"Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat"

Abstract:
Text passwords—a frequent vector for account compromise, yet still ubiquitous—have been studied for decades by researchers attempting to determine how to coerce users to create passwords that are hard for attackers to guess but still easy for users to type and memorize. Most studies examine one password or a small number of passwords per user, and studies often rely on passwords created solely for the purpose of the study or on passwords protecting low-value accounts. These limitations severely constrain our understanding of password security in practice, including the extent and nature of password reuse, password behaviors specific to categories of accounts (e.g., financial websites), and the effect of password managers and other privacy tools.

In the paper on which this presentation is based, we report on an *in situ* study of 154 participants over an average of 147 days each. Participants' computers were instrumented—with careful attention to privacy—to record detailed information about password characteristics and usage, as well as many other computing behaviors such as use of security and privacy web browser extensions. This data allows a more accurate analysis of password characteristics and behaviors across the full range of participants' web-based accounts. Examples of our findings are that the use of symbols and digits in passwords predicts increased likelihood of reuse, while increased password strength predicts decreased likelihood of reuse; that password reuse is more prevalent than previously believed, especially when partial reuse is taken into account; and that password managers may have no impact on password reuse or strength. We also observe that users can be grouped into a handful of behavioral clusters, representative of various password management strategies. Our findings suggest that once a user needs to manage a larger number of passwords, they cope by partially and exactly reusing passwords across most of their accounts.

Bio:
Sarah Pearman is a behavioral researcher who has worked with the CyLab Usable Privacy and Security research group since 2015. Sarah's primary focus in the CUPS group (and the focus of this talk) is the Security Behavior Observatory (SBO) project, a longitudinal field study of home computer user behavior. Sarah received her MA at the University of Pittsburgh and her bachelor's degree at Vanderbilt University.