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

The Saucer

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

Issue 6, Summer 2015

Contents

CUPS research sponsors

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

Privacy Illustrated

We asked children and adults to draw pictures of what privacy means to them. Browse these images on our website and contribute your own!

cups.cs.cmu.edu/privacyillustrated

Privacy Engineering Masters Program Trains Students for Privacy Jobs

In August 2014 we graduated the inaugural class of the world's first masters degree program in privacy engineering. Our first graduates have taken jobs at Google, Adobe, Oracle, eBay, and Linked-In.

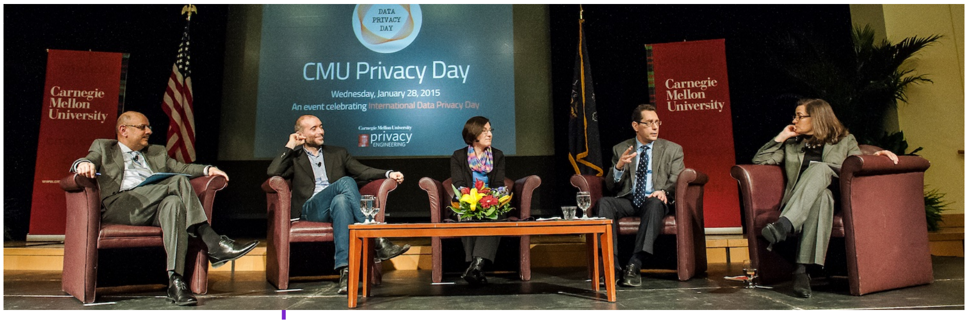
MSIT-PE '15 student Cameron Boozarjomehri asks a question at CMU Privacy Day in January.

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. See **http://privacy.cs.cmu.edu** for more information.

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 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. Students also participate in a privacy seminar held throughout the Fall and Spring semester. Guest speakers this year included speakers from Google, Yahoo!, American Express, the Federal Trade Commission, the National Security Agency, ICANN, and SpiderOak.

The program concludes with a summer-long learning-by-doing capstone project, where students are brought in as privacy consultants to work on client projects. Our first class completed capstone projects for Facebook, American Express, and the Future of Privacy Forum. Our second class is working on projects for Lufthansa and SpiderOak.


CMU Privacy Day
Wednesday, January 28, 2015
An event celebrating International Data Privacy Day
Carnegie Mellon University
Carnegie Mellon University

CMU faculty discuss their privacy research with FTC Commissioner Julie Brill at CMU Privacy Day in January.

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
Norman Sadeh
Marios Savvides

Students
Hazim Saleh Almuhimedi
Sekhar Bhagvatula
Jim Graves
Hanan Hibshi
Darya Kurilova
Shing-hon Lau
Bin Liu
Abby Marsh
Billy Melicher
Ashwini Rao
Sean Segreti
Stephen Siena
Manya Sleeper
Josh Tan
Yuan Tian
Blase Ur
Jason Wiese

Post-Docs & Staff
Matthias Beckerle
Alain Forget
Pedro Leon
Alessandro Oltramari
Sarah Pearman
Florian Schaub
Jeremy Thomas
Tiffany M. Todd

From the Director

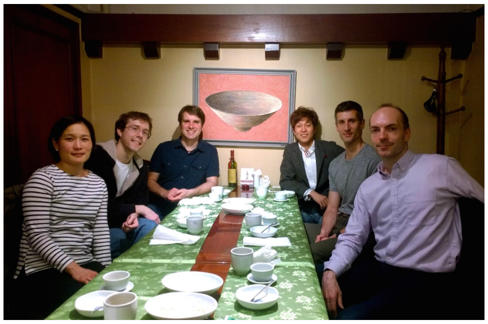
At the beginning of July I got an email from one of my first PhD students, Ponnurangum Kumaraguru (COS PhD 2009), congratulating me on becoming an academic grandmother. PK is an assistant professor at Indraprastha Institute of Information Technology (IIIT), Delhi. His first PhD student, Aditi Gupta, defended her thesis on mitigating misinformation spread on Twitter. I love hearing about all the great things our alumni are doing.

