Possible Presentation Topics (2017)

These are possible topics you may choose from to prepare both your portfolio and presentation. The idea is for each participant to work on a single topic of his/her choice. However, if you would like to partner with another classmate to work on a topic, please discuss this with the instructor.

Please indicate your preferences for the topic(s) you are interested in using the doodle poll by Monday, 15 May 2017.

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.

Topic #2: Usability of Text and Graphical Passwords

Authentication by means of text based passwords, and relatively recently, graphical passwords is fairly standard. However, using both authentication methods present significant usability challenges particularly when multiple user accounts exist, and password memorability becomes an issue. Why do users ignore safe usage warnings in spite of the risks of identity disclosure and privacy exposure, and why are the multitude of existing password schemes failing to address the problem of personal data protection, effectively? What would help improve usability while offering the same or even better protection?

Related References:

- D. Jaeger, C. Pelchen, H. Graupner, F. Cheng und C. Meinel, „Analysis of Publicly Leaked Credentials and the Long Story of Password Re-Use," in *11th International Conference on Passwords (PASSWORDS 2016)*, Bochum, Germany, December 5-7, 2016.

- „Identity Leak Checker,“ [Online]. Available: https://sec.hpi.uni-potsdam.de/leak-checker/search?lang=en.

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 centered 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.

Topic #4: Usability of client side anonymity tools

Anonymous communication protocols are typically interesting from the client’s perspective because they allow the users exchange information without revealing personal information. For example, political activists and journalists can use such systems to receive anonymous tips and communicate with informers. Browers like Tor, I2P, and Freenet are probably the best known anonymous browsing software tools, and allow clients (users) to browse the web anonymously. In this study we would like to evaluate the usability of anonymous browsing tools to consider the following questions:

- Are users using these tools properly? Or are they making usage mistakes that can potentially reveal personal information? For example, activating JavaScript, etc.
- How practically usable are such tools, including variants like Whonix and Tails, from the client’s perspective?
- Are the motivations for using such tools merely to protect personal information or are there other motivations?
- How can these tools be re-designed to protect clients but also prevent (or discourage) subversive activities?

Related References:

- 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.

Topic #5: Location and Context Privacy in a Smart World

The growing availability of smart devices (phone, watches, as well as health and fitness devices) and sensors (cameras, presence and touch sensors) in our environment offer a great deal of convenience and efficiency. This comes at a cost to privacy, since these devices track where we are at, what we do when, and where. A prerequisite for building mechanisms to help users maintain control of their privacy is to understand the fears and concerns of the users. How much information are users comfortable with revealing? Are they aware of what information is revealed? In this study, we examine user concerns with sensing based on the type of data collected (e.g. audio, video, location, …), where the data is collected (context – home, work, restaurant, street, shopping mall), how the data collected is used (targeted advertising, making infrastructure and services more efficient…), and how long the data is kept (forever, …), and other dimensions. This study can be conducted jointly with the next one (by a team of two).

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.

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