The Saucer

The Newsletter of the
CyLab Usable Privacy and Security (CUPS) Laboratory

Issue 5, Summer 2014

Contents

CUPS research sponsors

- Army Research Laboratory (ARL)
- Army Research Office (ARO)
- Department of Homeland Security (DHS)
- Google
- Microsoft
- National Institute of Standards and Technology (NIST)
- National Science Foundation (NSF)
- National Security Agency (NSA) Science of Security Lablet

New Privacy Engineering Masters Program

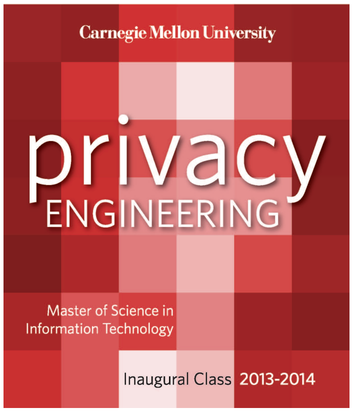
The inaugural class of the world's first masters degree program in privacy engineering arrived at Carnegie Mellon in August 2013. Co-directed by Norman Sadeh and Lorrie Cranor, the Master of Science in Information Technology—Privacy Engineering (MSIT-PE) degree is a one-year program designed for computer scientists and engineers who wish to pursue careers as privacy engineers or technical privacy managers.

The first class of the MSIT-PE program with the program directors at graduation in May 2014. The students finished their coursework in May and are spending the summer working on capstone projects sponsored by Facebook, American Express, and Future of Privacy Forum.

As organizations develop new products, services, infrastructures, and business processes that facilitate the collection and management of an ever-wider range of customer data, they are discovering that privacy issues need to be addressed from the very beginning of the design process. Over the past several years, both industry and government organizations have created positions for people responsible for ensuring that privacy is an integral part of the design process. These people are brought in as in-house consultants who work as part of multi-disciplinary teams. They have to understand technology and be able to integrate perspectives that span product design, software development, cyber security, human computer interaction, as well as business and legal considerations.

The MSIT-PE program includes two semesters of courses taught by leading academic privacy and security experts. Required semester-long courses include Privacy Policy, Law and Technology; Information Security and Privacy; Foundations of Privacy; Usable Privacy and Security; and Engineering Privacy in Software. Guest speakers this year included speakers from Google, Microsoft, Facebook, PNC Bank, the White House, and the National Security Agency.

The program concludes with a summer-long learning-by-doing, capstone project, where students will be brought in as privacy consultants to work on client projects.



Carnegie Mellon University

privacy
ENGINEERING

Master of Science in Information Technology

Inaugural Class 2013-2014

For more information, see **http://privacy.cs.cmu.edu**.

CyLab
Usable
Privacy *and*
Security
Laboratory

http://cups.cs.cmu.edu

Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213

Director
Lorrie Faith Cranor
lorrie@cmu.edu

Faculty
Alessandro Acquisti
Yuvraj Agrawal
Lujo Bauer
Travis Breaux
Nicolas Christin
Julie Downs
Coty Gonzalez
Jason Hong
Roy Maxion
Norman Sadeh
Marios Savvides

One of the first CUPS photos, taken in September 2007: Serge Egelman, Patrick Kelley, Rob Reeder, Janice Tsai, Steve Sheng, Lorrie Cranor , Aleecia McDonald, Ponnurangam Kumaraguru, Kami Vania.

CUPS students, faculty, and alumni gather for lunch at CHI 2014 in Toronto. Back row: Blase Ur, Greg Norcie, Rich Shay, Lujo Bauer, Serge Egelman, Alain Forget. Front row: Lorrie Cranor, Patrick Kelley, Rebecca Balebako, Manya Sleeper, Rob Reeder.

CUPS IGERT winds down but usable privacy and security doctoral training program continues

Five years ago, an NSF Integrative Graduate Education and Research Traineeship (IGERT) grant helped launch the Carnegie Mellon Usable Privacy and Security Doctoral Training Program. Now, as we enter into our final (no-cost extension) year of IGERT funding, the program has been institutionalized, and is ready to continue on into the future.