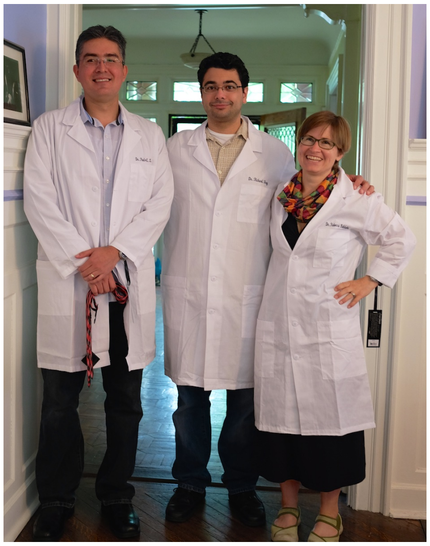
I had the opportunity to catch up with several alumni during my visit to the Bay Area in June. I had coffee with MSIT-PE 2014 alumni Adam Durity and Ziwei Hu at Google in Mountain View. Adam also visited CMU last spring and gave a privacy seminar talk. While in the Bay Area I met up with Aleecia McDonald (EPP PhD 2010), but missed Serge Egelman (COS PhD 2009). Instead, I got to see Serge in July when he came to our NSA Lablet meeting in Pittsburgh. Serge recently started his own laboratory, the Berkeley Laboratory for Usable and Experimental Security (BLUES). Great name!

A few of our PhD alumni are still in the Pittsburgh area. Rebecca Balebako (EPP PhD 2014) works for RAND and often comes to our CUPS seminars. Pedro Leon (EPP PhD 2014) has spent the past year working for Stanford while located at CMU. Steve Sheng (EPP PhD 2009) moved back to Pittsburgh, so I run into him periodically. Last spring he gave a CUPS talk about his work at ICANN. MSIT-PE 2014 alumna, Sakshi Garg, stopped by my office when she was on campus to recruit for Adobe at the TOC.

And there is more news from our alumni (and current faculty, staff, and students) on the next page….

Lorrie





Left top: Alumni Rob Reeder and Serge Egelman avoid landmines at the DMZ. Left bottom: Philip Huh takes the passwords team to dinner in Seoul. Right: Newly minted PhDs Pedro Leon, Rich Shay, and Rebecca Bakebako model their new lab coats at the CUPS graduation brunch.

New Additions

Jason Hong's daughter Zoey was born in July 2014.

Saranga Komanduri's son Shreyas was born in March 2015. Saranga is now an Engineering Technical Lead at Civis Analytics.

Michelle Mazurek's daughter Hannah was born in June 2014. Michelle is now an assistant professor at the University of Maryland.

Alessandro Oltramari and his wife Laura adopted Lady, an 8-year-old pit bull, from the Animal Rescue League.

Weddings

MSIT-PE 2014 alum **Adam Durity** married Katherine Harrington in April. Adam is now working at Google in Mountain View, CA.

CUPS Interns

Rupal Nahar is a rising sophomore at CMU. She is working with Blase Ur on developing data-driven browser privacy tools.

Brett Hubbard is entering 12th grade at South Side High School. He is working with Blase Ur and Abby Marsh on privacy notices for the internet of things and teen privacy.

Adam Buchinsky is an 11th grade student at the Pittsburgh Science and Technology Academy (SciTech).

Maung Aung finished his bachelor's degree at CMU this spring and is working with Blase Ur on a real-time password strength tool.

Ashwin Srinvasan is entering 10th grade at Pittsburgh Allerdice high school. He is continuing to develop his award-winning tool Privacy Tracker.

