A Body of Knowledge for Usable Security and Privacy Education

Heather Lipford
University of North Carolina at Charlotte
Department of Software and Information Systems
9201 University City Blvd.
Charlotte, NC 28223 USA
heather.lipford@uncc.edu

Yousra Javed
University of North Carolina at Charlotte
Department of Software and Information Systems
9201 University City Blvd.
Charlotte, NC 28223 USA
yjaved@uncc.edu

Abstract
The importance of usability in security and privacy technologies is now widely accepted. A vibrant and growing research community in usable security and privacy has contributed a wide range of results in the past 15 years. Despite this, the vast majority of computing students are being exposed to very little of this discipline. This poster describes our ongoing efforts to enable broader education in this area. We are leading the construction of a body of knowledge for usable security and privacy education, to serve as an organizing framework for the discipline. We define a comprehensive list of the topics in this field.

Introduction
The usability evaluation of PGP 5.0 in 1999 (proving PGP encryption unusable), demonstrated the importance of usability in security and privacy technologies [3]. Since then, a vast amount of research has been conducted on the application of HCI principles to the design and evaluation of security and privacy systems.

A variety of usable security courses are being taught, particularly by researchers within the SOUPS community. These courses are often electives taught to senior or graduate students, organized around the common and recent research themes in the field. One potential barrier to expanding the breadth and depth of usable security and privacy education across computing programs is the lack of

a framework or body of knowledge defining what students could and should know about usable security and privacy. How do we translate the research themes and results in the field into educational topics? What are the knowledge units, skills, and learning objectives for general computing and/or security students? Such a framework could also provide topic consistency and guidance on how to integrate those knowledge units into existing and new courses; and on the types of learning materials that need to be developed based upon the current and future research results.

In this poster, we describe work in progress on an NSF-funded effort to transform education in usable security and privacy, with a framework organizing this discipline, and online resources for students and faculty. Our goal is to inform the broader computing community about usable security and privacy education and this project, and to solicit feedback and participation. In this poster, we focus on the knowledge units.

Body of Knowledge

A body of knowledge is the set of concepts and activities that make up a domain. For example, the ACM Curricular Guidelines define the concepts for computer science undergraduate education [2]. The US National Security Agency has defined an extensive set of knowledge units in information security, however usability is mentioned as one sub topic of the knowledge unit on Security Design Principles [1]. Similarly, we aim to define the knowledge units that comprise usable security and privacy. This work began at the Workshop on Usable Security and Privacy education held at SOUPS 2015. Participants brainstormed topics and learning objectives in usable security and privacy. We collected all of the brainstorming outcomes and performed affinity diagrams to cluster related topics into a set of knowledge units. These were further refined with feedback from other experts in the field. In this poster, we present this first complete draft of the knowledge units, and seek feedback from the broader usable security and privacy community. The full body of knowledge is available for viewing and comment at http://hci.uncc.edu/usable-security-privacy-bok/.

This section presents a breakdown of usable security and privacy educational topics. Numbered topics were created by clustering sets of related topics.

Knowledge Units

We present the initial knowledge units as a set of topics and subtopics that define the field of usable security and privacy. Note that these are not meant to be a course syllabus or map to one specific course (although a course in usable security is likely to cover all of these topics), but an organization of the knowledge of the field more generally. As we refined these topics, we realized that some knowledge that students may need to learn or understand is not specific to the field itself - for example, quantitative and qualitative evaluation methods. We refer to these as supporting knowledge, and instead focus on the knowledge that is specific to the field. The below knowledge units are not presented in any particular order.

1. User Foundations
    - Overarching user issues impacting security and privacy, such as the notion that humans are the weakest link and that security and privacy are secondary tasks
    - The aspects of human cognition related to security and privacy perceptions and behaviors, including mental models, cognitive biases, and risk perceptions
    - Behavioral economics specific to Usable Privacy and Security
    - Cultural and demographic differences related to security and privacy concerns and behaviors