Students in PhD programs from throughout CMU have the opportunity to participate in the CUPS doctoral training program and earn a CyLab Usable Privacy and Security Meritorious Achievement Certificate.

The CUPS doctoral training program offers students a cross-disciplinary training experience that prepares them to produce the key research advances necessary to reconcile ostensible tensions between security, privacy, and usability, moving away from an “either-or” view of these goals to a deeper understanding of underlying tradeoffs and eventually towards solutions where security, privacy, and usability are configured to reinforce each other. The goal of this program is to serve as a catalyst to shape the field of usable privacy and security by developing and training a new generation of researchers in methodologies, principles, and approaches that can be applied across systems and applications.

CUPS students are required to take our Usable Privacy and Security course, plus three approved full-semester courses from a selection of courses in security, privacy, human computer interaction, social and decision sciences, and other areas. Students are also expected to participate in the weekly CUPS research seminar and be engaged in usable privacy and security research.

Prospective students should apply directly to a CMU PhD program of their choice, and also send a letter of interest to the CUPS program administrator indicating which CMU doctoral program they have applied to and describing their interest in CUPS-related research. See the CUPS website for more information **http://cups.cs.cmu.edu**.

From the Director

Back in Spring 2004 I started the CUPS Lab with a few students who heard there was a new faculty member at CMU doing research in usable privacy and security and responded to my invitation to go out to lunch together and discuss interesting papers. As I told the students at the time, we have a name and I appointed myself director, so we are a lab.

Over the summer of 2004 I created a logo, acquired a web server, and put up a website as I welcomed my first three PhD students and a couple of undergraduate summer students. After a few months the group was large enough that we started ordering lunch in. When Simson Garfinkel and I began editing chapters for our book *Security and Usability,* the lunch group agreed to read and discuss the draft chapters. Over time the CUPS email list expanded to include faculty, staff, and students from departments throughout the university who were interested in usable privacy and security. Now in our tenth year, we have over 200 mailing list members, and usually somewhere between 20 and 50 of them show up for our Wednesday CUPS lunches.

Early CUPS research projects focused on P3P user agents Privacy Bird and Privacy Finder, measuring P3P deployment, and conducting experiments to determine whether people would pay to protect their privacy (they will!). When we moved to the Collaborative Innovation Center building in 2005 we began working with the Grey project team to study usability issues related to the deployment of a smartphone access control system for doors in the CIC building (a system we still use). In 2005 we also received a large NSF grant to study the phishing problem. We developed anti-phishing training and filtering technologies that were later commercialized by Wombat Security Technologies, Inc. Subsequent research grants focused on user-controllable policy learning, effective security warning design, usable security for digital home storage, usable and secure passwords, and observing security-related behaviors of home Internet users. Two of our most recent large projects include an NSF Frontier grant *Towards Effective Web Privacy Notice And Choice: A Multi-Disciplinary Perspective,* and a multi-institution Army Research Lab collaborative project *MACRO: Models for Enabling Continuous Reconfigurability of Secure Missions.*

10 YEARS
2004 2014
CUPS
CyLab Usable Privacy & Security Laboratory
Carnegie Mellon University

Over the years we've built a number of practical prototypes and demos based on our research. One tool that we recently added to our website is a search engine for comparing the privacy policies of over 6000 U.S. financial institutions. It is still a work in progress, but you can check it out at **http://cups.cs.cmu.edu/bankprivacy**.

It is exciting to see the vibrant usable privacy and security research community that has developed at Carnegie Mellon University in just 10 years. I look forward to seeing what develops in the next 10 years and beyond!

Lorrie

Students

Hazim Saleh Almuhimedi
Rebecca Balebako
Jonathan Bees
Sekhar Bhagvatula
Justin Cranshaw
Adam Durity
Jim Graves
Hanan Hibshi
Eiji Hayashi
Candace Hoke
Peter Klemperer
Saranga Komanduri
Darya Kurilova
Shing-hon Lau
Pedro Leon
Bin Liu
Abby Marsh
Billy Melicher
Emmanuel Owusu
Ashwini Rao
Sean Segreti
Rich Shay
Stephen Siena
Manya Sleeper
Yuan Tian
Blase Ur
Timothy Vidas
Tatiana Vlahovic
Jason Wiese

Post-Docs & Staff

Matthias Beckerle
Cristian Bravo-Lillo
Alain Forget
Alessandro Oltramari
Florian Schaub
Tiffany M. Todd

Cristian Bravo-Lillo presents his award-winning paper at SOUPS 2013.