Jerome Williams and Jonathan Tran, both rising 12th graders at SciTech, are working with Blase Ur to develop improved visualizations for password-strength meters.

Alexander Butler and Brandon Jabout, both 12th grade students at SciTech, are working with Abby Marsh on teen privacy tools.

Daricia Wilkinson is a senior at the University of the Virgin Islands. She is working with Abby Marsh on teen privacy and helping on other projects.

Jonathan Bees, who worked on passwords projects at CUPS last summer (and co-authored a SOUPS paper), graduated from SciTech and is heading to Penn State this fall.

On the Move

Rebecca Balebako (EPP PhD 2014) joined the staff at RAND Corporation in January 2015.

Rich Shay (COS PhD 2015) is joining the staff at Lincoln Labs in Massachusetts in August.

Kami Vaniea (CSD PhD 2012) will join the faculty of the University of Edinburgh Scotland in August. She will be in the School of Informatics as part of their growing security group.

In Other News

Florian Schaub serves as technical observer of the Uniform Law Commission's drafting committee on limiting the use of social media in employment and admission decisions.

Peter Klemperer (ECE PhD 2014) spent part of last summer volunteering at Techbridge, a non-profit organization whose mission involves providing young women and girls access to the computer science education and programming.

Alessandro Oltramari and others started the CMU group of Interest on Ontology Studies.

Lorrie Cranor speaks at an NSF-sponsored briefing for congressional staff

Jason Hong speaks about smartphone privacy issues at a briefing for congressional staff.

Florian Schaub presents his research to FTC Commissioner Julie Brill at CMU Privacy Day.

The Usable Privacy Policy team in spring 2015. Learn about the project at http://usableprivacy.org.

Year in Review

July 2014

- Alessandro Acquisti delivered a keynote at the 27th Annual Computer Security Foundations Symposium.

August 2014

- Team CMU, composed of members of the CUPS research group on passwords, took first place in the "street" (non-professional) division of the 2014 DEF CON "Crack Me If You Can" password-cracking contest.
- The first class of the MSIT-Privacy Engineering program graduated.

September 2014

- Blase Ur and mentors Jaeyeon Jung and Stuart Schechter were awarded Best Paper at UbiComp 2014 for "Intruders Versus Intrusiveness: Teens' and Parents' Perspectives on Home-Entryway Surveillance."

October 2014

- Norman Sadeh and Anupam Datta coordinated CMU's response to the NITRD Request for Information on a National Privacy Research Strategy.
- Lorrie Cranor gave an invited talk at the Grace Hopper Celebration of Women in Computing.
- Lorrie Cranor and Jason Hong presented their research at Capitol Hill briefings.
- Jason Hong launched the **http://privacygrade.org** website that grades smartphone apps' privacy practices. The grades are based on research he conducted with Norman Sadeh and their students analyzing the privacy of 1 million Android smartphone apps.

November 2014

- Florian Schaub and co-authors received the Best Paper Award at the International Conference on Mobile and Ubiquitous Multimedia for the paper "PriPref Broadcaster: Enabling users to Broadcast Privacy Preferences in Their Physical Proximity."
- Alessandro Acquisti delivered keynotes at the 77th Association for Information Science and Technology (ASIST) Annual Meeting.
- Florian Schaub was one of four nominees for the 2014 CAST/GI dissertation award IT-Security by the Competence Center for Applied Security Technology for his doctoral Dissertation "Dynamic Privacy Adaptation in Ubiquitous Computing."
- Lorrie Cranor gave the closing keynote at the IAPP Practical Privacy Series government event.

December 2014

- Alessandro Acquisti delivered a keynote at the SPION Closing Workshop: "You Are Not Alone."
- Lorrie Cranor, Rebecca Balebako, Manya Sleeper, and Darya Kurilova participated in Deep Lab at the CMU STUDIO for Creative Inquiry and developed the Privacy Illustrated website **http://cups.cs.cmu.edu/privacyillustrated/**.

