Topics (Additional Reading Material)

Following the topic assignments, below is some additional literature you should try to read to help you structure the proposal for what you would like to study.

Remember that you can approach your project in a variety of ways (as discussed in class) but it is very important that you have a security/privacy usability research question as the centrally focus of your work.

Example:

> **Project topic:** Longer Passwords for Secure Authentication
> **Research Question:** "Can Longer Passwords be both Usable and Secure?"
> **A Possible Solution:** **"Can Longer Passwords be Secure and Usable?", Shay et al. (CHI 2014) DOI: 10.1145/2556288.2557377**

Topic #1: Two factor authentication

Two-factor authentication provides a method of allowing users to protect their online accounts by using combination of a password and a code sent to the user's mobile device. So, instead of authenticating a user using only the user's login and password information, the user is required to declare a trusted mobile device to which an authentication code is sent. The authentication code is what unlocks access to the account. The advantage here is that the user's account is protected because an attacker required both the user's password and mobile device – which makes the attacker's job harder. However, on the downside, this introduces a number of usability problems. For example, what happens when the user loses the trusted mobile device? And how do we deal with cases in which network, or device malfunctions make receiving the code difficult or impossible? The goal of this project is to examine the usability of two factor authentication. Does it make users feel more secure? Does it make users feel annoyed/frustrated? Why are users using or not using this technology? What about location and context privacy?

Related References:

- Google's Two-Factor Authentication Scheme. Google 2-Step Verification
- Microsoft's Two-Factor Authentication Scheme. Two-step verification: FAQ
- Apple's Two-Factor Authentication Scheme. When Things go wrong.

Additional References:

1. Ding Wang, Qianchen Gu, Haibo Cheng, and Ping Wang. 2016. The Request for Better Measurement: A Comparative Evaluation of Two-Factor Authentication Schemes. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security* (ASIA CCS '16). ACM, New York, NY, USA, 475-486. DOI: http://dx.doi.org/10.1145/2897845.2897916

2. Joshua Tan, Lujo Bauer, Joseph Bonneau, Lorrie Faith Cranor, Jeremy Thomas, and Blase Ur. 2017. Can Unicorns Help Users Compare Crypto Key Fingerprints?. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing*

Systems (CHI '17). ACM, New York, NY, USA, 3787-3798. DOI: https://doi.org/10.1145/3025453.3025733

3. Alexander De Luca, Alina Hang, Emanuel von Zezschwitz, and Heinrich Hussmann. 2015. I Feel Like I'm Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (CHI '15). ACM, New York, NY, USA, 1411-1414. DOI: https://doi.org/10.1145/2702123.2702141

4. Vijay Rajanna, Seth Polsley, Paul Taele, and Tracy Hammond. 2017. A Gaze Gesture-Based User Authentication System to Counter Shoulder-Surfing Attacks. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (CHI EA '17). ACM, New York, NY, USA, 1978-1986. DOI: https://doi.org/10.1145/3027063.3053070

5. Can Liu, Gradeigh D. Clark, and Janne Lindqvist. 2017. Where Usability and Security Go Hand-in-Hand: Robust Gesture-Based Authentication for Mobile Systems. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (CHI '17). ACM, New York, NY, USA, 374-386. DOI: https://doi.org/10.1145/3025453.3025879

6. Tobias Seitz, Manuel Hartmann, Jakob Pfab, and Samuel Souque. 2017. Do Differences in Password Policies Prevent Password Reuse?. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (CHI EA '17). ACM, New York, NY, USA, 2056-2063. DOI: https://doi.org/10.1145/3027063.3053100

Topic #3: Privacy on Social Media Platforms

Most social platforms offer methods of configuring privacy settings to protect against disclosure of information to unauthorised parties. Yet, quite frequently privacy exposure occurs by transitive disclosures due mainly to users failing to configure privacy settings. Possible reasons for this are centred on the complexity of the privacy configuration process. In this study we would like to go beyond the idea of privacy setting complexity to discover why users engage in using social media platforms without considering the potential for privacy disclosure. One potential idea to base this study on is the notion of "learned helplessness", and social graph deanonymization (see also Six Degrees of Kevin Bacon).

Related References:

- Ming Cheung and James She. 2016. "Evaluating the Privacy Risk of User-Shared Images". *ACM Trans. Multimedia Comput. Commun. Appl.* 12, 4s, Article 58 (September 2016)
- Suhendry Effendy, Roland H.C. Yap, and Felix Halim. 2012. Revisiting link privacy in social networks. In *Proceedings of the second ACM conference on Data and Application Security and Privacy* (CODASPY '12). ACM, New York, NY, USA, 61-70.
- Anirban Basu, Juan Camilo Corena, Shinsaku Kiyomoto, Stephen Marsh, Jaideep Vaidya, Guibing Guo, Jie Zhang, and Yutaka Miyake. 2014. Privacy preserving trusted social feedback.

In *Proceedings of the 29th Annual ACM Symposium on Applied Computing* (SAC '14). ACM, New York, NY, USA, 1706-1711.

