If You Can't Get Them to the Lab: Evaluating a Virtual Study Environment with Security Information Workers

Nicolas Huaman, Alexander Krause, Dominik Wermke, Jan H. Klemmer, Christian Stransky, Yasemin Acar, Sascha Fahl

Abstract: Usable security and privacy researchers use many study methodologies, including interviews, surveys, and laboratory studies. Of those, lab studies allow for particularly flexible setups, including programming experiments or usability evaluations of software. However, lab studies also come with challenges: Often, it is particularly challenging to recruit enough skilled participants for in-person studies. Especially researchers studying security information workers reported on similar recruitment challenges in the past. Additionally, situations like the COVID-19 pandemic can make in-person lab studies even more challenging Finally, institutions with limited resources may not be able to conduct lab studies.

Therefore, we present and evaluate a novel virtual study environment prototype, called OLab, that allows researchers to conduct lab-like studies remotely using a commodity browser. Our environment overcomes lab-like study challenges and supports flexible setups and comprehensive data collection. In an iterative engineering process, we design and implement a prototype based on requirements we identified in previous work and conduct a comprehensive evaluation including a cognitive walkthrough with usable security experts, a guided and supervised online study with DevOps, and an unguided and unsupervised online study with computer science students. We can confirm that our prototype supports a wide variety of lab-like study setups and received positive feedback from all study participants.

The Potential of S&P Adepts to Serve as a Social Resource in the Users' Quest for More Secure and Privacy-Preserving Behavior

Nina Gerber, Karola Marky

There are several ways to inform individuals about secure and privacy-preserving behavior in private social environments. Experts who are versed in security and privacy (S&P), who might be social peers, such as family members or friends, can provide advice or give recommendations. In this paper, we specifically investigate how S&P adepts inform peers in their private social environment about security and privacy. For this, we first conducted thirteen in-depth interviews with S&P adepts, revealing 1) their own S&P behavior and strategies in their personal lives, 2) obstacles in S&P conversations with peers, 3) situations in which S\&P adepts intervene in the behavior of others, and 4) the perception of S&P adepts and stereotypes. Based on the interview results, we conducted three co-design workshop sessions with S&P adepts to explore options to better support S&P adepts informing their peers about secure and privacy-preserving behavior.

"Fast, Easy, Convenient." Studying Adoption and Perception of Digital Covid Certificates

Franziska Herbert, Marvin Kowalewski, Theodor Schnitzler, Leona Lassak, Markus Dürmuth

Digital vaccination certificates, used to enforce access restrictions during the COVID-19 pandemic, represent an interesting showcase for digital security and privacy in the context of sensitive personal data. In this paper, we take a look at which types of certificates and related apps people in Germany use, which factors influence their adoption, and which misconceptions exist concerning the security and use of certificates. We report the results of a census-representative online survey in Germany (n = 800) conducted in December 2021, complemented with 30 qualitative street interviews.

"As soon as it's a risk, I want to require MFA": How Administrators Configure Risk-based Authentication

Philipp Markert, Theodor Schnitzler, Maximilian Golla, Markus Dürmuth

Risk-based authentication complements standard password-based logins by using knowledge about previously observed user behavior to prevent malicious login attempts. In this paper, we observed how n = 28 system administrators configure RBA using a mock-up system modeled after Amazon Cognito. We find that administrators want to have a thorough understanding of the system they configure, show the importance of default settings as they are either directly adopted or depict an important orientation.

Exploring User Authentication with Windows Hello in a Small Business Environment

Florian M. Farke, Leona Lassak, Jannis Pinter, Markus Dürmuth

Windows Hello for Business is an alternative to password-based authentication that addresses common password problems like weak passwords, password leaks, and phishing attacks. We conducted a qualitative study with 13 employees accompanying its introduction in a small business studying its usability and deployability. Participants found it more usable and faster than the traditional Windows sign-in scheme. Interestingly, participants tended to use PINs instead of biometrics, due to privacy concerns as well as lack of hardware support and workplace setup.