

Shanghai Jiao Tong University

CS267 Computer Usability and Security (Online)

Instructor Information	<p>Chentao Wu Home Institution: Shanghai Jiao Tong University Email: wuct@cs.sjtu.edu.cn</p>		
Term	December 17, 2020 - January 8, 2021	Credits	4 units
Course Delivery	<p>The class will be delivered in the format of online. Other than recorded lecture videos, the instructor will arrange 4 hours' real-time interactions with students per week (via discussion forum, zoom meeting, and WeChat). The workload students are expected to complete to properly pass this course is about 20 hours per week.</p>		
Required Texts (with ISBN)	<p>No Required Textbooks</p> <p>References:</p> <ol style="list-style-type: none"> Jonathan Lazar, Jinjuan Heidi Feng, Harry Hochheiser. Research Methods in Human-Computer Interaction. ISBN: 9780128053904. Lorrie Cranor, Simson Garfinkel. Security and Usability: Designing Secure Systems that People Can Use. ISBN: 9780596008277. 		
Prerequisite	<p>Programming language, data structures, operating systems, computer organization, computer network, etc.</p>		

Course Overview

Regardless of how secure a system is in theory, failing to consider how humans actually use the system leads to disaster in practice. This course will examine how to design for security and privacy from a user-centered perspective by combining insights from computer systems, human-computer interaction (HCI), and public policy. We will introduce core security and privacy technologies, as well as HCI techniques for conducting robust user studies. Topics will include usable authentication, user-centered web security, anonymity software, privacy notices, security warnings, and data-driven privacy tools in domains ranging from social media to the Internet of Things. Students will complete weekly problem sets, as well as conduct novel research in a group capstone project. No prior experience in security, privacy, or HCI is required.

Learning Outcomes

Successful participants can answer all the security/privacy and usability HCI questions as below,

How do **users** select graphical passwords? How can we help them choose passwords harder for **attackers** to predict?

As the password space increases, what are the impacts on usability factors and predictability of human selection?

Course Structure

This course bridges security and usability as below

Security	Usability/HCI	Usable Security
Humans are a secondary constraint to security constraints	Humans are the primary constraint, security rarely considered	Human factors and security are both primary constraints
Humans considered primarily in their role as adversaries/attackers	Concerned about human error but not human attackers	Concerned about both normal users and adversaries
Involves threat models	Involves task models, mental models, cognitive models	Involves threat models AND task models, mental models, etc.
Focus on security metrics	Focus on usability metrics	Considers usability and security metrics together
User studies rarely done	User studies common	User studies common, often involve deception + active adversary



Grading Policy

Attendance	10%
Middle Exam	20%
Projects	30%
Final Exam	40%

Grading Scale is as follows

Number grade	Letter grade	GPA
90-100	A	4.0
85-89	A-	3.7
80-84	B+	3.3
75-79	B	3.0
70-74	B-	2.7
67-69	C+	2.3
65-66	C	2.0
62-64	C-	1.7
60-61	D	1.0
≤59	F (Failure)	0

Class Schedule

Date	Lecture	Readings
Day 1	Course overview and introductions Introduction to security; usable encryption	Reading I
Day 2	Reasoning about the human in the loop	Reading II
Day 3	Introduction to privacy	Reading III
Day 4	Online meeting and discussion	
Day 5	Introduction to experimental design: overview of methods, ethics/deception, and ecological validity Introduction to crowdsourced studies	Reading IV
Day 6	Participant recruitment and surveys Interviews, focus groups, and diary studies + analyzing qualitative data	Reading V
Day 7	Analyzing quantitative data with statistics Quantitative data collection, lab and field studies, simulating attacks	Reading VI
Day 8	Online meeting, review & discussion	Reading VII
Day 9	Middle Exam	
Day 10	Analyzing quantitative data with statistics	Reading VII
Day 11	Security warnings	Reading VIII
Day 12	Passwords	Reading IX
Day 13	Online meeting and discussion	
Day 14	Authentication beyond text passwords Privacy notice and choice	Reading X
Day 15	Evaluating disclosures Privacy and anonymity tools	Reading XI
Day 16	Social networks and privacy Privacy and security for mobile devices and IoT	Reading XII
Day 17	Online meeting, review & discussion	
Day 18	Final Exam	