Additional References:

1. Carol Moser, Tianying Chen, and Sarita Y. Schoenebeck. 2017. Parents? and Children?s Preferences about Parents Sharing about Children on Social Media. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (CHI '17). ACM, New York, NY, USA, 5221-5225. DOI: https://doi.org/10.1145/3025453.3025587

2. Jose M. Such, Joel Porter, Sören Preibusch, and Adam Joinson. 2017. Photo Privacy Conflicts in Social Media: A Large-scale Empirical Study. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (CHI '17). ACM, New York, NY, USA, 3821-3832. DOI: https://doi.org/10.1145/3025453.3025668

3. Wali Ahmed Usmani, Diogo Marques, Ivan Beschastnikh, Konstantin Beznosov, Tiago Guerreiro, and Luís Carriço. 2017. Characterizing Social Insider Attacks on Facebook. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (CHI '17). ACM, New York, NY, USA, 3810-3820. DOI: https://doi.org/10.1145/3025453.3025901

4. Wael Ghonim. 2017. Mobocratic Algorithms: Could Social Media be a Threat to Democracy?. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (CHI EA '17). ACM, New York, NY, USA, 3-3. DOI: https://doi.org/10.1145/3027063.3056455

5. Yang Wang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. 2011. "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* (SOUPS '11). ACM, New York, NY, USA, , Article 10 , 16 pages. DOI: https://doi.org/10.1145/2078827.2078841

Topic #4: Usability of client side anonymity tools

Many users are interested in anonymous communications, for a number of reasons. In particular, journalists and activists may want to protect their sources, receive anonymous tips, and so forth. The Tor Browser Bundle is probably one of the best known anonymous software tools, and allows clients to browse the web anonymously. There has however not be any principled usability study of Tor and its alternatives (e.g., I2P, Freenet) showing whether or not users might be making very dangerous mistakes. The first study here would be to look at the usability of such tools including anonymity bundles like Whonix and Tails from a client perspective. Since those are supposed to be providing complete anonymity out-of-the-box, do people configure them properly? Do they engage in activities that could actually reveal information about them (e.g., activating JavaScript, etc). This project could be merged with the next project.

Related items:

- Secure Drop.https://securedrop.org/
- Joseph Cox. This Researcher Is Hunting Down IP Addresses of Dark Web Sites. Motherboard. June 2015.
- Susan E. McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. Investigating the Computer Security Practices and Needs of Journalists. In Proceedings of USENIX Security. August 2015.

Additional References:

1. Mikhail Bilenko and Matthew Richardson. 2011. Predictive client-side profiles for personalized advertising. In *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining* (KDD '11). ACM, New York, NY, USA, 413-421. DOI=http://dx.doi.org/10.1145/2020408.2020475

2. Daniel Arp, Fabian Yamaguchi, and Konrad Rieck. 2015. Torben: A Practical Side-Channel Attack for Deanonymizing Tor Communication. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security* (ASIA CCS '15). ACM, New York, NY, USA, 597-602. DOI: http://dx.doi.org/10.1145/2714576.2714627

3. Alfred Kobsa, Bart P. Knijnenburg, and Benjamin Livshits. 2014. Let's do it at my place instead?: attitudinal and behavioral study of privacy in client-side personalization. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '14). ACM, New York, NY, USA, 81-90. DOI: https://doi.org/10.1145/2556288.2557102

Topic #5: Location and Context Privacy in the Internet of Things

The Internet of Things (IoT) promises great advances in convenience and efficiency. This comes at potentially a significant cost to privacy, however, as both our devices (e.g., mobile phones, health and fitness devices) and sensors in our environment (e.g., cameras, presence sensors, microphones) track where we are and what we do, anytime and anywhere. A prerequisite for building mechanisms to help users maintain control of their privacy is understanding users' concerns: which types of sensing are users most or least comfortable with and why. This project will examine (potentially via an experience-sampling study) users' concerns to sensing based on type of data collected (e.g., audio, video, heart rate, location), where the sensing happens (e.g., home, work, restaurant, street, shopping mall), how the collected data is used (e.g., to provide users with specific features that benefit them, to provide better ads, to make city infrastructure more efficient), how long the collected data is kept, and other dimensions.

Related references:

- S. Higginbotham. Companies need to share how they use our data. Here are some ideas. Fortune, July 6, 2015.
- Internet of Things: Privacy and Security in a Connected World. FTC Staff Reports. January 2015.

Additional References:

1. Xiaoxun Sun, Hua Wang, and Jiuyong Li. 2009. Injecting purpose and trust into data anonymisation. In *Proceedings of the 18th ACM conference on Information and knowledge management* (CIKM '09). ACM, New York, NY, USA, 1541-1544. DOI=http://dx.doi.org/10.1145/1645953.1646166

2. Ji Zhang, Xuemei Liu, and Yonglong Luo. 2013. An efficient and robust privacy protection technique for massive streaming choice-based information. In *Proceedings of the 22nd ACM international conference on Information & Knowledge Management* (CIKM '13). ACM, New York, NY, USA, 1169-1172. DOI=http://dx.doi.org/10.1145/2505515.2507816

