Project title

Eliminate password custodians with hardware/USB key

Names of group members

Hsin-ih Tu

Dataset(s) (either existing or self-collected)

Troy Hunt's "Have I Been Pwned" database

Problem(s) to work on

Trust in providers to store passwords (continues to be violated).

- Looking at the OWASP cheatsheet for password management (we expect providers to stay current)
- Eval'ed the Moodle, Open edX LMS treatment of passwords (Canvas?)
- Postpone (non-solution) of password managers (e.g., LastPass, Bitwarden)
- what is the prediction of quantum computers breaking exisiting hash values? (best case; versus worst case, which are the current rash of violations)

Potential ways to solve problem(s)

1. OAuth2
2. 2FA, Multi-factor authentication
   A. OTP app
   B. biometric, phone, sms, e-mail
3. None (password-less)
   A. hardware key (e.g., Yubikey, Solokey)

What to complete by the milestone

1. Follow the Tock OS tutorial
   A. OpenSK (Fido2)
2. Authenticate to the WebAuthn site

References

1. Meta fined $101M; Techcrunch Sep 2024 *(https://techcrunch.com/2024/09/27/meta-fined-101-5m-for-2019-breach-that-exposed-hundreds-of-millions-of-facebook-passwords/)*
2. Google released quantum resilient FIDO2 key; Bleeping Computer Aug 2023 *(https://www.bleepingcomputer.com/news/security/google-released-first-quantum-resilient-fido2-key-implementation/)*
3. Tock OS; *(https://tockos.org/papers/)*