SOUPS 2012

Proceedings of the

Eighth Symposium On Usable Privacy and Security

**Washington, DC, USA
July 11-13, 2012**

http://cups.cs.cmu.edu/soups/

CyLab Usable Privacy & Security Laboratory
HTTP://CUPS.CS.CMU.EDU

**Carnegie Mellon
CyLab**
CONFIDENCE FOR A NETWORKED WORLD

isr **institute for
SOFTWARE
RESEARCH**

Foreword

Welcome to the Eighth Symposium On Usable Privacy and Security! This year's program features 14 technical papers, one workshop, one tutorial, 14 posters, 13 posters published in the past year at other conferences, a panel, lightning talks and demo session, and an invited talk. On Thursday evening SOUPS 2012 attendees will enjoy a dinner at the Microsoft DC office.

This year we received 67 technical paper submissions. The program committee provided two rounds of reviews. In the first round papers received an average of three reviews. In the second round, papers that had received one or more reviews better than "weak reject" in the first round received additional reviews. The goal of the second round was to ensure that a consistent standard of acceptance could be applied across all papers and, to this end, papers received as many as six reviews. We held an in-person program committee meeting on May 11. Fourteen papers were selected for presentation and publication.

The technical papers committee selected the paper "Android Permissions: User Attention, Comprehension, and Behavior" by Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner to receive the best paper award. Through two comprehensive user studies, this paper thoroughly examines the timely topic of users' understanding of the Android application permissions.

SOUPS 2012 features an invited talk by Julie Brill on "Privacy in the mobile world: A big task on a small screen." In her remarks, Commissioner Brill will discuss the privacy implications of the increasing shift of consumers' online experiences to the mobile environment. Among other topics, she will discuss children's privacy in the mobile space, issues surrounding effective disclosures on mobile devices, and the privacy implications of mobile payments.

The closing session will feature a panel titled: "Will No Humans be Harmed? The argument against IRB approval for some human subjects research." After what is sure to be a lively discussion, we will conclude with the traditional SOUPS ice cream social.

This is the eighth year of SOUPS and the first time SOUPS has been held in Washington, DC. We are excited to have the opportunity to engage policy makers and government agency staff in discussions about usable privacy and security. We are also pleased to award SOUPS travel scholarships to twenty students, thanks to a grant from the National Science Foundation.

We would like to thank all of the authors and the members of the technical papers committee and organizing committee for helping to produce this program. We are grateful to everyone whose assistance with logistical arrangements made this event possible: the staff at CyLab, the Institute for Software Research, and the Engineering & Public Policy department at Carnegie Mellon University, and the CyLab Usable Privacy and Security (CUPS) Laboratory student volunteers. We would also like to thank CyLab, the National Science Foundation, Microsoft, Nielsen, and RIM for their sponsorship of this event, and ACM for publishing our proceedings in the ACM Digital Library. SOUPS 2012 is held in cooperation with ACM SIGCHI.

Lorrie Faith Cranor
General Chair
Carnegie Mellon University

Heather Richter Lipford
Technical Papers Co-Chair
University of North Carolina at Charlotte

Konstantin Beznosov
Technical Papers Co-Chair
University of British Columbia

SOUPS 2012 Organization

General Chair:	Lorrie Faith Cranor, Carnegie Mellon University
Interactive Sessions Chair:	Lujo Bauer, Carnegie Mellon University
Invited Talks and Panels Chair:	Janice Tsai, Microsoft
Local Activities Chair:	Jeremy Epstein, SRI International
Poster Session Co-Chairs:	Sonia Chiasson Carleton University Kirstie Hawkey, Dalhousie University
Technical Papers Co-Chairs:	Heather Richter Lipford, University of North Carolina at Charlotte Konstantin Beznosov, University of British Columbia
Tutorials and Workshops Chair:	Sylvie Noel, Communications Research Centre Canada
Technical Papers Committee:	Alessandro Acquisti, Carnegie Mellon University Lujo Bauer, Carnegie Mellon University Robert Biddle, Carleton University L. Jean Champ, Indiana University Sonia Chiasson, Carleton University Lynne Coventry, Northumbria University Alexander De Luca, University of Munich Rachna Dhamija, Usable Security Systems Serge Egelman, University of California, Berkeley Simson L. Garfinkel, Naval Postgraduate School Cormac Herley, Microsoft Research Apu Kapadia, Indiana University Andrew Patrick, Office of the Privacy Commissioner of Canada Rob Reeder, Microsoft Michael Reiter, University of North Carolina at Chapel Hill Stuart Schechter, Microsoft Research Diana Smetters, Google Rick Wash, Michigan State University Mary Ellen Zurko, Cisco
U-PriSM Workshop Organizers:	Jaeyeon Jung, Microsoft Research Sonia Chiasson, Carleton University
Hacking Public Policy Tutorial Leaders:	Janice Tsai, Microsoft Harlan Yu, Princeton University