Reading I

Required reading:

- Alma Whitten and J.D. Tygar. [Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.](#) In *Proceedings of the 8th USENIX Security Symposium*, 1999. (USENIX '99)

Optional reading:

- Sascha Fahl, Marian Harbach, Thomas Muders, Matthew Smith, and Uwe Sander. [Helping Johnny 2.0 to Encrypt His Facebook Conversations.](#) In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 2012. (SOUPS '12)
- [HCI] Shirley Gaw, Edward W. Felten, and Patricia Fernandez-Kelly. [Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted Email.](#) In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2006. (CHI '06)
- Sumeet Gujrati and Eugene Y. Vasserman. [The usability of Truecrypt, or how I learned to stop whining and fix an interface.](#) In *Proceedings of the third ACM Conference on Data and Application Security and Privacy*, 2013. (CODASPY '13)
- [HCI] Scott Ruoti, Nathan Kim, Ben Burgon, Timothy van der Horst, Kent Seamons. [Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes.](#) In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, 2013. (SOUPS '13)
- [Security] Mark D. Ryan. [Enhanced certificate transparency and end-to-end encrypted mail.](#) In *Proceedings of the 21st Annual Network & Distributed System Security Symposium*, 2014. (NDSS '14)

Reading II

Required reading:

- Lorrie Faith Cranor. [A Framework for Reasoning About the Human in the Loop.](#) In *Proceedings of the 1st Conference on Usability, Psychology, and Security*, 2008. (UPSEC '08)

Optional reading:

- Anne Adams and Martina Angela Sasse. [Users Are Not The Enemy.](#) In *Communications of the ACM*, Volume 42, Issue 12, pp. 40-46, December 1999.
- L. Jean Camp. [Reconceptualizing the Role of Security User.](#) In *Daedalus*, Volume 140, Number 4, pp. 93-107, Fall 2011.
- W. Keith Edwards, Erika Shehan Poole, and Jennifer Stoll. [Security Automation Considered Harmful?](#) In *Proceedings of the 2007 New Security Paradigms Workshop*, 2007. (NSPW '07)
- Steven Furnell. [Making security usable: Are things improving?](#) In *Computers & Security*, Volume 26, Issue 6, pg. 434-443, September 2007.
- M.E. Kabay. [Using Social Psychology to Implement Security Policies.](#) In *Computer Security Handbook*, 4th edition, 2002.
- Butler Lampson. [Usable Security: How to Get It.](#) In *Communications of the ACM*, Volume 52, Issue 11, pp. 25-27, November 2009.

Reading III

Required reading:

- Allison Woodruff, Vasyl Pihur, Sunny Consolvo, Lauren Schmidt, Laura Brandimarte, and Alessandro Acquisti. [Would a Privacy Fundamentalist Sell Their DNA for \\$1000...If Nothing Bad Happened as a Result? The Westin Categories, Behavioral Intentions, and Consequences.](#) In *Proceedings of the Tenth Symposium on Usable Privacy and Security*, 2014. (SOUPS '14)

Optional reading:

- Alex Braunstein, Laura Granka, and Jessica Staddon. [Indirect Content Privacy Surveys: Measuring Privacy Without Asking About It](#). In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, 2011. (SOUPS '11)
- Lorrie Faith Cranor, Adam L. Durity, Abigail Marsh, and Blase Ur. [Parents' and Teens' Perspectives on Privacy In a Technology-Filled World](#). In *Proceedings of the Tenth Symposium on Usable Privacy and Security*, 2014. (SOUPS '14)
- Alexei Czeskis, Ivayla Dermendjieva, Hussein Yapit, Alan Borning, Batya Friedman, Brian Gill, and Tadayoshi Kohno. [Parenting from the Pocket: Value Tensions and Technical Directions for Secure and Private Parent-Teen Mobile Safety](#). In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, 2010. (SOUPS '10)
- Giovanni Iachello and Jason Hong. [End-User Privacy in Human-Computer Interaction](#). In *Foundations and Trends in HCI*, Volume 1, Number 1, pp. 1-137, 2007.
- Scott Lederer, Jason I. Hong, Anind K. Dey, James A. Landay. [Personal Privacy through Understanding and Action: Five Pitfalls for Designers](#). Carnegie Mellon University Technical Report. Human-Computer Interaction Institute. Paper 78. 2004.