January 2015

- The MSIT-Privacy Engineering program hosted CMU Privacy Day with guest speaker Julie Brill, Commissioner of the Federal Trade Commission.
- Lorrie Cranor was named a 2014 ACM Fellow for her contributions to usable privacy and security research and education.

- Florian Schaub spoke on a panel on automated notice processing at the International Conference on Computers, Privacy & Data Protection in Brussels.

February 2015

- Lorrie Cranor spoke at the White House Cybersecurity Summit.
- Ashwin Srinivasan, a 9th-grader at Pittsburgh Allderdice High School, received a first place award at the Pennsylvania Junior Academy of Science (PJAS) Pittsburgh Regional science fair. At the Pittsburgh Regional Science and Engineering Fair (PRSEF), Ashwin placed third in Computer Science/Math in the Senior Division and won three special awards. He was advised by Blase Ur in developing the PrivacyTracker Chrome plugin.

March 2015

- Lorrie Cranor gave a "game changer talk" at the IAPP Global Privacy Summit.
- Abby Marsh received a Facebook Fellowship to support her research on how parents and their teenaged children make privacy-related decisions about teens' use of the internet and digital technologies.

April 2015

- Alessandro Acquisti was awarded an Andrew Carnegie Fellowship from Carnegie Corporation of New York.
- CUPS alumni Serge Egelman and Eyal Peer received an Honorable Mention Award for the paper "Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS) at CHI 2015.
- A mobile privacy nudging field study by Hazin Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Josh Gluck, Lorrie Cranor and Yuvraj Agrawal,was featured in several press articles.
- Lorrie Cranor graduated from the ELATE @ Drexel leadership development program for senior women faculty in STEM fields.

May 2015

- Norman Sadeh co-chaired the 2015 International Workshop on Privacy Engineering.
- Lorrie Cranor helped write the Computing Community Consortium report "Towards a Privacy Research Roadmap for the Computing Community."
- Jonathan Bees and Shane Cranor, 12th-grade and 8th-grade students at the Pittsburgh Science and Technology Academy, received first place awards at both the regional and state-level competitions of the PJAS science fair. Jonathan worked with Sean Segreti, Blase Ur, and the rest of the passwords research group in examining users' perceptions of password security. Shane worked with Blase Ur to study listeners' perceptions of compressed audio.

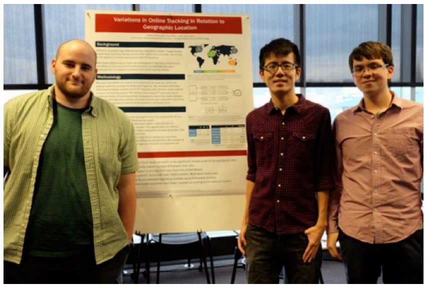
June 2015

- Lorrie Cranor and Blase Ur received a grant from the Data Transparency Lab (DTL) for their work "Providing Users Data-Driven Privacy Awareness."
- Jason Hong was named a 2015 National Cybersecurity Fellow by New America.
- Alessandro Oltramari received the "Above and Beyond" award for his work with the Army Research Lab (ARL) Cyber-security CRA program.

July 2015

- Lujo Bauer, Travis Breaux, Lorrie Cranor, Jason Hong, and Norman Sadeh briefed commissioners and staff at the Federal Trade Commission on their privacy research. They also presented a briefing to the Future of Privacy Forum.

Abby Marsh presented a paper on teen privacy at SOUPS 2014. She won a Facebook Fellowship to continue this research.



MSIT-PE students Scott Stevenson and Hsin Miao, and undergraduate Nathaniel Fruchter present their class project on "Variations in Tracking in Relation to Geographic Location." This team, along with Rebecca Balebako, presented their paper at the 2015 IEEE Security and Privacy Workshop on Web 2.0 for Security and Privacy.

Lorrie Cranor was inducted as an ACM Fellow at an awards banquet in June.

