all materials that are turned in for credit or evaluation must be written solely by the submitting student or group. Similarly, you may consult books, publications, or online resources to help you study. In the end, you must always credit and acknowledge all consulted sources in your submission (including other persons, books, resources, etc.).

Assignments

When homework is assigned, it will be due two hours before the beginning of the live session.

Late Submission Policy

Solutions will be discussed during the live sessions of the course. Therefore, any assignment that is submitted after the deadline will be returned without grading and will receive a grade of zero.

Participation

Participation and taking an active part in every aspect of the course are key to internalizing the material of the course. Participation includes, but is not limited to, (i) active participation in live sessions, (ii) discussing assignments with other students, and/or (iii) activity in the class forum (by asking questions and/or contributing to answering other students' questions).

Readings

You will be provided with links to PDF versions of the assigned reading when available; see the weekly schedule below for more information.

Textbook

(Required) *Research Methods in Human-Computer Interaction* by Lazar, Feng, and Hochheiser.

Schedule

Unit 1: Usability and Security Systems

Reading

- Lazar et al., Chapter 1 Introduction
- Lazar et al., Chapter 2 Experimental Research
- A Framework for Reasoning About the Human in the Loop
- Usable Security: How to Get It

Assignments

- Assignment 1

Unit 2: Studying Decision Making

Reading

- "The Framing of Decisions and the Psychology of Choice"
- "Judgment Under Uncertainty: Heuristics and Biases"
- "Institutional Review Board (IRB) and Ethical Issues in Clinical Research"

Assignments

- Assignment 2

Unit 3: Research Methods (Experimental)

Reading

- Lazar et al., Chapter 3 Experimental Design
- Lazar et al., Chapter 10 Usability Testing
- Lazar et al., Chapter 12 Automated Data Collection Methods

Assignments

- Assignment 3

Unit 4: Research Methods (Descriptive and Relational)

Reading

- Lazar et al., Chapter 5 Surveys
- Lazar et al., Chapter 8 Interviews and Focus Groups
- Lazar et al., Chapter 9 Ethnography
- Lazar et al., Chapter 11 Analyzing Qualitative Data

Assignments

- No assignment this week. Check the website for updates about the synchronous session.

Unit 5: Statistics

Reading

- Lazar et al., Chapter 4 Statistical Analysis
- Choosing a Statistical Test

Assignments

- No assignment this week. Check the website for updates about the synchronous session.

Unit 6: Usable Security

Reading

- Why Johnny Can't Encrypt
- Users Are Not the Enemy
- The Emperor's New Security Indicators: An Evaluation of Website Authentication and the Effect of Role Playing on Usability Studies
- Simson Garfinkel's Thesis, Chapter 1.1–1.5, pp. 13–34, and Chapter 10.6 General Patterns and Patterns for Overall Security

Assignments

- Assignment 4

Unit 7: Privacy

Reading

- A Taxonomy of Privacy
- Privacy Indexes: A Survey of Westin's Studies
- Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting
- The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study

Assignments

- No assignment this week. Check the website for updates about the synchronous session.

Unit 8: More Usable Security

Reading

- No One Can Hack My Mind
- When Security Gets in the Way

Assignments

- Project proposal. Check the website for updates about the synchronous session.

Unit 9: Authentication

Reading

- Of Passwords and People: Measuring the Effect of Password-Composition Policies
- It's No Secret: Measuring the Security and Reliability of Authentication via "Secret" Questions
- It's Not What You Know, but Who You Know: A Social Approach to Last-Resort Authentication

Assignments

- Assignment 5

Unit 10: Access Control

Reading

- Anderson, R. (2008) *Security engineering: A guide to building dependable distributed systems*. Chapter 4. https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c04.pdf
- Maxion, R. A., & Reeder, R. W. (2005). Improving user-interface dependability through mitigation of human error. *International Journal of Human–Computer Studies, 63*(1–2), 25–50. http://www.robreeder.com/pubs/salmonIJHCS2005.pdf
- Mazurek, M. L., Arsenault, J. P., Bresee, J., Gupta, N., Ion, I., Johns, C., . . . Reiter, M. K. (2010). *Access control for home data sharing: Attitudes, needs and practices.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, https://www.archive.ece.cmu.edu/~lbauer/papers/2010/chi2010-home-access-control.pdf