Reading IV

Required reading:

- Lazar et al. [Research Methods in Human-Computer Interaction](#). Chapter 2: Experimental Research
- Lazar et al. [Research Methods in Human-Computer Interaction](#). Chapter 3: Experimental Design
- Lazar et al. [Research Methods in Human-Computer Interaction](#). Chapter 14: Working With Human Subjects
- Tom Jagatic, Nathaniel Johnson, Markus Jakobsson, and Filippo Menczer. [Social phishing](#). In *Communications of the ACM*, Volume 50, Issue 10, pp. 94-100, October 2007.
- Richard Shay, Saranga Komanduri, Adam L. Durity, Philip (Seyoung) Huh, Michelle L. Mazurek, Sean M. Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. [Can long passwords be secure and usable?](#). In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2014. (CHI '14)
- Manya Sleeper, Justin Cranshaw, Patrick Gage Kelley, Blase Ur, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. ["I read my Twitter the next morning and was astonished": A Conversational Perspective on Twitter Regrets](#). In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2013. (CHI '13)
- Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. [Privacy Attitudes of Mechanical Turk Workers and the U.S. Public](#). In *Proceedings of the Tenth Symposium on Usable Privacy and Security*, 2014. (SOUPS '14)
-

Optional reading:

- Lazar et al. [Research Methods in Human-Computer Interaction](#). Chapter 10: Usability Testing
- [Ethics] Cristian Bravo-Lillo, Serge Egelman, Cormac Herley, Stuart Schechter, and Janice Tsai. [You Needn't Build That: Reusable Ethics-Compliance Infrastructure for Human Subjects Research](#). In *Proceedings of the Cyber-security Research Ethics Dialog & Strategy Workshop*, 2013. (CREDS '13)
- Roy A. Maxion. [Making Experiments Dependable](#). In *Dependable and Historic Computing*, Lecture Notes in Computer Science Volume 6875, pp. 344-357, 2011.



- Michael Buhrmester, Tracy Kwang, and Samuel D. Gosling. [Amazon's Mechanical Turk: A New Source of Inexpensive, Yet High-Quality, Data?](#). In *Perspectives on Psychological Science*, Volume 6, Number 1, pp. 3-5, 2011.
- Panagiotis G. Ipeirotis. [Demographics of Mechanical Turk](#). New York University Technical Report, 2010.
- Panagiotis G. Ipeirotis, Foster Provost, and Jing Wang. [Quality Management on Amazon Mechanical Turk](#). In *Proceedings of the ACM SIGKDD Workshop on Human Computation*, 2010. (HCOMP '10)
- Patrick Gage Kelley. [Conducting usable privacy and security studies with Amazon's Mechanical Turk](#). In *Proceedings of the Usable Security Experiment Reports Workshop*, 2010. (USER '10)
- Aniket Kittur, Ed H. Chi, and Bongwon Suh. [Crowdsourcing User Studies With Mechanical Turk](#). In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2008. (CHI '08)

Reading V

Required reading:

- Lazar et al. [Research Methods in Human-Computer Interaction](#). Chapter 5: Surveys
- Lazar et al. [Research Methods in Human-Computer Interaction](#). Chapter 8: Interviews and Focus Groups
- Xuan Zhao, Niloufar Salehi, Sashi Naranjit, Sara Alwaalan, Stephen Volda, and Dan Cosley. [The Many Faces of Facebook: Experiencing Social Media as Performance, Exhibition, and Personal Archive](#). In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2013. (CHI '13)
- Lazar et al. [Research Methods in Human-Computer Interaction](#). Chapter 11: Analyzing Qualitative Data
- B. Ur, F. Noma, J. Bees, S. Segreti, R. Shay, L. Bauer, N. Christin, L. Cranor. ["I Added '!' At The End To Make It Secure": Observing Password Creation in the Lab](#). SOUPS2015.
- A. Forget, S. Pearman, J. Thomas, A. Acquisti, N. Christin, L. Cranor, S. Egelman, M. Harbach, R. Telang. [Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes](#). SOUPS2016.

