Announcement and Call for Papers USENIX

Usability, Psychology, and Security 2008

Sponsored by USENIX, The Advanced Computing Systems Association

http://www.usenix.org/upsec08

April 14, 2008 **San Francisco, CA, USA**

Co-located with the 5th USENIX Symposium on Networked Systems Design & Implementation (NSDI '08), which will take place April 16–18, 2008, and the First USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '08), which will take place April 15, 2008

Important Dates:

Submissions due: *January 25, 2008*
Notification of acceptance: *February 28, 2008*
Final papers due: *March 18, 2008*

Workshop Organizers

Program Chairs

Elizabeth Churchill, *Yahoo! Research*
Rachna Dhamija, *Harvard University*

Program Committee

Steven M. Bellovin, *Columbia University*
Dan Boneh, *Stanford University*
Coye Cheshire, *University of California, Berkeley*
Julie Downs, *Carnegie Mellon University*
Stuart Schechter, *Microsoft Research*
Sean Smith, *Dartmouth University*
J.D. Tygar, *University of California, Berkeley*
Paul Van Oorschot, *Carleton University*

Overview

Information security involves both technology and people. To design and deploy secure systems, we require an understanding of how users of those systems perceive, understand, and act on security risks and threats.

This one-day workshop will bring together an interdisciplinary group of researchers, systems designers, and developers to discuss how the fields of human computer interaction, applied psychology, and computer security can be brought together to inform innovations in secure systems design. We seek to deepen the conversation about usable security to go beyond the user interface, toward developing useful and usable *systems* of humans and technology.

Topics

Topics include but are not limited to:

- Error detection and recovery
- Human perception and cognitive information processing
- Identity and impression management
- Individual and cultural differences
- Information seeking and evaluation
- Judgment and decision-making
- Learning, training, and experience
- Mental models
- Models of privacy, sharing, and trust
- Organizational, group, and individual behavior
- Risk perception, risk analysis, and risk communication
- Security behavior study methodology
- Social engineering
- Social influence and persuasion
- System proposals and design approaches
- Threat evaluation
- Usability
- User motivation and incentives for secure behavior

The study of human attention, learning, reasoning, and behavior addresses issues of central relevance to computer security. For example:

- Security weaknesses often arise from biases in human perception and cognitive information processing. For example, phishing attacks use confusing perceptual cues and fear to trick users into revealing sensitive information.
- Assessing, creating, and managing secure systems requires ongoing information seeking and information evaluation, as new threats emerge constantly. However, understanding complex and dynamic systems is time-consuming and error-prone, and users have little motivation to spend the time and effort that is required.

- The perception of risk can influence users' willingness to employ security mechanisms or engage in risky behavior. However, risk perception and decision-making are often based on limited domain knowledge and are subject to bias; we underestimate some risks and exaggerate others.
- People's level of confidence in their risk assessments can be perceptually and socially manipulated, independent of actual risks. Attackers (and system designers) often create the perception of security, even when none exists.
- Human reasoning follows certain patterns, which are subject to change with experience. Through training and education, we can help users to learn methods and procedures and develop mental models of how security systems work.
- People learn through interaction with others. Models of social influence suggest that information garnered from a trusted source can affect people's behavior or attitudes, but the level of trust conferred on others is dependent on situational factors. Organizational factors and group behavior can also have a large effect on individual behavior.
- Approaches to risk assessment, identity and impression management, and trust vary from one individual to another and also vary by culture.

Submissions

Usability, Psychology, and Security 2008 invites insightful new contributions that apply aspects of human/computer interaction and applied psychology to solving problems in computer security. We invite submissions in two categories.

1. **Short papers:** We encourage short papers that describe innovative work in progress or position papers that map out directions for future research or design. Short papers should be no longer than five (5) pages.
2. **Full papers:** Full papers may describe systems, case studies, fieldwork descriptions, experimental studies, and design frameworks. Full papers must be no longer than ten (10) single-spaced 8.5" x 11" pages, including figures, tables, and references.

All submissions should offer new contributions that have not been published elsewhere. Author names and affiliations should appear on the title page. Submissions must be in PDF and must be submitted via the form on the Usability, Psychology, and Security 2008 Call for Papers Web site, http://www.usenix.org/upsec08/cfp.

Papers accompanied by nondisclosure agreement forms will not be considered. All submissions will be treated as confidential prior to publication in the Proceedings.

Simultaneous submission of the same work to multiple venues, submission of previously published work, and plagiarism constitute dishonesty or fraud. USENIX, like other scientific and technical conferences and journals, prohibits these practices and may, on the recommendation of a program chair, take action against authors who have committed them. In some cases, program committees may share information about submitted papers with other conference chairs and journal editors to ensure the integrity of papers under consideration. If a violation of these principles is found, sanctions may include, but are not limited to, barring the authors from submitting to or participating in USENIX conferences for a set period, contacting the authors' institutions, and publicizing the details of the case.

Note, however, that we expect that many papers accepted for the workshop will eventually be extended as full papers suitable for presentation at future conferences.

Authors uncertain whether their submission meets USENIX's guidelines should contact the Program Chair, upsec08chairs@usenix.org, or the USENIX office, submissionspolicy@usenix.org.

Accepted papers will appear in the workshop Proceedings, which will be published on the USENIX Web site.

History

This workshop evolved from Usable Security (USEC'07). The USEC'07 program and papers are available on the workshop Web site, http://www.usablesecurity.org.