USEC 2014

Workshop on Usable Security

23rd February 2014

Co-located with

NDSS

San Diego, California.

http://www.usecap.org/usec14.html

Many aspects of information security combine technical and human factors. If a highly secure system is unusable, users will try to circumvent the system or move entirely to less secure but more usable systems. Problems with usability are a major contributor to many high-profile security failures today.

However, usable security is not well-aligned with traditional usability for three reasons. First, security is rarely the desired goal of the individual. In fact, security is usually orthogonal and often in opposition to the actual goal. Second, security information is about risk and threats. Such communication is often unwelcome. Increasing unwelcome interaction is not a goal of usable design. Third, since individuals must trust their machines to implement their desired tasks, risk communication itself may undermine the value of the networked interaction. For the individual, discrete technical problems are all understood under the rubric of online security (e.g., privacy from third parties use of personally identifiable information, malware). A broader conception of both security and usability is therefore needed for usable security.

The workshop on Usable Security invites submissions on all aspects of human factors and usability in the context of security and privacy. USEC'14 aims to bring together researchers already engaged in this interdisciplinary effort with other computer science researchers in areas such as visualization, artificial intelligence and theoretical computer science as well as researchers from other domains such as economics or psychology.

We invite authors to submit original papers describing research or experience in all areas of usable privacy and security. We particularly encourage collaborative research from authors in multiple fields. Topics include, but are not limited to:

- Evaluation of usability issues of existing security & privacy models or technology
- Design and evaluation of new security & privacy models or technology
- Impact of organizational policy or procurement decisions
- Lessons learned from designing, deploying, managing or evaluating security & privacy technologies
- Foundations of usable security & privacy
- Methodology for usable security & privacy research
- Ethical, psychological, sociological and economic aspects of security & privacy technologies

New at USEC'14:

- Reports of replicating previously published studies and experiments
- Reports of failed or negative usable security studies or experiments, with the focus on the lessons learned from such experience.
- Reports on deploying usable security & privacy technology in industry

It is the aim of USEC to increase the scientific quality of usable security and privacy research. To this end we encourage the use of replication studies to validate research findings. This important and often very insightful branch of research is sorely underrepresented in usable security and privacy research to date. Papers in these categories should be clearly marked as such and will not be judged against regular submissions on novelty. Rather they will be judged based on scientific quality and value to the community. Please contact the chairs in advance of submitting such work.

Submissions and Important Dates
Papers should be written in English. Papers must be no more than 8-10 pages total (including the references and appendices). Papers must be formatted for US letter size (not A4) paper in a two-column layout, with columns no more than 9.25 in. high and 3.5 in. wide. The text must be in Times font, 10-point or larger, with 11-point or larger line spacing. Authors are encouraged to use the IEEE conference proceedings templates found at http://www.computer.org/portal/web/cscps/formatting

We also invite short papers of up to 6 pages covering work in progress, novel or provocative ideas, replication or failed experiment studies. These will be selected based on their potential to spark interesting discussions during the workshop.

Submission site: https://usec2014.cs.berkeley.edu/
Submissions deadline: ~~**6th of November 2013**~~ **13th December 2013**
Notification: ~~**5th January 2014**~~ **18th January 2014**
Camera ready: ~~**15th January 2014**~~ **26th January 2014**

Venue
NDSS Symposium 2014
February 23-26 will be the dates for the 2014 Network and Distributed System Security (NDSS) Symposium. The venue will be the Catamaran Resort Hotel and Spa in San Diego, California.

Steering Committee:
Jean Camp, Indiana University
Jim Blythe, University of Southern California
Angela Sasse, University College London

Chairs:
Matthew Smith (LUH) and David Wagner (UC Berkeley)

Replication-Study Track Chair:
Marian Harbach (LUH)

Keynote Speaker:
Serge Egelman, UC Berkeley

Program Committee:
Alessandro Acquisti, CMU Heinz College
Andrew A. Adams, Meiji University, Tokyo
Ross Anderson, University of Cambridge
Pamela Briggs, Northumbria University
Dirk Balfanz, Google
Lorrie Faith Cranor, CMU
Sunny Consolvo, Google
Alexander De Luca, LMU
Serge Egelman, UC Berkeley
Sascha Fahl, LUH
Neil Gandal, Tel Aviv University
Peter Gutmann, University of Auckland
Seda Gürses, New York University
Tiffany Hyun-Jin Kim, CMU
Maritza Johnson, Facebook
Yoshi Kohno, University of Washington
Sameer Patil, Helsinki Institute for Information Technology
Andrew Patrick, Carleton University
Rob Reeder, Google
Hovav Shacham, UC San Diego
Sara Sinclair, Google
Douglas Stebila, Queensland University of Technology
Kami Vaniea, Michigan State University
Eugene Y. Vasserman, Kansas State University
Rick Wash, Michigan State University