Optional reading:

- Lazar et al. [Research Methods in Human-Computer Interaction](#). Chapter 6: Diaries
- Lazar et al. [Research Methods in Human-Computer Interaction](#). Chapter 7: Case Studies
- Blase Ur, Jaeyeon Jung, and Stuart Schechter. [Intruders versus intrusiveness: Teens' and parents' perspectives on home-entryway surveillance](#). In *Proceedings of the 2014 ACM Conference on Ubiquitous Computing*, 2014. (UbiComp '14)
- [HCI] A.J. Brush, Jaeyeon Jung, Ratul Mahajan, and Frank Martinez. [Digital Neighborhood Watch: Investigating the Sharing of Camera Data Amongst Neighbors](#). In *Proceedings of the 2013 conference on Computer Supported Cooperative Work*, 2013. (CSCW '13)
- Michelle L. Mazurek, J.P. Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, Richard Shay, Kami Vaniea, Lujo Bauer, Lorrie Faith Cranor, Gregory R. Ganger, and Michael K. Reiter. [Access Control for Home Data Sharing: Attitudes, Needs and Practices](#). In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2010. (CHI '10)
- Stuart Schechter. [The User IS the Enemy, and \(S\)he Keeps Reaching for that Bright Shiny Power Button!](#) In *Proceedings of the Workshop on Home Usable Privacy and Security*, 2013. (HUPS '13)

Reading VI

Required reading:

- Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. [It's a Hard Lock Life: A Field Study of Smartphone \(Un\)Locking Behavior and Risk Perception](#). In *Proceedings of the Tenth Symposium on Usable Privacy and Security*, 2014. (SOUPS '14)
- Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. [The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies](#). In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, 2007. (Oakland '07)

Optional reading:

- Lazar et al. [Research Methods in Human-Computer Interaction](#). Chapter 12: Automated Data Collection Methods
- Devdatta Akhawe and Adrienne Porter Felt. [Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness](#). In *Proceedings of the 22nd USENIX Security Symposium*, 2013. (USENIX '13)
- Alexander De Luca, Marc Langheinrich, and Heinrich Hussmann. [Towards Understanding ATM Security - A Field Study of Real World ATM Use](#). In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, 2010. (SOUPS '10)
- Dinei Florêncio and Cormac Herley. [A Large-Scale Study of Web Password Habits](#). In *Proceedings of the 16th international conference on World Wide Web*, 2007. (WWW '07)
- Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. [A Field Trial of Privacy Nudges for Facebook](#). In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2014. (CHI '14)

Reading VII

Required reading:

- Lazar et al. [Research Methods in Human-Computer Interaction](#). Chapter 4: Statistical Analysis

Optional reading:

- (Various) Mark S. Kaiser. Any one of the [chapters on advanced statistical methods](#).
- (Factor Analysis) Frank J. Floyd and Keith F. Widaman. [Factor Analysis in the Development and Refinement of Clinical Assessment Instruments](#).
- (Mixed Models) Donald Hedeker. [Generalized Linear Mixed Models](#).
- (Mixed Models) Any one of the [chapters on mixed-effects models](#) (with R tutorials)
- (Repeated Measures) Michael Kristensen and Thomas Hansen. [Statistical analyses of repeated measures in physiological research: a tutorial](#)
- (Regression Analysis) Alan O. Sykes. [An Introduction to Regression Analysis](#).
- (Regression Analysis) Robert Kieschnick and B.D. McCullough. [Regression analysis of variates observed on \(0, 1\): percentages, proportions and fractions](#)

Reading VIII

Required reading:

- Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, Saranga Komanduri, Robert W. Reeder, Stuart Schechter, and Manya Sleeper. [Your Attention Please: Designing security-decision UIs to](#)

make genuine risks harder to ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, 2013. (SOUPS '13)

Optional reading:

- Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Emre Acer, Elisabeth Morant, and Sunny Consolvo. Rethinking Connection Security Indicators. SOUPS 2016.
- Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. Bridging the gap in computer security warnings: A mental model approach. In *IEEE Security and Privacy magazine*, Volume 9, Issue 2, pp. 18-26, March 2011.
- Cristian Bravo-Lillo, Lorrie Faith Cranor, Saranga Komanduri, Stuart Schechter, and Manya Sleeper. Harder to Ignore? Revisiting Pop-Up Fatigue and Approaches to Prevent It. In *Proceedings of the Tenth Symposium on Usable Privacy and Security*, 2014. (SOUPS '14)
- Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, Saranga Komanduri, Stuart Schechter, and Manya Sleeper. Operating system framed in case of mistaken identity. In *Proceedings of the 2012 ACM SIGSAC conference on Computer & Communications Security*, 2012. (CCS '12)
- [HCI] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2008. (CHI '08)
- David Modic and Ross J. Anderson. Reading this May Harm Your Computer: The Psychology of Malware Warnings. Available online on SSRN, 2014.
- [HCI] Na Wang, Jens Grossklags, and Heng Xu. An Online Experiment of Privacy Authorization Dialogues for Social Applications. In *Proceedings of the 2013 conference on Computer Supported Cooperative Work*, 2013. (CSCW '13)

Reading IX

Required reading:

- Michelle L. Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur. Measuring Password Guessability for an Entire University. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security*, 2013. (CCS '13)

Optional reading:

- Robert Biddle, Sonia Chiasson, and P.C. van Oorschot. Graphical Passwords: Learning from the First Twelve Years. In *ACM Computing Surveys*, Volume 44, Issue 4, August 2012.
- [Security] Joseph Bonneau. The science of guessing: analyzing an anonymized corpus of 70 million passwords. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, 2012. (S&P '12 / Oakland '12)
- Joseph Bonneau and Stuart Schechter. Towards reliable storage of 56-bit secrets in human memory. In *Proceedings of the 23rd USENIX Security Symposium*, 2014. (USENIX '14)
- Sonia Chiasson, Alain Forget, Elizabeth Stobert, P.C. van Oorschot, and Robert Biddle. Multiple password interference in text and click-based graphical passwords. In *Proceedings of the 2009 ACM SIGSAC conference on Computer & Communications Security*, 2009. (CCS '09)
- [Security] Darren Davis, Fabian Monrose, and Michael K. Reiter. On user choice in graphical password schemes. In *Proceedings of the 13th USENIX Security Symposium*, 2004. (USENIX '04)
- Eiji Hayashi, Jason Hong, and Nicolas Christin. Security through a different kind of obscurity: Evaluating Distortion in Graphical Authentication Schemes. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2011. (CHI '11)



- [Security] Ari Juels and Ronald L. Rivest. [Honeywords: Making Password-Cracking Detectable](#). In *Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security*, 2013. (CCS '13)
- Saranga Komanduri, Richard Shay, Lorrie Faith Cranor, Cormac Herley, and Stuart Schechter. [Telepathwords: Preventing Weak Passwords by Reading Users' Minds](#). In *Proceedings of the 23rd USENIX Security Symposium*, 2014. (USENIX '14)
- [HCI] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman. [Of passwords and people: Measuring the effect of password-composition policies](#). In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2011. (CHI '11)
- Daniel McCarney, David Barrera, Jeremy Clark, Sonia Chiasson, Paul C. van Oorschot. [Tapas: Design, Implementation, and Usability Evaluation of a Password Manager](#). In *Proceedings of the 28th Annual Computer Security Applications Conference*, 2012. (ACSAC '12)
- [HCI] Florian Schaub, Marcel Walch, Bastian Könings, and Michael Weber. [Exploring the Design Space of Graphical Passwords on Smartphones](#). In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, 2013. (SOUPS '13)
- [Security] David Silver, Suman Jana, Dan Boneh, Eric Chen, and Collin Jackson. [Password Managers: Attacks and Defenses](#). In *Proceedings of the 23rd USENIX Security Symposium*, 2014. (USENIX '14)
- [HCI] Elizabeth Stobert and Robert Biddle. [The Password Life Cycle: User Behaviour in Managing Passwords](#). In *Proceedings of the Tenth Symposium on Usable Privacy and Security*, 2014. (SOUPS '14)
- Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz. [Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns](#). In *Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security*, 2013. (CCS '13)
- Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. [How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation](#). In *Proceedings of the 21st USENIX Security Symposium*, 2012. (USENIX '12)

