Prioritizing Security over Usability: Strategies for How People Choose Passwords

Rick Wash and Emilee Rader, Michigan State University

How do people choose which password to use on which website?

We tested four hypotheses against real password data from 134 university students to see which of 4 classes of strategies are consistent with password data.

Strong inference: Rather than test hypotheses against uninformative null hypotheses, find "**critical situations**" where multiple hypotheses cannot simultanously hold, and see which predicts the observed outcome (Platt, 1964).

A Critical Situation: University Passwords

High usability needs: entered every day. *H3 predicts low complexity.*
High security needs: protects grades, personal and financial info. *H4 predicts high complexity.*

H3 and H4 can't both hold for university passwords!

H1 People reuse the same password everywhere.

Only 1.5% (2 of 136) users reused the same password everywhere.

Only 14% (19 of 136) even have a dominant password that they use on 75% or more of websites.

On average, each user has 4-8 distinct passwords.

X H1 is inconsistent with data.

H2 People choose passwords focusing on ease of creation (aka mimimum password policies).

Only 16.2% of passwords are at or below the minumum entropy.

Passwords average 21 bits of complexity more than required.

70% of passwords are more complex than required across all websites they are used on.

60% of passwords exceed both the character class and length minimums.

X H2 is inconsistent with data.

H3 People make a security/usability tradeoff focusing on ease of use.

Correlation between password complexity and how often the password is entered: 0.00

Correlation between password complexity and how often the website is visited: -0.03

Correlation between password complexity and number of website visits per password entry: 0.03

X H3 is inconsistent with data.

H4 People make a security/usability tradeoff focusing on security.

High complexity (>50 bits) categories:

- Economy and Finance (55)
- Information Tech (54)
- Education (51)
- Business (51)

Low complexity (<50 bits)

- Games (46)
- Sports (45)

Correlation between password complexity and website importance: 0.11

H4 is consistent with data.

Conclusion: Participants chose passwords most consistent with H4.

Results suggest participants made a usability/security tradeoff.

- Used **more complex passwords** on types of websites with **high security needs**.
- Used **less complex passwords** on types of websites that are **less security sensitive.**

For university passwords, **H4** is the only one consistent with the data:

University password complexity averages 57 bits.

- Higher than any other category of website
- Over 10 bits higher than the mimimum required

This work was supported by the U.S. National Science Foundation under grants no. CNS-1116544 and CNS-1115926.