Lujo Bauer and Lorrie Cranor practicing broomstick skills at the SOUPS dinner at Hogwarts (Alnwick Castle).

Deputy US Chief Technology Officer Nicole Wong was our keynote speaker at Data Privacy Day 2014. See cups.cs.cmu.edu/privacy-day/

MSIT-PE student Adam Durity organized a Privacy Clinic as part of Data Privacy Day.

Year in Review

July 2013

- Cristian Bravo-Lillo, Lorrie Cranor, Julie Downs, Saranga Komanduri, Manya Sleeper and collaborators (alumnus) Rob Reeder and Stuart Schechter won a SOUPS 2013 distinguished paper award for their paper "Your Attention Please: Designing security-decision UIs to make genuine risks harder to ignore"
- Lorrie Cranor gave a keynote talk at the Privacy Enhancing Technologies Symposium

August 2013

- The inaugural class of the MSIT-Privacy Engineering Program arrived on campus
- Norman Sadeh and co-PIs Alessandro Acquisti, Travis Breaux, Lorrie Cranor, Noah Smith, Joel Reidenberg, and Aleecia McDonald received a $3.75 million grant from the National Science Foundation for their Usable Privacy Policy Project **http://www.usableprivacy.org**

September 2013

- Norman Sadeh was awarded a research grant under Google's "Privacy and Security Focused Program" for his work on "Smart privacy profiles for mobile apps"
- Sauvik Das, Eiji Hayashi, and Jason Hong won a best paper award at Ubicomp'13 for their paper "Autobiographical Authentication"

October 2013

- CUPS researchers Lorrie Cranor, Lujo Bauer, Nicolas Christin, and Coty Gonzalez joined with the Army Research Lab (ARL) and other academic partners for a five-year research program focusing on cyber security
- Lorrie Cranor was interviewed in the article "What Chase and other banks won't tell you about selling your data" in *Forbes*

November 2013

- Lorrie Cranor gave a talk entitled "Computers, Quilts, and Privacy" to accompany an exhibition of her original art quilts at the Frame Gallery at Carnegie Mellon

January 2014

- Privacy Engineering faculty and students hosted CMU's Data Privacy Day celebration, with a keynote talk from Nicole Wong, Deputy Chief Technology Officer, White House Office of Science and Technology
- CUPS student Cristian Bravo-Lillo successfully defended his thesis "Improving Computer Security Dialogs: An Exploration of Attention and Habituation"

February 2014

- Nicolas Christin was program committee chair of Financial Cryptography 2014
- Lorrie Cranor received the Distinguished Alumni Award from the Montgomery Blair High School Magnet Foundation in Silver Spring, Maryland
- Lorrie Cranor's quilt entitled Security Blanket received an honorable mention in the 2013 International Science and Engineering Visualization Challenge hosted by the National Science Foundation; the quilt appeared in *Science Magazine*

March 2014

- Alumna Janice Tsai contributed to the paper "Bootstrapping Privacy Compliance in Big Data Systems" which won the Best Student Paper Award at the 2014 IEEE Symposium on Security and Privacy

- Alessandro Acquisti was interviewed by the *New York Times* in the Article "Letting Down Your Guard with Web Privacy"
- Lorrie Cranor gave a TEDxCMU talk titled "I love you password 123456"
- Yuan Tian (along with Ying-Chuan Liu, Amar Bhosale, Lin-Shung Huang, Patrick Tague, and Collin Jackson) won the best poster runner-up award at the Women in Cyber Security Conference for the poster "Attacks and Defenses for the New HTML5 Screen Sharing API"

