Passwords are still the most common authentication method on the web. They are inexpensive and easy to implement. Users are largely accustomed to this kind of authentication but passwords represent a considerable nuisance, because they are tedious to create, remember, and maintain. In many cases, usability issues turn into security problems, because people try to work around the challenges and create easily predictable credentials. Often, they reuse their passwords for many purposes, which aggravates the risk of identity theft. There have been numerous attempts to remove the root of the problem and replace passwords, e.g., through biometrics. However, no other authentication strategy can fully replace them, so passwords will probably stay a go-to authentication method for the foreseeable future.

Researchers and practitioners have thus aimed to improve users' situation in various ways. There are two main lines of research on helping users create both usable and secure passwords. On the one hand, password policies notably influence password practices, because they enforce certain characteristics. However, enforcement reduces users' autonomy and often causes frustration if the requirements are poorly communicated or overly complex. On the other hand, user-centered designs have been proposed: Assistance and persuasion are typically more user-friendly but their influence is often limited. In this thesis, we explore potential reasons for the inefficacy of certain persuasion strategies. From the gained knowledge, we derive novel persuasive design elements to support users in password authentication.

The exploration of contextual factors in password practices is based on four projects that reveal both psychological aspects and real-world constraints. Here, we investigate how mental models of password strength and password managers can provide important pointers towards the design of persuasive interventions. Moreover, the associations between personality traits and password practices are evaluated in three user studies. A meticulous audit of real-world password policies shows the constraints for selection and reuse practices.

Based on the review of context factors, we then extend the design space of persuasive password support with three projects. We first depict the explicit and implicit user needs in password support. Second, we craft and evaluate a choice architecture that illustrates how a phenomenon from marketing psychology can provide new insights into the design of nudging strategies. Third, we tried to empower users to create memorable passwords with emojis. The results show the challenges and potentials of emoji-passwords on different platforms. Finally, the thesis presents a framework for the persuasive design of password support. It aims to structure the required activities during the entire process. This enables researchers and practitioners to craft novel systems that go beyond traditional paradigms, which is illustrated by a design exercise.

Tobias Seitz - Supporting Users in Password Authentication with Persuasive Design

Supporting Users in Password Authentication with Persuasive Design

Tobias Seitz

Dissertation an der Fakultät für Mathematik, Informatik und Statistik der Ludwig-Maximilians-Universität München

München, 26. April 2018