Reading X

Required reading:

- Shrirang Mare, Mary Baker, Jeremy Gummeson. [A study of authentication in daily life](#). SOUPS 2016.
- Florian Schaub, Rebecca Balebako, Adam Durity, Lorrie Cranor. [A Design Space for Effective Privacy Notices](#). SOUPS 2015.

Optional reading:

- J. Bonneau, C. Herley, P. C. van Oorschot and F. Stajano. [The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes](#). IEEE Security & Privacy (Oakland) 2012.
- Stuart Schechter, A. J. Bernheim Brush, and Serge Egelman. [It's No Secret: Measuring the Security and Reliability of Authentication via 'Secret' Questions](#). In *Proceedings of the 2009 IEEE Symposium on Security and Privacy*, 2009. (S&P '09 / Oakland '09)
- Chandrasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides. [Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption](#). In *Proceedings of the NDSS Workshop on Usable Security*, 2015. (USEC '15)



- [Application] Eric Grosse and Mayank Upadhyay, [Authentication at Scale](#), *IEEE Security & Privacy (magazine)*, vol. 11, no. 1, pp. 15-22, January-February 2013.
- Eiji Hayashi, Sauvik Das, Shahriyar Amini, Jason Hong, Ian Oakley. [CASA: Context-Aware Scalable Authentication](#). In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, 2013. (SOUPS '13)
- Anil K. Jain, Arun Ross, and Salil Prabhakar. [An introduction to biometric recognition](#). In *IEEE Transactions on Circuits and Systems for Video Technology*, Volume 14, Issue 1, pp. 4-20, 2004.
- [HCI] Mike Just and David Aspinall. [Personal choice and challenge questions: a security and usability assessment](#). In *Proceedings of the Fifth Symposium on Usable Privacy and Security*, 2009. (SOUPS '09)
- Kat Krol, Eleni Philippou, Emiliano De Cristofaro, and M. Angela Sasse. ["They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking](#). In *Proceedings of the NDSS Workshop on Usable Security*, 2015. (USEC '15)
- [Security] Tey Chee Meng, Payas Gupta, and Debin Gao. [I can be You: Questioning the use of Keystroke Dynamics as Biometrics](#). In *Proceedings of the 20th Annual Network & Distributed System Security Symposium*, 2013. (NDSS '13)
- Saurabh Panjwani and Edward Cutrell. [Usably Secure, Low-Cost Authentication for Mobile Banking](#). In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, 2010. (SOUPS '10)
- Robert W. Reeder and Stuart Schechter. [When the Password Doesn't Work: Secondary Authentication for Websites](#). In *IEEE Security and Privacy magazine*, Volume 9, Issue 2, pp. 43-49, March 2011.
- Stuart Schechter, Serge Egelman, and Robert W. Reeder. [It's not what you know, but who you know: A social approach to last-resort authentication](#). In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2009. (CHI '09)
- Travis D. Breaux and Florian Schaub. [Scaling Requirements Extraction to the Crowd: Experiments with Privacy Policies](#). In *22nd IEEE International Requirements Engineering Conference*, 2014. (RE '14)
- Joel R. Reidenberg, Travis D. Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James T. Graves, Fei Liu, Aleecia M. McDonald, Thomas B. Norton, Rohan Ramanath, N. Cameron Russell, Norman Sadeh, Florian Schaub. [Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding](#). In *Berkeley Technology Law Journal*, vol. 30, 2015 (forthcoming).
- Lorrie Faith Cranor, Pedro Giovanni Leon, and Blase Ur. 2016. [A Large-Scale Evaluation of U.S. Financial Institutions' Standardized Privacy Notices](#). ACM Trans. Web 10, 3, Article 17 (August 2016), 33 pages.