April 2014

- Sauvik Das won a Qualcomm Innovation Fellowship along with Gierad Laput for the proposal "Everyday Objects for Physical Space Authentication"
- Rebecca Balebako won the Graduate Student Service Award
- Travis Breaux gave a keynote talk at the NIST Privacy Engineering Workshop
- Alain Forget gave an invited talk and poster presentation of research on the Security Behavior Observatory at the Symposium and Bootcamp on the Science of Security (HotSos); Darya Kurilova also presented a poster

May 2014

- The Presidential Council of Advisors on Science and Technology (PCAST) released a report on Big Data and Privacy that cited expert input from Lorrie Cranor and papers by Travis Breaux, Anupam Datta, and their students
- Nicolas Christin was program committee chair of the security track at WWW 2014
- The International Association of Privacy Professionals Certified Information Privacy Professional (IAPP CIPP) exams were administered on campus, free of charge to CMU students who are IAPP members
- MSIT-PE Co-Directors Lorrie Cranor and Norman Sadah participated in the first commencement for students in the inaugural class of the MSIT-PE program
- Billy Melicher won an ECE Outstanding Graduate Student Teaching Assistant Award
- Lujo Bauer was appointed program co-chair of IEEE S&P 2015

June 2014

- The CUPS Lab launched the **http://cups.cs.cmu.edu/bankprivacy/** website that displays summarized privacy policies of over 6,000 bank websites and provides privacy search and comparison tools
- Lorrie Cranor and her password dress were featured in the CNET article "Password dress: A frock covered in a security faux pas" and on the Women You Should Know website in the article "She Made Bad Passwords Fashionable"
- Lorrie Cranor and Norman Sadeh hosted the Future of Privacy Notice and Choice Workshop at Carnegie Mellon University
- Yuvraj Agrawal co-chaired the Mobile Cloud Computing & Services Workshop

July 2014

- SOUPS 2014 will be held July 9-11 at Facebook headquarters in Menlo Park, CA
- Lorrie Cranor is general chair and Lujo Bauer is program committee co-chair of SOUPS 2014

Tiffany Todd, Cristian Bravo-Lillo, and Alain Forget explore Newcastle at SOUPS 2013.

Rebecca Balebako receiving her Graduate Student Service Award.

Billy Melicher receiving an Outstanding Graduate Student Teaching Assistant Award.

New Additions

Janice Tsai (EPP 2009) welcomed a new addition to her family. Ada Owen Sharp was born March 6, 2014.

Weddings

Postdoc **Florian Schaub** married Ashleigh Ellison May 3 in Chattanooga, TN and celebrated again on May 10 in Germany.

Alumnus **Serge Egelman** married Carolyn Denomme on October 12 in Lexington, KY.

On the Move

Serge Egelman was appointed Senior Researcher at the International Computer Science Institute last fall.

Kami Vaniea will join the faculty of the School of Informatics at Indiana University in the fall.

Michelle Mazurek will join the faculty of Computer Science at the University of Maryland in the fall.

In Other News

Lorrie Cranor, Pedro Leon, and other CUPS members mentored three seniors from the Pittsburgh Science and Technology Academy as they worked on a year-long project on online security and privacy for teenagers. The students developed a website for teens at **cups.cs.cmu.edu/privacy4teens/**

SciTech senior **Jonathan Bees** has started working with the CUPS passwords group on a project that he will work on throughout the year.

Rich Shay took second place in a Magic tournament with over 400 players on June 15. He wrote an article for a leading Magic website about the experience.

Postdoc **Florian Schaub** successfully defended his Ph.D. thesis at the University of Ulm in Ulm, Germany. His thesis title was "Dynamic Privacy Adaptation in Ubiquitous Computing." In Germany it's tradition to decorate the graduation hat with themes from the thesis and research. So Florian's doctor's hat has movable privacy curtains (to symbolize dynamic privacy) and a "paper machine" spitting out publications.

Research assistant **Emily Forney** volunteered for the CMU Admissions Council and the National Junior Classical League, a high school Latin organization which holds state and national conventions. Emily will join a masters program at Pitt next Fall to study higher education administration with a focus on student services.

Postdoc **Alessandro Oltramari** is area chair of the COLING conference (Lexical Semantics and Ontologies), to be held in Dublin next August.

