Project Topics. (Usable Security and Privacy Seminar – Summer 2018)

Project #1: "I forgot my XXX Password"

A common problem users face is that of remembering several passwords for multiple accounts. The result is that users have adopted various coping strategies such as using the same password on multiple accounts, using the same password with only slight character changes, and so on. In order to address this issue security experts have come up with various countermeasures such as graphical passwords, password managers, multi-factor authentication, and so on. In this project we seek to find answers to the following two questions:

- To what extent do users use password managers to support password memorability over multiple websites?
- Are users aware that password managers collect private or sensitive information about web usage behavior?
- Are users aware that the auto-fill functions in password manager applications could be abused to steal stored passwords through hidden phishing attacks?

References:

- Open source password managers
- Pearman et al. (2017). "Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat." In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17). ACM, New York, NY, USA, pp. 295-310
- Wash et al. (2016). "Understanding Password Choices: How Frequently Entered Passwords Are Re-used across Websites." In Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), pp. 175 – 187
- Jaeger et al. (2016), "Analysis of Publicly Leaked Credentials and the Long Story of Password Re-Use", In Proceedings of the 11th International Conference on Passwords (PASSWORS 2016), Bochum, Germany, Dec. 5-7, 2016

Project #2: Two-Factor Authentication

Two-factor authentication provides a method of allowing users to protect their online accounts from shoulder surfing attacks by using a combination of a password and a code shared with a trusted device. The authentication code is what unlocks access to the user account. From the security expert's perspective, this makes the adversary's job harder because both the user's password and trusted device are required to access the account. On the user's end a number of questions arise. For example:

- What happens if the trusted device is lost/stolen?
- What happens if network delay makes receiving the code impossible?

In this project, we seek to answer the following questions:

- Why users don't use two-factor authentication (if given the choice not to)?
- What measures can be taken to encourage using two-factor authentication?

References:

- Apple's Two-Factor Authentication Scheme
- Khamis et al. (2017), "GTmoPass: Two-Factor Authentication on Public Displays Using Gaze-Touch Passwords and Personal Mobile Devices", In Proceedings of the 6th ACM International Symposium on pervasive Displays (PerDis), Article No. 8, Lugano, Switzerland
- Wang et al. (2016), "The Request for Better Measurement: A Comparative Evaluation of Two-Factor Authentication Schemes", In Proceedings of the 11th ACM Asia Conference on Computer and Communications Security, pp. 475-486, May 30-June 03, 2016

Project #3: Privacy and Third-Party Applications

Social media platforms offer a variety of methods to protect user privacy. While users are increasingly privacy-aware, quite frequently privacy exposure occurs by transitive disclosures via third-party apps, shared images, and location/context settings. In this project, we would like to answer three questions namely:

- Do users actually understand data sharing with third-party apps when using social login tools?
- Do users feel a sense of lack of control in preventing private information exposure?
- Have users given up trying to control private information exposure?

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)
- Lujo Bauer, Cristian Bravo-Lillo, Elli Fragkaki, and William Melicher. 2013. A comparison of users' perceptions of and willingness to use Google, Facebook, and Google+ single-sign-on functionality. In Proceedings of the 2013 ACM workshop on Digital identity management (DIM '13). ACM, New York, NY, USA, 25-36. DOI=http://dx.doi.org/10.1145/2517881.2517886

Project #4: Anonymous Browsing

Anonymous communication protocols are typically interesting from the user's perspective because of the opportunities provided to users to exchange information without revealing personal information. Browsers like Tor, I2P, and Freenet are good examples. In this project we want to answer the following questions:

- Are users making usage mistakes that can potentially reveal personal information? (e.g. activating JavaScript, location settings on mobile devices, etc.)

- What are user perceptions of the capabilities of anonymous browsers?
- What are user motivations for using anonymous browsers?

References:

- Jessica Su, Ansh Shukla, Sharad Goel, and Arvind Narayanan. 2017. De-anonymizing Web Browsing Data with Social Networks. In Proceedings of the 26th International Conference on World Wide Web (WWW '17). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland, 1261-1269. DOI: https://doi.org/10.1145/3038912.3052714
- McGregor et al. (2015), “Investigating the Computer Security Practices and Needs of Journalists”, In Proceedings of USENIX Security, August 2015
- Joseph Cox (2015), “This Researcher is Hunting Down IP Addresses of Dark Web Sites”, June 2015.