Reading XI

Required reading:

- Lorrie Faith Cranor. [Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice](#). In *Journal of Telecommunications and High Technology Law*, Volume 10, Number 2, 2012.
- Pedro G. Leon, Blase Ur, Rebecca Balebako, Lorrie Faith Cranor, Richard Shay, and Yang Wang. [Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising](#). In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2012. (CHI '12)

Optional reading:



- Rebecca Balebako, Richard Shay, and Lorrie Faith Cranor. [Is Your Inseam a Biometric? Evaluating the Understandability of Mobile Privacy Notice Categories](#). Carnegie Mellon University Technical Report CMU-CyLab-13-011, 2013.
- Pedro G. Leon, Justin Cranshaw, Lorrie Faith Cranor, Jim Graves, Manoj Hastak, Blase Ur, and Guzi Xu. [What Do Online Behavioral Advertising Disclosures Communicate to Users?](#) In *Proceedings of the 11th annual ACM Workshop on Privacy in the Electronic Society*, 2012. (WPES '12)
- Aleecia McDonald, Robert W. Reeder, Patrick Gage Kelley, and Lorrie Faith Cranor. [A Comparative Study of Online Privacy Policies and Formats](#). In *Proceedings of the 9th International Symposium on Privacy Enhancing Technologies*, 2009. (PETS '09)
- Patrick Gage Kelley, Lucian Cescas, Joanna Bresee, and Lorrie Faith Cranor. [Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach](#). In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2010. (CHI '10)
- S. Egelman, J. Tsai, L. Cranor, and A. Acquisti. 2009. [Timing Is Everything? The Effects of Timing and Placement of Online Privacy Indicators](#). CHI 2009.
- Lorrie Faith Cranor, Praveen Guduru, and Manjula Arjula. [User interfaces for privacy agents](#). In *ACM Transactions on Computer-Human Interaction (TOCHI)*, Volume 13, Issue 2, pp. 135-178, June 2006.
- W. Melicher, M. Sharif, J. Tan, L. Bauer, M. Christodorescu, P. Leon. [\(Do Not\) Track Me Sometimes: Users' Contextual Preferences for Web Tracking](#). Proceedings on Privacy Enhancing Technologies, Volume 2016, Issue 2 (Apr 2016).
- [Security] Gunes Acar, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan, and Claudia Diaz. [The Web Never Forgets: Persistent Tracking Mechanisms in the Wild](#). In *Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security*, 2014. (CCS '14)
- Gaurav Aggarwal, Elie Bursztein, Collin Jackson, and Dan Boneh. [An analysis of private browsing modes in modern browsers](#). In *Proceedings of the 19th USENIX Security Symposium*, 2010. (USENIX '10)
- Rachna Dhamija and J.D. Tygar. [The Battle Against Phishing: Dynamic Security Skins](#). In *Proceedings of the First Symposium on Usable Privacy and Security*, 2005. (SOUPS '05)
- Jonathan R. Mayer and John C. Mitchell. [Third-Party Web Tracking: Policy and Technology](#). In *Proceedings of the 2013 IEEE Symposium on Security and Privacy*, 2013. (S&P '13 / Oakland '13)
- Franziska Roesner, Christopher Rovillos, Tadayoshi Kohno, and David Wetherall. [ShareMeNot: Balancing Privacy and Functionality of Third-Party Social Widgets](#). In *USENIX ;login: magazine*, Volume 37, Number 4, August 2012.
- Blase Ur, Pedro G. Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. [Smart, Useful, Scary, Creepy: Perceptions of Behavioral Advertising](#). In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 2012. (SOUPS '12)
- Greg Norcie, Jim Blythe, Kelly Caine, and L. Jean Camp. [Why Johnny Can't Blow the Whistle: Identifying and Reducing Usability Issues in Anonymity Systems](#). In *Proceedings of the NDSS Workshop on Usable Security*, 2014. (USEC '14)
- [Security] Roger Dingledine, Nick Matthewson, and Paul Syverson. [Tor: The Second-Generation Onion Router](#). In *Proceedings of the 13th USENIX Security Symposium*, 2004. (USENIX '04)
- [Security] Prateek Mittal, Matthew Wright, and Nikita Borisov. [Pisces: Anonymous Communication Using Social Networks](#). In *Proceedings of the 20th Annual Network & Distributed System Security Symposium*, 2013. (NDSS '13)