Recent Publications

Most CUPS publications are available on the CUPS website. The following are a selection of publications from the past year.

Privacy Decision Making

A Field Trial of Privacy Nudges for Facebook

Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh

CHI 2014

Anecdotal evidence and scholarly research have shown that Internet users may regret some of their online disclosures. To help individuals avoid such regrets, we designed two modifications to the Facebook web interface that nudge users to consider the content and audience of their online disclosures more carefully. We implemented and evaluated these two nudges in a 6-week field trial with 28 Facebook users. We analyzed participants' interactions with the nudges, the content of their posts, and opinions collected through surveys.
We found that reminders about the audience of posts can prevent unintended disclosures without major burden; however, introducing a time delay before publishing users' posts can be perceived as both beneficial and annoying. On balance, some participants found the nudges helpful while others found them unnecessary or overly intrusive. We discuss implications and challenges for designing and evaluating systems to assist users with online disclosures

The Post Anachronism: The Temporal Dimension of Facebook Privacy

Lujo Bauer, Lorrie Faith Cranor, Saranga Komanduri, Michelle Mazurek, Michael Reiter, Manya Sleeper, Blase Ur

Workshop on Privacy in the Electronic Society (WPES 2013)

This paper reports on two studies that investigate empirically how privacy preferences about the audience and emphasis of Facebook posts change over time. In a 63-participant longitudinal study, participants gave their audience and emphasis preferences for up to ten of their Facebook posts in the week they were posted, again one week later, and again one month later. In a 234-participant retrospective study, participants expressed their preferences about posts made in the past week, as well as one year prior. We found that participants did not want content to fade away wholesale with age; the audience participants wanted to be able to access posts remained relatively constant over time. However, participants did want a handful of posts to become more private over time, as well as others to become more visible. Participants' predictions about how their preferences would change correlated poorly with their actual changes in preferences over time, casting doubt on ideas for setting an expiration date for content. Although older posts were seen as less relevant and had often been forgotten, participants found value in these posts for reminiscence. Surprisingly, we observed few concerns about privacy or self-presentation for older posts. We discuss our findings' implications for retrospective privacy mechanisms.

The Privacy and Security Behaviors of Smartphone App Developers

Rebecca Balebako, Abigail Marsh, Jialiu Lin, Jason Hong, Lorrie Faith Cranor

Workshop on Usable Security (USEC 2014)

We explore how smartphone app developers make decisions about privacy and security. Additionally, we examine whether any privacy and security behaviors are related to characteristics of the app development companies. We conduct a series of interviews with 13 app developers to obtain rich qualitative information about privacy and security decision-making. We use an online survey of 228 app developers to quantify behaviors and test our hypotheses about the relationship between privacy and security behaviors and company characteristics. We find that smaller companies are less likely to demonstrate privacy and security behaviors. Although third-party tools for ads and analytics are pervasive, developers aren't aware of the data collected by these tools. We suggest tools and opportunities to reduce the barriers for app developers to implement privacy and security best practices.

Is Your Inseam a Biometric? A Case Study on the Role of Usability Studies in Developing Public Policy

Rebecca Balebako, Rich Shay, and Lorrie Faith Cranor

Workshop on Usable Security (USEC 2014)

We present a case study of applying usable privacy methodologies to inform debate regarding a multi-stakeholder public policy decision. In particular, the National Telecommunications and Information Administration (NTIA) relied on a multi-stakeholder process to define a set of categories for short-form privacy notices on mobile devices. These notices are intended for use in a US national code of conduct to assist mobile device users in making decisions regarding data collection. We describe a791-participant online study to determine whether users consistently understand these proposed categories and their definitions. We found that many users did not understand the terms in our study. The heart of our contribution, however, is a case study of our participation in this group as academic usable privacy and security experts, and a presentation of lessons learned regarding the application of usable privacy and security methodology to public policy discussion. We believe this work is valuable to usable privacy and security researchers wishing to affect public policy.

The Usable Privacy Policy team.

Passwords

Can Long Passwords Be Secure and Usable?

