

# Security User Studies: Methodologies and Best Practices

## INTRODUCTION

As networked computing weaves itself into many aspects of daily life, ensuring the security of networked systems is becoming vitally important. Interest in usable security -- the research, development, and study of systems that are both usable and secure -- has been growing both in the CHI and information security communities in the past several years. Despite this growing interest, however, the process of conducting effective, ethical security-related user studies remains daunting. Users deal with security infrequently and irregularly, and most do not notice or care about security until it is missing or broken. Security is rarely a primary goal or task of users, making many traditional HCI evaluation techniques difficult or even impossible to use.

This workshop, held in conjunction with the ACM CHI 2007 conference, will bring together researchers and practitioners from the HCI and information security communities to explore methodological challenges and best practices for conducting security-related user studies, including:

- **Study Design:** How can evaluators design studies that are faithful to the fact that in the real world, security is almost never a primary goal? How can evaluators motivate study participants to complete security-related tasks without overemphasizing security? How should evaluators even decide what to test in a security user study? How can researchers handle the problem that users may claim to take particular steps to protect their security, but in reality do something else?
- **Ethical Issues:** How can evaluators conduct realistic studies involving attacks on users, yet at the same time protect study participants from harm or embarrassment? When is it appropriate to launch security attacks or employ deception in studies?
- **Lessons Learned & Best Practices:** Why have previous security user studies succeeded or failed? What are best practices for security user studies? What would security user study processes, checklists, and criteria look like?

## JOINING THE WORKSHOP

People interested in joining the workshop should submit a position paper of up to four pages along with a cover letter describing their research interests and background in this area to Erika Shehan ([erika@cc.gatech.edu](mailto:erika@cc.gatech.edu)) by January 12, 2007.

We encourage submissions from practitioners as well as researchers interested and involved in all forms of empirical usable security research. Position papers may describe prior empirical work in usable security (including successes or difficulties encountered), discussions of specific problems associated with security-related user studies, and proposals for possible user studies (both realistic and outlandish). Position papers will be reviewed for relevance, overall quality, and potential to generate discussion. To facilitate interaction, the workshop will be limited to twenty participants. Prior experience with security user studies is recommended, but submissions from enthusiastic newcomers to usable security will be warmly welcomed. Please note that at least one of the authors of an accepted paper needs to register for the workshop and one day of the CHI 2007 conference.

Additional information about the workshop is available online at <http://www.verbicidal.org/hcisec-workshop>.

## IMPORTANT DATES

12 January 2007, 5:00 PM (1700) PDT:

February 1, 2007:

April 28, 2007:

Position papers due

Authors notified of acceptance

Workshop date