Table of Contents

Mobile Privacy and Security

User Perceptions

Authentication

Online Social Networks

Access Control

SOUPS 2012 Program

Wednesday, July 11

8 - 9 am: Breakfast and registration

8:45 am – 11:30 am: **Hacking Public Policy Tutorial –** *White House tour, depart AAAS promptly at 8:45 for .5 mile walk to White House (advance registration required)*

9 am – 12 pm: Workshop on Usable Privacy and Security for Mobile Devices (U-PriSM)

12 - 1 pm: **Lunch**

1 – 4:30 pm: **Hacking Public Policy Tutorial** and **Workshop on Usable Privacy & Security for Mobile Devices (U-PriSM)**

4:45 – 6:45 – **Poster Session and evening reception –** First Floor lobby
Sponsored by Nielsen

Thursday, July 12

8 - 9 am: Breakfast and registration

9 am - 10:30 am: Opening session

- Welcome and best paper award presentation
    - o Lorrie Cranor, SOUPS General Chair
    - o Heather Richter Lipford and Konstantin Beznosov, SOUPS Technical Papers Co-Chairs

- NSF Secure and Trustworthy Cyberspace Program
    - o Jeremy Epstein, NSF
    - o Peter Muhlberger, NSF

- Invited talk: Julie Brill, Comissioner, Federal Trade Commission
  Privacy in the mobile world: A big task on a small screen

  In her remarks, Commissioner Brill will discuss the privacy implications of the increasing shift of consumers' online experiences to the mobile environment. Among other topics, she will discuss children's privacy in the mobile space, issues surrounding effective disclosures on mobile devices, and the privacy implications of mobile payments.

10:30-11 am: break

11 am - 12:30 pm: Technical paper session: **Mobile Privacy and Security**, Session chair: Mary Ellen Zurko, Cisco

Measuring and Improving User Confidence in Mobile Phone Security and Privacy
Erika Chin, Adrienne Porter Felt, Vyas Sekar, David Wagner

Goldilocks and the Two Mobile Devices: Going Beyond All-Or-Nothing Access to a Device's Applications
Eiji Hayashi, Oriana Riva, Karin Strauss, A.J. Bernheim Brush, Stuart Schechter

Android Permissions: User Attention, Comprehension, and Behavior
Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, David Wagner

12:30 – 1:30 pm: Lunch- Second floor lobby
Sponsored by RIM

1:30 - 3 pm: Technical paper session: **User Perceptions**, Session chair: Serge Egelman, University of California, Berkeley

Smart Useful, Scary, Creepy: Perceptions of Behavioral Advertising
Blase Ur, Pedro G. Leon, Lorrie Faith Cranor, Richard Shay, Yang Wang

Reasons, Rewards, Regrets: Privacy Considerations in Location Sharing as an Interactive Practice
Sameer Patil, Greg Norcie, Apu Kapadia, Adam J. Lee

Stories as Informal Lessons about Security
Emilee Rader, Rick Wash, Brandon Brooks

3 – 3:30 pm: Break

3:30 - 4:30 pm: Technical paper session: **Authentication**, Session chair: Stuart Schechter, Microsoft Research

Correct horse battery staple: Exploring the usability of system-assigned passphrases
Richard Shay, Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Blase Ur, Tim Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor

Do You See Your Password? Applying Recognition to Textual Passwords
Nicolas Wright, Andrew S. Patrick, Robert Biddle

4;30-5:45 pm: Demos and lightning talks

6 - 9 pm: Dinner reception at Microsoft (901 K St. NW, 11th Floor) – a 5-minute walk from AAAS

Friday, July 13

8 - 9 am: Breakfast and registration

9 - 10:30 am: Technical paper session: **Online Social Networks,** Session chair: Robert Biddle, Carleton University

Facebook and Privacy: It's Complicated
Maritza Johnson, Serge Egelman, Steven M. Bellovin

Are Privacy concerns a turn-off? Engagement and privacy in social networks
Jessica Staddon, David Huffaker, Larkin Brown, Aaron Sedley

Helping Johnny 2.0 to Encrypt His Facebook Conversations
Sascha Fahl, Marian Harbach, Thomas Muders, Uwe Sander, Matthew Smith

10:30 - 11 am: Break

11 am - 12:30 pm: Technical paper session: **Access Control**, Session chair: Rob Reeder, Microsoft

+Your Circles: Sharing Behavior on Google+
Jason Watson, Andrew Besmer, Heather Richter Lipford

The PViz Comprehension Tool for Social Network Privacy Settings
Alessandra Mazzia, Kristen LeFevre, Eytan Adar

Relating Declarative Semantics and Usability in Access Control
Vivek Krishnan, Mahesh V. Tripunitara, Kinson Chik, Tony Bergstrom

12:30 - 1:30 pm: Lunch

1:30 - 3 pm: Panel – **Will No Humans be Harmed? The argument against IRB approval for some human subjects research**

The role of the Institutional Review Board is to ensure that human subjects protections are in place in research. The principles and guidelines that guide IRBs in their processes were set forth in the Belmont Report in 1979. As the medium of conducting research has evolved, is the IRB holding back usable privacy and security research and is it still equipped to properly evaluate the risks of our protocols? Are we any further along than the previously troublesome "trust me" model?