Richard Shay, Saranga Komanduri, Adam L. Durity, Phillip (Seyoung) Huh, Michelle L. Mazurek, Sean M. Segreti, Blase Ur, Lujo Bauer, Nicolas Cristin, and Lorrie Faith Cranor

CHI 2014

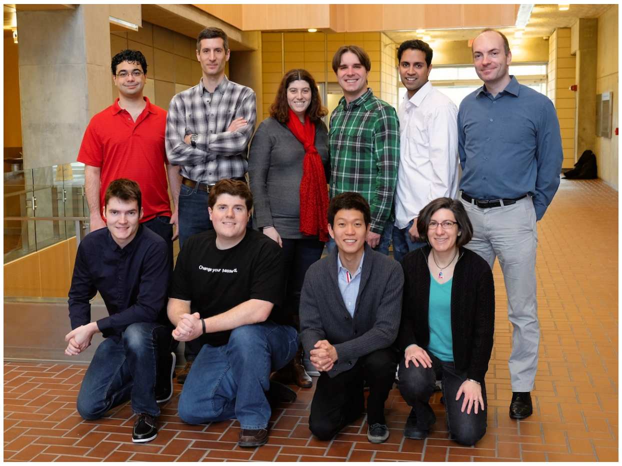
To encourage strong passwords, system administrators employ password-composition policies, such as a traditional policy requiring that passwords have at least 8 characters from 4 character classes and pass a dictionary check. Recent research has suggested, however, that policies requiring longer passwords with fewer additional requirements can be more usable and in some cases more secure than this traditional policy. To explore long passwords in more detail, we conducted an online experiment with 8,143 participants. Using a cracking algorithm modified for longer passwords, we evaluate eight policies across a variety of metrics for strength and usability. Among the longer policies, we discover new evidence for a security/usability tradeoff, with none being strictly better than another on both dimensions. However, several policies are both more usable and more secure that the traditional policy we tested. Our analyses additionally reveal common patterns and strings found in cracked passwords. We discuss how system administrators can use these results to improve password-composition policies.

Measuring Password Guessability for an Entire University

Michelle L. Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur

ACM CCS 2013

Empirical studies of password strength have been limited by lack of access to plaintext passwords, small data sets, and password sets collected for a research study or from low-value accounts. Properties of passwords used for high-value accounts thus remain poorly understood. We study the single-sign-on passwords used by over 25,000 faculty, staff, and students at a research university with a complex password policy. Key aspects of our contributions rest on our (indirect) access to plaintext passwords. We describe our data collection methodology, particularly the many precautions we took to minimize risks to users. We then analyze how guessable the collected passwords would be during an offline attack by subjecting them to a state-of-the-art password cracking algorithm. We discover significant correlations between a number of demographic and behavioral factors and password strength. For example, we find that users associated with the computer science school make passwords more than 1.8 times as strong as those of users associated with the business school. In addition, we find that stronger passwords are correlated with a higher rate of errors entering them. We also compare the guessability and other characteristics of the passwords we analyzed to sets previously collected in controlled experiments or leaked from low-value accounts.



The CUPS passwords research group. Back row: Rich Shay, Lujo Bauer, Michelle Mazurek, Blase Ur, Saranga Komanduri, Nicolas Christin. Front row: Sean Segreti, Adam Durity, Philip Huh, Lorrie Cranor.

Dissertations and Proposals

Modeling the adversary to evaluate password strength with limited samples

PhD Thesis Proposal, Computation, Organizations & Society
Saranga Komanduri
December 2013

Creating usable policies for stronger passwords with MTurk

PhD Thesis Proposal, Computation, Organizations & Society
Richard Shay
December 2013

Improving Computer Security Dialogs: An Exploration of Attention and Habituation

Doctoral Dissertation, Engineering & Public Policy
Cristian Bravo-Lillo
January 2014

A Tag-Based, Logical Access-Control Framework for Personal Data Sharing

Doctoral Dissertation, Electrical & Computer Engineering
Michelle L. Mazurek
May 2014

Without Borders: Addressing Regulatory Requirements in Multi-Jurisdictional IT Environments

Doctoral Dissertation, Engineering & Public Policy
David G. Gordon
June 2014