3. Xuan Shang, Ke Chen, Lidan Shou, Gang Chen, and Tianlei Hu. 2010. (k,P)-anonymity: towards pattern-preserving anonymity of time-series data. In *Proceedings of the 19th ACM international conference on Information and knowledge management* (CIKM '10). ACM, New York, NY, USA, 1333-1336. DOI=http://dx.doi.org/10.1145/1871437.1871614

4. George Theodorakopoulos, Reza Shokri, Carmela Troncoso, Jean-Pierre Hubaux, and Jean-Yves Le Boudec. 2014. Prolonging the Hide-and-Seek Game: Optimal Trajectory Privacy for Location-Based Services. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society* (WPES '14). ACM, New York, NY, USA, 73-82. DOI=http://dx.doi.org/10.1145/2665943.2665946

5. Dingqi Yang, Daqing Zhang, Bingqing Qu, and Philippe Cudré-Mauroux. 2016. PrivCheck: privacy-preserving check-in data publishing for personalized location based services. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (UbiComp '16). ACM, New York, NY, USA, 545-556. DOI: http://dx.doi.org/10.1145/2971648.2971685

6. Eran Toch. 2014. Crowdsourcing privacy preferences in context-aware applications. *Personal Ubiquitous Comput.* 18, 1 (January 2014), 129-141. DOI: http://dx.doi.org/10.1007/s00779-012-0632-0

7. Thore Fechner and Christian Kray. 2012. Attacking location privacy: exploring human strategies. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (UbiComp '12). ACM, New York, NY, USA, 95-98. DOI=http://dx.doi.org/10.1145/2370216.2370232

Topic #6: Exploring Users' Privacy Preferences and Publicly Shared Data

Anonymizing data is important in protecting the privacy of individual users in a sample of data collected. For example, healthcare and population sampling data can be used to discover meaningful trends, but should not allow users to be able to identify individuals from the sample dataset. Studies however, indicate that obtaining "perfect" anonymization is a time consuming process, and that taking into account user privacy preferences can be used to drop the performance requirements of anonymization algorithms. In this study, we consider standard anonymization algorithms, and examine user concerns with personal information disclosure based on the type of data collected. Can a given user's privacy preference requirements affect (negatively or positively) other users' preferences? What are the implications of merging privacy preference-aware datasets with ones that aren't or that have conflicting preference expressions?

Related References:

- Pedro Giovanni Leon, Blase Ur, Yang Wang, Manya Sleeper, Rebecca Balebako, Richard Shay, Lujo Bauer, Mihai Christodorescu, and Lorrie Faith Cranor. 2013. What matters to users?: factors that affect users' willingness to share information with online advertisers. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (SOUPS '13). ACM, New York, NY, USA, , Article 7 , 12 pages. DOI: http://dx.doi.org/10.1145/2501604.2501611
- Andrew McNamara, Akash Verma, Jon Stallings, and Jessica Staddon. 2016. Predicting Mobile App Privacy Preferences with Psychographics. In *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society* (WPES '16). ACM, New York, NY, USA, 47-58. DOI: https://doi.org/10.1145/2994620.2994631

Additional References:

1. Noman Mohammed, Benjamin C.M. Fung, and Mourad Debbabi. 2009. Walking in the crowd: anonymizing trajectory data for pattern analysis. In *Proceedings of the 18th ACM conference on Information and knowledge management* (CIKM '09). ACM, New York, NY, USA, 1441-1444. DOI=http://dx.doi.org/10.1145/1645953.1646140

2. Ji Zhang, Xuemei Liu, and Yonglong Luo. 2013. An efficient and robust privacy protection technique for massive streaming choice-based information. In *Proceedings of the 22nd ACM international conference on Information & Knowledge Management* (CIKM '13). ACM, New York, NY, USA, 1169-1172. DOI=http://dx.doi.org/10.1145/2505515.2507816

3. Xuan Shang, Ke Chen, Lidan Shou, Gang Chen, and Tianlei Hu. 2010. (k,P)-anonymity: towards pattern-preserving anonymity of time-series data. In *Proceedings of the 19th ACM international conference on Information and knowledge management* (CIKM '10). ACM, New York, NY, USA, 1333-1336. DOI=http://dx.doi.org/10.1145/1871437.1871614

4. Jeremy Birnholtz, Nicholas Aaron Ross Merola, and Arindam Paul. 2015. "Is it Weird to Still Be a Virgin": Anonymous, Locally Targeted Questions on Facebook Confession Boards. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (CHI '15). ACM, New York, NY, USA, 2613-2622. DOI: https://doi.org/10.1145/2702123.2702410

5. Ari Schlesinger, Eshwar Chandrasekharan, Christina A. Masden, Amy S. Bruckman, W. Keith Edwards, and Rebecca E. Grinter. 2017. Situated Anonymity: Impacts of Anonymity, Ephemerality, and Hyper-Locality on Social Media. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (CHI '17). ACM, New York, NY, USA, 6912-6924. DOI: https://doi.org/10.1145/3025453.3025682

6. Thore Fechner and Christian Kray. 2012. Attacking location privacy: exploring human strategies. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (UbiComp '12). ACM, New York, NY, USA, 95-98. DOI=http://dx.doi.org/10.1145/2370216.2370232