This panel will explore the ethics of gathering data online via public postings, working with data (both identifiable and anonymized), and observational research.

Maritza Johnson, Columbia University, Moderator
Michael Zimmer, University of Wisconsin-Milwaukee
Simson Garfinkel, Naval Postgraduate School
Doug Maughan, DHS Science & Technology Directorate

3 pm: **Ice cream social**

Hacking Public Policy Tutorial:
How technologists can influence the public policy process

Wednesday, July 11

8:45   Leave AAAS for .5 mile walk to White House

Noon   Lunch at AAAS

1:00pm   Keynote: Amber Hartman Scholtz, Assistant Executive Director, President's Council of
          Advisors on Science and Technology (PCAST)

2:00pm   Break

2:15pm   Intro by Janice Tsai and Harlan Yu

2:30pm   FTC: Manas Mohapatra, Director of Mobile Policy, Mobile Technology Unit, FTC; Ashkan
          Soltani, independent research, former technology consultant to the FTC

3:00pm   Media: Kashmir Hill, staff writer, Forbes

3:30pm   Congress: Senate Judiciary Staffer

4:00pm   Wrap-up

Workshop on Usable Privacy & Security for Mobile Devices (U-PriSM)

Wednesday, July 11

9:00am   Welcome and opening remarks
9:15am   Invited talk: **"Honey, I Shrunk the Auth!" - Authentication and Authorization on Mobile
          Devices** – Dirk Balfanz (Google)
10:15am   Break
10:40am   Session A: **Users and mobile devices**, Chair: Mary Ellen Zurko (Cisco)

          A-1 (10 min): **I've Got 99 Problems, But Vibration Ain't One: A Survey of Smartphone
          Users' Concerns** – Adrienne Porter Felt, Serge Egelman, David Wagner (UC Berkeley)

          A-2 (10 min): **Privacy as Part of the App Selection Process** – Patrick Kelly (CMU)
          A-3 (20 min): Discussion

          Session B: **User privacy vs. mobile apps**, Chair: Kristie Hawkey (Dalhousie University)

          B-1 (10 min): **"How Come I'm Allowing Strangers to Go Through My Phone?": Smart
          Phones and Privacy Expectations** – Jen King (UC Berkeley)

B-2 (10 min): **Privacy in Mobile Personalized Systems: The Effect of Disclosure Justifications** – Bart P. Knijnenburg (UC Irvine, Samsung R&D), Alfred Kobsa (UC Irvine), Gokay Saldamli (Samsung R&D)

B-3 (20 min): Discussion

Noon   Lunch

1:00pm   Session C: **Location privacy**, Chair: Sunny Consolvo (Google)

C-1 (10 min): **To Share or Not To Share? An Activity-centered Approach for Designing Usable Location Sharing Tools** – Marcello Paolo Scipioni, Marc Langheinrich (University of Lugano)

C-2 (10 min): **Position Paper: Privacy-Preserving Location Tracking with Client-based Modeling** – Janne Lindqvist, Mor Naaman, Marco Gruteser (Rutgers University), Winter Mason (Stevens Institute of Technology)

C-3 (20 min): Discussion

Session D: **Potpourri** – Chair: Janne Lindqvist (Rutgers)

D-1 (10 min): **Understanding the user experience of secure mobile online transactions in realistic contexts of use** – Julio Angulo, Erik Wastlund, Peter Gullberg, Daniel Kling, Daniel Tavemark, Simone Fischer-Hubner (Karlstad University)

D-2 (10 min): **Position Paper: Motivating the need for evaluation criteria for CAPTCHAS** – Gerardo Reynaga (Carleton University)

D-3 (20 min): Discussion

2:20pm   Break

2:50pm   Session E: **user authentication on mobile devices**, Chair: Stuart Schechter (Microsoft Research)

E-1 (10 min): **CASA: context-aware scalable authentication** – Eiji Hayashi, Sauvik Das, Shahriyar Amini, Emmanuel Owusu, Jun Han, Jason Hong, Ian Oakley, Adrian Perrig, Joy Zhang (Carnegie Mellon University)

E-2 (10 min): **Who did you call last?** – Hyoungshick Kim, Konstantin Beznosov (University of British Columbia)

E-3 (10 min): **Anomaly detection—a possible way to address physical threats to smartphones** – Ildar Muslukhov, Yazan Boshmaf, Hyoungshick Kim, Konstantin Beznosov (University of British Columbia), Cynthia Kuo, Jonathan Lester (Nokia Research Center)

E-4 (30 min): Discussion

3:50pm   **Open mic**, Chair: Serge Egelman (UC Berkeley)
Please contact Serge, [email: serge at guanotronics.com] if you would like to have 5-10 minutes to talk about your research, this workshop, or something interesting and relevant to the audience.