2. Privacy
    - Various privacy definitions and theories, and their application to computing scenarios and technologies
    - Privacy attitudes and measurement, and the relationship (or lack thereof) of attitudes to behavior
3. Privacy notifications and controls
    - The concept of notice and choice, and the implications for privacy notices
    - The usability of online privacy policies and privacy policy interfaces
    - User concerns and behaviors with app (such as Android) permissions
    - Mechanisms and interfaces for policy and permissions communciation
    - Machine-readable policies, such as P3P, and their uses and issues
4. Encryption
    - Usability of email and message encryption tools
    - User perceptions of encryption, including SSL
5. End-user access control
    - How people manage and control the sharing of files, photos, and other media
    - Usability of interfaces and mechanisms for performing access control
    - Non-traditional mechanisms, such as reactive or real-time access control
6. Authentication
    - The various types of authentication mechanisms, including passwords, graphical passwords, biometrics, tokens, and their variations
        - People's perceptions towards each mechanism
        - People's behaviors and their security implications
        - Tradeoffs in usability, security, and deployability of the various mechanisms
    - Authentication challenges with mobile devices
    - Multi-factor authentication
    - Secondary or fall-back authentication, including challenge questions
    - CAPTCHAs
7. Warnings
    - Usability of the common types of warnings that users encounter, such as certificate, malware, and phishing warnings
    - Risk communication theories and methods
    - Design guidelines for improving warnings
8. Phishing and social engineering
    - Why people are susceptible for falling for phishing attacks
    - Cues to help people detect phishing attacks
    - User education to train users how to not fall prey to phishing attacks
9. End-user security tools
    - Usability of tools for personal and computer security, e.g., firewalls,and anti-virus software
    - Device pairing methods and their implications for user behavior and security
10. Tracking technologies
    - Web tracking technologies and applications, including behavioral advertising
        - User perceptions on web tracking and its uses
        - Usability of software to prevent web tracking
        - Software for online anonymity
    - Location tracking
        - Perceptions and behaviors of sharing location with other people

    - Perceptions and behaviors of sharing location with applications and organizations
  - Behavioral tracking
    - Security and privacy issues regarding applications and devices for tracking other kinds of real world behavior, such as step counts.

11. Social media privacy
    - Social theories of privacy and their relevance to social media sites
    - Privacy behaviors and concerns of users of social media sites
    - Interfaces and mechanisms for managing social media privacy
12. Administrators and Expert tools
    - The general work tasks and needs of security administrators
    - The usability of specific expert tools, such as firewalls, IDS/IPS interfaces, etc.
    - The use of visualization for security information
    - Design guidelines and heuristics for expert security tools
13. Design Principles
    - General design principles for usable security and privacy, such as safe and secure defaults, automating security, placing decisions in context.
    - Security and privacy nudges
    - Visualization for security and privacy interfaces
14. Design Process
    - Secure interaction design process
    - Privacy sensitive design
    - Human in the loop framework
15. Security and Privacy processes
    - Incentives and disincentives for users to adhere to security policies or behave securely
    - Methods for security compliance and achieving a culture of security within an organization
    - Strategies and outcomes for security/privacy user education
    - End-user security/privacy advice, and how users learn such advice
16. User studies of security and privacy
    - Deception studies and ethical considerations
    - Ecological validity of security/privacy studies
    - Measuring security and privacy knowledge, attitudes, and behaviors
17. Emerging technologies
    - The potential usable security and privacy issues and user concerns in emerging technologies and domains, including cloud computing and cloud storage, healthcare, smart meters, and the Internet of Things.

Conclusion

In this poster, we describe work in progress on an NSF-funded effort to transform education in usable security and privacy, with a framework organizing this discipline, and online resources for students and faculty. We present the initial knowledge units as a set of topics and subtopics that define the field of usable security and privacy. A final draft of the entire body of knowledge will be available at our project website at http://hci.uncc.edu/usable-security-privacy-bok/. We hope this body of knowledge can help to drive further curricular development efforts to broaden the opportunities for more students to learn about usable security and privacy.

Acknowledgments

We thank the participants of the Workshop on Usable Security and Privacy Education. This work is funded by the National Science Foundation #1500052.

REFERENCES

1. National Security Agency. 2013. National Centers of Academic Excellence in Information Assurance/Cyber Defense (IA/CD) Knowledge Units. (June 2013). http://www.cisse.info/pdf/2014/2014%20CAE%20Knowledge%20Units.pdf.

2. Association for Computing Machinery (ACM) and IEEE Computer Society. 2013. Curriculum Guidelines for Undergraduate Degree Programs in Computer Science. (Dec 2013). http://www.acm.org/education/CS2013-final-report.pdf.

3. Alma Whitten and J. D. Tygar. 1999. Why Johnny Can'T Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8 (SSYM'99)*. USENIX Association, Berkeley, CA, USA, 14–14. http://dl.acm.org/citation.cfm?id=1251421.1251435