Norman Sadeh, Lorrie Cranor, Lujo Bauer, Travis Breaux and Jason Hong present a briefing to the Future of Privacy Forum.

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

Your Location has been Shared 5,398 Times!: A Field Study on Mobile App Privacy Nudging

H. Almuhimedi, F. Schaub, I. Adjerid, A. Acquisti, J. Gluck, L. Cranor, Y. Agarwal

CHI 2015

Smartphone users are often unaware of the data collected by apps running on their devices. We report on a study that evaluates the benefits of giving users an app permission manager and sending them nudges intended to raise their awareness of the data collected by their apps. Our study provides both qualitative and quantitative evidence that these approaches are complementary and can each play a significant role in empowering users to more effectively control their privacy. For instance, even after a week with access to the permission manager, participants benefited from nudges showing them how often some of their sensitive data was being accessed by apps, with 95% of participants reassessing their permissions, and 58% of them further restricting some of their permissions. We discuss how participants interacted both with the permission manager and the privacy nudges, analyze the effectiveness of both solutions, and derive some recommendations.

A Design Space for Effective Privacy Notices

F. Schaub, R. Balebako, A. Durity, and L. Cranor

SOUPS 2015

Notifying users about a system's data practices is supposed to enable users to make informed privacy decisions. Yet, current notice and choice mechanisms, such as privacy policies, are often ineffective because they are neither usable nor useful, and are therefore ignored by users. Constrained interfaces on mobile devices, wearables, and smart home devices connected in an Internet of Things exacerbate the issue. Much research has studied usability issues of privacy notices and many proposals for more usable privacy notices exist. Yet, there is little guidance for designers and developers on the design aspects that can impact the effectiveness of privacy notices. In this paper, we make multiple contributions to remedy this issue. We survey the existing literature on privacy notices and identify challenges, requirements, and best practices for privacy notice design. Further, we map out the design space for privacy notices by identifying relevant dimensions. This provides a taxonomy and consistent terminology of notice approaches to foster understanding and reasoning about notice options available in the context of specific systems. Our systemization of knowledge and the developed design space can help designers, developers, and researchers identify notice and choice requirements and develop a comprehensive notice concept for their system that addresses the needs of different audiences and considers the system's limitations and opportunities for providing notice.

What do they know about me? Contents and Concerns of Online Behavioral Profiles

A. Rao, F. Schaub, N. Sadeh

UbiComp 2014

Data aggregators collect large amount of information about individual users and create detailed online behavioral profiles of individuals. Behavioral profiles benefit users by improving products and services. However, they have also raised concerns regarding user privacy, transparency of collection practices and accuracy of data in the profiles. To improve transparency, some companies are allowing users to access their behavioral profiles. In this work, we investigated behavioral profiles of users by utilizing these access mechanisms. Using in-person interviews (n=8), we analyzed the data shown in the profiles, elicited user concerns, and estimated accuracy of profiles. We confirmed our interview findings via an online survey (n=100). To assess the claim of improving transparency, we compared data shown in profiles with the data that companies have about users. More than 70% of the participants expressed concerns about collection of sensitive data such as credit and health information, level of detail and how their data may be used. We found a large gap between the data shown in profiles and the data possessed by companies. A large number of profiles were inaccurate with as much as 80% inaccuracy. We discuss implications for public policy management.