4:20pm   Closing remarks (10 min)

Posters

Poster: Anti-Phishing system using footprint-sharing web site
Manabu Okamoto, Eri Otsuka, Ayaka Miyazawa

Poster: CommonTerms – Magnifying the Fine Print
Par Lannero, Gregg Bernstein

Poster: Preliminary Investigation of Gesture-Based Password: Integrating Additional User Behavioral Features
Lakshmidevi Sreeramareddy, Jinjuan Feng, Andrew Sears

Poster: Towards Measuring Warning Readability
Marian Harbach, Sascha Fahl, Thomas Muders, Matthew Smith

Poster: On Design of Audio Instructions for Multisensory Authentication for Portable Touchscreen Device
Madoka Hasegawa, Naoaki Isogai, Shigeo Kato

Poster: Attitudes to IT-Security When Using a Smartphone
Zinaida Benenson, Nadina Hintz, Olaf Kroll-Peters, Matthias Krupp

Poster: Friendship in German Online Social Networks
Nadina Hintz, Zinaida Benenson, Thorsten Strufe

Poster: Cellphones and Punishment: Encouraging Secure Mobile Behavior Through Morality
Dirk Van Bruggen, Shu Liu, Aaron Striegel, Chuck Crowell, John D'Arcy

Poster: Is a Picture Worth a Thousand Alerts?
Nicklaus A. Giacobe

Poster: User perception of usability and security of a mobile payment system
Hanul SIeger, Niklas Kirschnick, Sebastian Moller

Poster: Usability Evaluation of Gesture-Based Authentication Using a Mobile Phone
Niklas Kirschnick, Benjamin Muller, Sebstian Moller

Poster: Towards improving usability of access certification interfaces
Pooya Jagerian, Hootan rashtian, Konstantin Beznosov

Poster: Examining Confidant Disclosures through Facebook Apps and Tagging
Kim RoSser, Emmanueo Bello-Ogunu, Pamela Karr Wisniewski

Poster: Visualization of user's end-to-end security risks
Takeshi, Takahashi, Shin'ichiro Matsuo, Akira Kanaoka, Keita Emura, Yuuki Takano

Posters Showcasing Usable Privacy and Security Papers Published in the Past Year at Other Conferences

PhorceField: A Phish-Proof Password Ceremony
Michael Hart, Claude Castille, Manoj Harpalani, Jonathon Toohil, Rob Johnson

Third-Party Apps on Facebook: Privacy and the Illusion of Control
Na Wang, Heng Xu, Jens Grossklags

ASIDE: IDE Support for Web Application Security
Jing Xie, Bill Chu, Heather Richter Lipford, John T. Melton

Social Authentication: Harder than it Looks
Hyoungshick Kim, John Tang, Ross Anderson

Tag, you can see it!: using tags for access in control in photo sharing
Peter Klemperer, Yuan Liang, Michelle Mazurek, Manya Sleeper, Blase Ur, Lujo Bauer, Lorrie Faith Cranor, Michael K. Reiter

The Implications of Offering More Disclosure Choices for Social Location Sharing
Karen P. Tang, Jason I. Hong, Dan P. Siewiorek

Don't bump, shake on it: The exploitation of a popular accelerometer-based smart phone exchange and its secure replacement
Ahen Studer, Timothy Passaro, Lujo Bauer

How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation
Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor

On the need for different security methods on mobile phones
Noam Ben-Asher, Niklas Kirschnick, Hanul Sieger, Joachim Meyer, Sebastian Moller

Security and Privacy Considerations in Digital Death
Michael E. Locasto, Mike Massimi, Peter J. DePasquale

A Conundrum of Permissions: Installing Application on an Android Smartphone
Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, David Wetherall

Security and Usability Challenges of Moving-Object CAPTCHAs: Decoding Codewords in Motion
Yi Xiu, Gerardo Reynaga, Sonia Chiasson, Jan-Micheal Frahm, Fabian Monrose, P.C. van Oorschot

Security Privacy and Usability Requirements for Federated Identity
Michael Hackett, Kirstie Hawkey