OnePass

A Stateless Password Manager

Claire Cannatti, Christophe Hauser, Jelena Mirkovic, and Matteo Dell'Amico

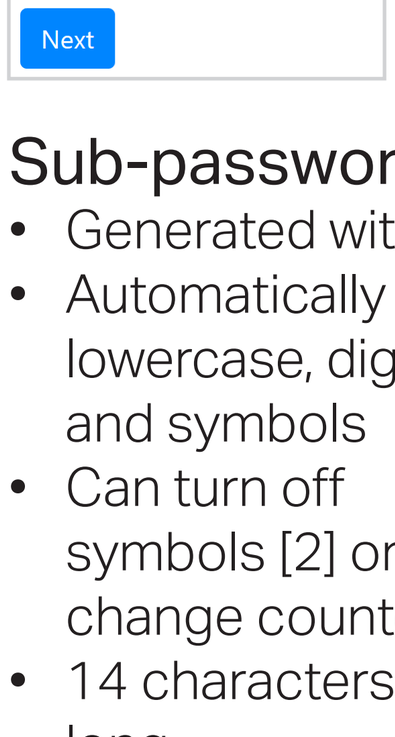
PROBLEM STATEMENT

Passwords are difficult to remember, and users have many accounts that require passwords. This causes users to choose memorable but weak passwords and then reuse them, which creates major security problems.

We propose a method for users to only need to remember one password that they use to access all their other passwords from any device at any time.

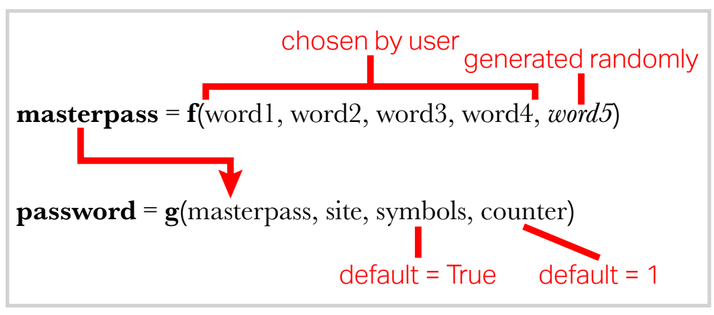
APPROACH

Master passphrase



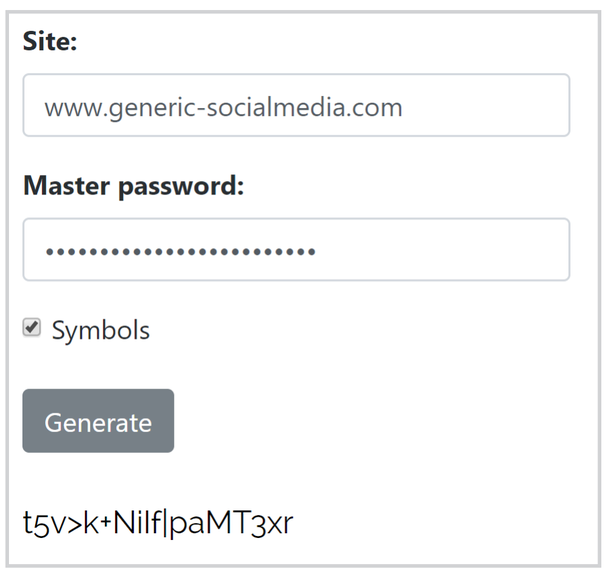
1. User chooses 4 words
2. We give them 1 word
3. Check the strength of the whole passphrase with Monte Carlo method [1]

This approach maximizes memorability while ensuring sufficient strength against attackers.



Sub-password

- Generated with PBKDF2-HMAC, SHA-256
- Automatically includes uppercase, lowercase, digits, and symbols
- Can turn off symbols [2] or change counter
- 14 characters long



BENEFITS

- Stateless
  - Accessible from anywhere
  - Passwords are never stored
- Password manager
  - Never forget passwords or have to write them down
- OnePass
  - As little memorization as possible
    - Symbol inclusion
  - State of the art master password quality control
  - User-tested

RELATED WORK

[1] Matteo Dell'Amico and Maurizio Filippone. Monte carlo strength evaluation: Fast and reliable password checking. In Proceedings of the 22nd ACMSIGSAC Conference on Computer and Communications Security, pages158–169. ACM, 2015.

[2] Ding Wang and Ping Wang. The emperor's new password creation policies. In European Symposium on Research in Computer Security, pages 456–477.Springer, 2015.

Usability testing

- Amazon Mechanical Turk testing for master password memorability, overall usability
  - Two-part study includes week-later evaluation of memorability

USC University of Southern California

If interested contact Claire Cannatti
ccannatt@wellesley.edu

Work performed under REU Site program
supported by NSF grant #1659886

USC Viterbi School of Engineering