Reading XII

Required reading:

- Maritza Johnson, Serge Egelman, and Steven M. Bellovin. [Facebook and Privacy: It's Complicated](#). In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 2012. (SOUPS '12)
- Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. [Android Permissions: User Attention, Comprehension, and Behavior](#). SOUPS 2012

Optional reading:

- Lujo Bauer, Lorrie Faith Cranor, Saranga Komanduri, Michelle L. Mazurek, Michael K. Reiter, Manya Sleeper, and Blase Ur. [The Post Anachronism: The Temporal Dimension of Facebook Privacy](#). In *Proceedings of the 12th annual ACM Workshop on Privacy in the Electronic Society*, 2013. (WPES '13)
- Michael S. Bernstein, Eytan Bakshy, Moira Burke, and Brian Karrer. [Quantifying the Invisible Audience in Social Networks](#). In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2013. (CHI '13)
- Sanjay Kairam, Michael J. Brzozowski, David Huffaker, and Ed H. Chi. [Talking in Circles: Selective Sharing in Google+](#). In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2012. (CHI '12)
- Huina Mao, Xin Shuai, and Apu Kapadia. [Loose Tweets: An Analysis of Privacy Leaks on Twitter](#). In *Proceedings of the 10th annual ACM Workshop on Privacy in the Electronic Society*, 2011. (WPES '11)
- Manya Sleeper, Rebecca Balebako, Sauvik Das, Amber Lynn McConahy, Jason Wiese, and Lorrie Faith Cranor. [The Post that Wasn't: Exploring Self-Censorship on Facebook](#). In *Proceedings of the 2013 conference on Computer Supported Cooperative Work*, 2013. (CSCW '13)
- Fred Stutzman, Ralph Gross, and Alessandro Acquisti. [Silent Listeners: The Evolution of Privacy and Disclosure on Facebook](#). In *Journal of Privacy and Confidentiality*, Volume 4, Number 2, pp. 7-41, 2012.
- Yang Wang, Saranga Komanduri, Pedro Giovanni Leon, Gregory Norcie, Alessandro Acquisti, and Lorrie Faith Cranor. ["I regretted the minute I pressed share": A Qualitative Study of Regrets on Facebook](#). In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, 2011. (SOUPS '11)
- Jason Watson, Andrew Besmer, Heather Richter Lipford. [+Your Circles: Sharing Behavior on Google+](#). In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 2012. (SOUPS '12)
- [HCI] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Cranor, and Carolyn Nguyen. ["Little Brothers Watching You:" Raising Awareness of Data Leaks on Smartphones](#). In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, 2013. (SOUPS '13)
- Serge Egelman, Sakshi Jain, Rebecca S. Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. [Are You Ready to Lock? Understanding User Motivations for Smartphone Locking Behaviors](#). In *Proceedings of the 2014 ACM SIGSAC conference on Computer & Communications Security*, 2014. (CCS '14)
- [HCI] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. [Privacy as part of the app decision-making process](#). In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2013. (CHI '13)
- [Security] Benjamin Livshits and Jaeyeon Jung. [Automatic Mediation of Privacy-Sensitive Resource Access in Smartphone Applications](#). In *Proceedings of the 22nd USENIX Security Symposium*, 2013. (USENIX '13)



- [Security] Iasonas Polakis, Panagiotis Ilia, Federico Maggi, Marco Lancini, Georgios Kontaxis, Stefano Zanero, Sotiris Ioannidis, and Angelos D. Keromytis. [Faces in the Distorting Mirror: Revisiting Photo-based Social Authentication](#). In *Proceedings of the 2014 ACM SIGSAC conference on Computer & Communications Security*, 2014. (CCS '14)
- [Security] Shashi Shekhar, Michael Dietz, and Dan S. Wallach. [AdSplit: Separating smartphone advertising from applications](#). In *Proceedings of the 21st USENIX Security Symposium*, 2012. (USENIX '12)