Passwords

Measuring Real-World Accuracies and Biases in Modeling Password Guessability

B. Ur, S. Segreti, L. Bauer, N. Christin, L. Cranor, S. Komanduri, D. Kurilova, M. Mazurek, W. Melicher, R. Shay

USENIX Security 2015 (forthcoming)

Parameterized password guessability—how many guesses a particular cracking algorithm with particular training data would take to guess a password—has become a common metric of password security. Unlike statistical metrics, it aims to model real-world attackers and to provide per-password strength estimates. We investigate how cracking approaches often used by researchers compare to real-world cracking by professionals, as well as how the choice of approach biases research conclusions. We find that semi-automated cracking by professionals outperforms popular fully automated approaches, but can be approximated by combining multiple such approaches. These approaches are only effective, however, with careful configuration and tuning; in commonly used default configurations, they underestimate the real-world guessability of passwords. We find that analyses of large password sets are often robust to the algorithm used for guessing as long as it is configured effectively. However, cracking algorithms differ systematically in their effectiveness guessing passwords with certain common features (e.g., character substitutions). Our results highlight the danger of relying only on a single cracking algorithm as a measure of password strength and constitute the first scientific evidence that automated guessing can often approximate guessing by professionals.

"I Added '!' at the End to Make It Secure": Observing Password Creation in the Lab

B. Ur, F. Noma, J. Bees, S. Segreti, R. Shay, L. Bauer, N. Christin, L. Cranor

SOUPS 2015

Users often make passwords that are easy for attackers to guess. Prior studies have documented features that lead to easily guessed passwords, but have not probed why users craft weak passwords. To understand the genesis of common password patterns and uncover average users' misconceptions about password strength, we conducted a qualitative interview study. In our lab, 49 participants each created passwords for fictitious banking, email, and news website accounts while thinking aloud. We then interviewed them about their general strategies and inspirations. Most participants had a well-defined process for creating passwords. In some cases, participants consciously made weak passwords. In other cases, however, weak passwords resulted from misconceptions, such as the belief that adding "!" to the end of a password instantly makes it secure or that words that are difficult to spell are more secure than easy-to-spell words. Participants commonly anticipated only very targeted attacks, believing that using a birthday or name is secure if those data are not on Facebook. In contrast, some participants made secure passwords using unpredictable phrases or non-standard capitalization. We identify aspects of password creation ripe for guidance or automated intervention.

A Spoonful of Sugar? The Impact of Guidance and Feedback on Password-Creation Behavior

R. Shay, L. Bauer, N. Christin, L. Cranor, A. Forget, S. Komanduri, M. Mazurek, W. Melicher, and B. Ur

CHI 2015

Users often struggle to create passwords under strict requirements. To make this process easier, some providers present real-time feedback during password creation, indicating which requirements are not yet met. Other providers guide users through a multi-step password-creation process. Our 6,435-participant online study examines how feedback and guidance affect password security and usability. We find that real-time password-creation feedback can help users create strong passwords with fewer errors. We also find that although guiding participants through a three-step password-creation process can make creation easier, it may result in weaker passwords. Our results suggest that service providers should present password requirements with feedback to increase usability. However, the presentation of feedback and guidance must be carefully considered, since identical requirements can have different security and usability effects depending on presentation.

Telepathwords: Preventing Weak Passwords by Reading Users' Minds

S. Komanduri, R. Shay, L. Cranor, C. Herley, and S. Schechter

USENIX Security 2014

To discourage the creation of predictable passwords, vulnerable to guessing attacks, we present *Telepathwords*. As a user creates a password, Telepathwords makes realtime predictions for the next character that user will type. While the concept is simple, making accurate predictions requires efficient algorithms to model users' behavior and to employ already-typed characters to predict subsequent ones. We first made the Telepathwords technology available to the public in late 2013 and have since served hundreds of thousands of user sessions. We ran a human-subjects experiment to compare password policies that use Telepathwords to those that rely on composition rules, comparing participants' passwords using two different password-evaluation algorithms. We found that participants create far fewer weak passwords using the Telepathwords-based policies than policies based only on character composition.

Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption.

