SaTC: CORE: Small:
Identifying and Quantifying Design Principles For Improving Password Manager Usage

Scott Ruoti, University of Tennessee, Knoxville

https://userlab.utk.edu/projects/nsf-satc-2022

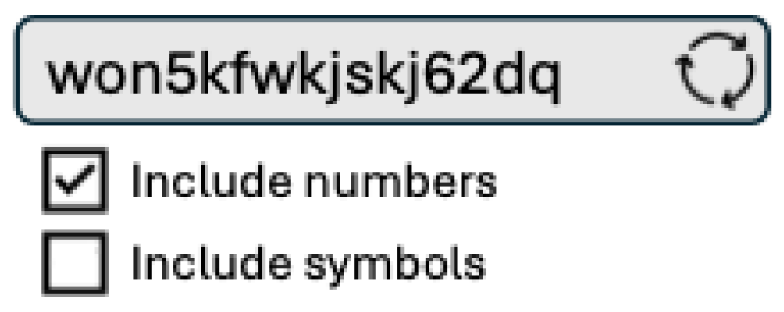
Everyone knows that **passwords are insecure**. **Password managers** have the potential to radically **improve users' password hygiene**. However, research consistently shows users **underutilize the security-critical functionality** of password managers that would improve password hygiene.

What can be done?

Objectives

Our work seeks to identify blockers for the adoption and consistent usage of security-critical functionality in password managers. It also seeks to create design principles to addressing these blockers. We plan to start with three types of functionality:

Password generation



won5kfwkjskj62dq

☑ Include numbers

□ Include symbols

Credential audits

Parent-child management

Approach

1. Study existing security-critical features to better understand why users reject using them
2. Design and prototype potential solutions to those issues
3. Conduct empirical studies to measure the extent to which competing designs address these issues
4. Leverage qualitative feedback to explain the strengths and weaknesses of each design, allowing for the creation of generalizable design principles

Impact on Society

- Our work has the potential to improve the password hygiene of the *hundred million plus users* who already use a password manager
- Our work aims to lower the barrier to adoption for password managers, making it easier for the entirety world's population to secure their passwords

Scientific Impact

- We are identifying, quantifying, and explaining the ability of various design principles to improve the usage of password managers' security-critical functionality
- We have gathered data on input metrics for entering passwords using a range of input modalities (e.g., keyboard, remote control, game controller), allowing the community to crate more effective human-oriented password generation algorithms and schemes
- We will explore how parents and children navigate the collaborative usage of password managers

Breakthrough

We created a trusted, in-browser pathway for password autofill that prevents password theft by browser-based injection attacks and malicious extensions. We also developed a provenance scheme that enables the rapid attribution of attack campaigns stealing passwords. We have also extended our defense to protect FIDO2-based 2FA against local attacks.

Impact on Students and Education

This grant has supported 1 Ph.D. dissertation, 2 MS theses, and 2 REU. It is currently supporting 2 Ph.D. candidates and 2 REU. Students come from a range of background, including traditionally underrepresented communities.

Results from this research have been integrated into units on authentication and usable security for an *Introduction to Cybersecurity* and a *Software Security* course

The 6th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
September 4-5, 2024 | Pittsburgh, Pennsylvania

Video