Optional

- Bauer, L., Cranor, L. F., Reeder, R. W., Reiter, M. K., & Vaniea, K. (2009, April). *Real life challenges in access-control management*. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI. https://www.archive.ece.cmu.edu/~lbauer/papers/2009/chi09-management.pdf
- Johnson, M. L., Bellovin, S. M., Reeder, R. W., & Schechter, S. E. (2009). Laissez-faire file sharing: Access control designed for individuals at the endpoints. *New Security Paradigms Workshop*, NSPW. https://academiccommons.columbia.edu/doi/10.7916/D8D79J6W/download
- He, W., Golla, M., Padhi, R., Ofek, J., Durmuth, M., Fernandes, E., & Ur, B. (2018). *Rethinking access control and authentication for the home internet of things (IoT*). Proceedings of the 27th USENIX Security Symposium (USENIX Security 18). https://www.blaseur.com/papers/usenixsec18.pdf
- Jaferian, P., Rashtian, H., & Beznosov, K. (2014). *To authorize or not authorize: Helping users review access policies in organizations.* Proceedings of the 10th Symposium on Usable Privacy and Security, SOUPS. https://www.usenix.org/system/files/conference/soups2014/soups14-paper-jaferian.pdf

Assignments

- No assignment this week. Check the website for updates about the synchronous session.

Unit 11: Warnings

Reading

- Communication-Human Information Processing (C-HIP) Model
- You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings
- Experimenting at Scale With Google Chrome's SSL Warning

Assignment

- Assignment 6

Unit 12: Application Permissions

Reading

- Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). *Android permissions: User attention, comprehension, and behavior.* Proceedings of the 8th Symposium on Usable Privacy and Security. ACM. http://cups.cs.cmu.edu/soups/2012/proceedings/a3_Felt.pdf

Optional

- Kelley, P. G., Cranor, L. F., & Sadeh, N. (2013). *Privacy as part of the app decision-making process.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI.
- Egelman, S., Felt, A. P., & Wagner, D. (2013). Choice architecture and smartphone privacy: There's a price for that. In *The economics of information security and privacy.* Berlin, Germany: Springer, 211–236. https://www.guanotronic.com/~serge/papers/weis12.pdf
- Balebako, R., Jung, J., Lu, W., Cranor, L., & Nguyen, C. (2013). *Little brother's watching you: Raising awareness of data leaks on smartphones.* Proceedings of the 9th Symposium on Usable Privacy and Security, SOUPS. http://cups.cs.cmu.edu/soups/2013/proceedings/a12_Balebako.pdf
- Thompson, C., Johnson, M., Egelman, S., Wagner, D., & King, J. (2013). *When it's better to ask forgiveness than get permission: Attribution mechanisms for smartphone resources.* Proceedings of the 9th Symposium on Usable Privacy and Security, ACM. https://www.guanotronic.com/~serge/papers/soups13.pdf

Assignment

- Assignment 7

Unit 13: Secure Communication

Reading

- Unger, N., Dechand, S., Bonneau, J., Fahl, S., Perl, H., Goldberg, I. & Smith, M. (2015). *SoK: Secure messaging*. Proceedings of the 2015 IEEE Symposium on Security and Privacy, pp. 232–249, IEEE. https://oaklandsok.github.io/papers/unger2014.pdf

Optional

- Lerner, A., Zeng, E., & Roesner, F. (2017). *Confidante: Usable encrypted email: A case study with lawyers and journalists*. Proceedings of the 2017 IEEE European Symposium on Security and Privacy (EuroS&P), IEEE. https://www.franziroesner.com/pdf/confidante-eurosp17.pdf

- Edwards, W. K., Poole, E. S., & Stoll, J. (2007). *Security automation considered harmful?* Proceedings of the 2007 Workshop on New Security Paradigms, ACM. https://www.cs.drexel.edu/~greenie/cs680/nspw07-security-automation.pdf
- Smetters, D. K., & Grinter, R. E. (2002). *Moving from the design of usable security technologies to the design of useful secure applications.* Proceedings of the 2002 Workshop on New Security Paradigms, ACM. https://www.nspw.org/2009/proceedings/2002/nspw2002-smetters.pdf

Assignment

- Assignment 8

Unit 14: Privacy Policies

Reading

- User Interfaces for Privacy Agents
- What Do Online Behavioral Advertising Privacy Disclosures Communicate to Users?
- A Comparative Study of Online Privacy Policies and Formats

Optional

- Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice

Assignment

- Final Project due. Check the website for updates about the synchronous session.