C. Bhagavatula, B. Ur, K. Iacovino, S. Kywe, L. Cranor, M. Savvides.

USEC 2015

While biometrics have long been promoted as the future of authentication, the recent introduction of Android face unlock and iPhone fingerprint unlock are among the first large-scale deployments of biometrics for consumers. In a 10- participant, within-subjects lab study and a 198-participant online survey, we investigated the usability of these schemes, along with users' experiences, attitudes, and adoption decisions. Participants in our lab study found both face unlock and fingerprint unlock easy to use in typical scenarios. The notable exception was that face unlock was completely unusable in a dark room. Most participants preferred fingerprint unlock over face unlock or a PIN. In our survey, most fingerprint unlock users perceived it as more secure and convenient than a PIN. In contrast, face unlock users had mixed experiences, and many had stopped using it. We conclude with design recommendations for biometric authentication on smartphones.

Social Networks

I Would Like To..., I Shouldn't..., I Wish I...: Exploring Behavior-Change Goals for Social Networking Sites

M. Sleeper, A. Acquisti, L. Cranor, P. Kelley, S. Munson, N. Sadeh

CSCW 2015

Despite the benefits they derive from social networking sites (SNSs), members of those services are not always satisfied with their online behaviors. The investigation of desires for behavior change in SNSs both provide insight into users' perceptions of how SNSs impact their lives (positively or negatively) and can inform tools for helping users achieve desired behavior changes. We use a 604-participant online survey to explore SNS users' behavior-change goals for Facebook, Instagram, and Twitter. While some participants want to reduce site use, others want to improve their use or increase a range of behaviors. These desired changes differ by SNS, and, for Twitter, by participants' levels of site use. Participants also expect a range of benefits from these goals, including more free time, contact with others, intrinsic benefits, better security/privacy, and improved self presentation. We provide insights both into how participants perceive different SNSs, as well as potential designs for behavior-change mechanisms to target SNS behaviors.

Dissertations

Mitigating the Risks of Smartphone Data Sharing: Identifying Opportunities and Evaluating Notice
PhD Thesis , Engineering & Public Policy
Rebecca Balebako, *August 2014*

Privacy Notice and Choice in Practice
PhD Thesis , Engineering & Public Policy
Pedro Leon, *August 2014*

Creating Usable Policies for Stronger Passwords with MTurk
PhD Thesis , Computation, Organizations & Society
Rich Shay, *December 2015*

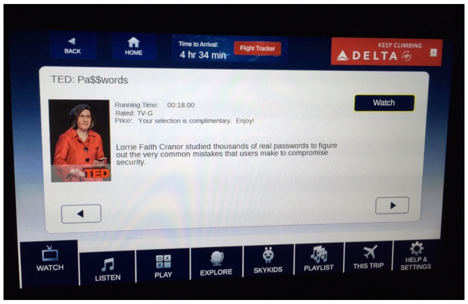
Modeling the Adversary to Evaluate Password Strength with Limited Samples
PhD Thesis , Computation, Organizations & Society
Saranga Komanduri, *May 2015*

Proposals

Supporting Security and Privacy Decisions with Data
PhD Thesis Proposal, Computation, Organizations & Society
Blase Ur, *July 2015*

Everyday Online Sharing
PhD Thesis Proposal, Computation, Organizations & Society
Manya Sleeper, *July 2015*

Blase Ur and Manya Sleeper spent a lot of time at the library while working on their thesis proposals.



Time to Arrival:
4 hr 34 min

TED: Pa$$words

Running Time: 00:18:00
Rated: TV-G
Price: Your selection is complimentary. Enjoy!

Lorrie Faith Cranor studied thousands of real passwords to figure out the very common mistakes that users make to compromise security.

Lorrie Cranor's TEDxCMU talk was featured in-flight entertainment on Delta this past winter.

CUPS students Saranga Komanduri, Blase Ur, Billy Melicher, Rich Shay, and Sean Segretti enjoying ice cream.

Tiffany Todd breathed a sigh of relief at the end of the SOUPS 2014 reception. Tiffany keeps everything running smoothly at CUPS and SOUPS.

CUPS summer interns Rupal Nahar, Daricia Wilkinson, and Adam Buchinsky discuss their research.