Password policies of most top websites fail to follow best practices

Kevin Lee

kvnl@cs.princeton.edu

Graduate Student Researcher
Princeton University

Joint work with Sten Sjöberg, Arvind Narayanan
Passwords aren’t going anywhere

• Password strength is still important.
• Best practices from research to encourage stronger passwords:
  – Use blocklists
  – Use a strength meter (that accurately models adversarial guessability)
  – Don’t require specific types of characters
But are websites listening to the research?

• Research questions:
  – Are websites preventing users from using the most common passwords?
  – Are websites using password strength meters to encourage hard-to-guess passwords?
  – What composition rules/policies (PCPs) are used?
• Tested 120 English-language websites among most popular websites in the world (according to Tranco)
Study 1: Are websites preventing setting the most common passwords?

- **Best practice**: use blocklists to prevent users from choosing bad passwords (Kelley et al., 2012, Shay et al., 2015, Habib et al., 2017).

- **We tested 2 sets of 20 passwords:**
  - **leaked passwords** (sampled from HIBP-100k most common list)
  - **easiest-guessed passwords** (guessed by an ensemble of password cracking tools, CMU’s Password Guessability Service)
  - Websites with identical PCPs (1class6, 3class8, etc.) tested with same set of passwords
Study 1: 71 sites allowed all *leaked* and *easiest-guessed* PWs

- 71 websites, including Amazon, TikTok, Netflix, WSJ, allowed all 40 PWs.
  - 123456, p@ssw0rd allowed
  - Sensitive user information stored at these websites
- 19 websites had insufficient strategies, such as only blocking “123”
- Only 22 websites allowed ≤ 5 of the 40 PWs tested
Study 2: Are websites using strength meters?

- **Best practice**: use meter to estimate resistance to adversary cracking (guessability), not complexity (Tan et al., 2020, de Carnavalet et al., 2014)
- We tested the password input fields and looked for any feedback.
• Low adoption: only 23 websites were using strength meters at all.
• Of those, 10 use meters as nudges toward character-class PCPs
  – 6 websites have minimum-length PCPs (no character-class reqs) only, so strength
    meter being used as proxy for character-class PCPs
  – 4 websites use meters to encourage even more complexity than required.
• **Also**: inconsistency with server: 12/23 websites were inconsistent between
  meter feedback and password acceptance
Study 3: Have sites moved on from character-class PCPs?

• Best practice: don’t require specific types of characters in passwords
  (Komanduri et al., 2011, Kelley et al., 2012, Tan et al., 2020).

• We manually extracted and reverse-engineered the PCPs at all 120 websites
Study 3: Character-class PCPs are still widely used

• We found 54 websites still using character-class PCPs, despite all the research and recommendations against using them
• Websites with character-class PCPs are more likely to allow leaked and easiest-guessed passwords
  – 38/54 (70%) allowed all 40 passwords we tested in Study 1 (compared to 50% for websites with a no character-class requirements)
All in all: only 15 websites were following best practices

- **Security:** allows $\leq 5$ of the 40 common known-weak passwords we tried (e.g. “12345678”).

- **Security:** uses a strength meter that accurately models guessability OR requires a minimum length of 8.*

- **Usability:** does not require specific types of characters.

- Websites following all three criteria:
Why is this research-practice gap so large?

• More research is needed!
  – Engage with system administrators to get their perspectives on password security.

• Some hypotheses:
  – Password policy is security theater.
  – Websites have shifted their attention to adopting other authentication technologies, and believe that it is unnecessary to strengthen their password policies.
  – Websites need to pass security audits, and the firms who do these audits, such as Deloitte, recommend or mandate outdated practices.
  – Some other practical constraint that the academic community does not know about.
Recap

• Most top websites are not following best practices in their password policy.
  – Users are either at risk from being allowed to set vulnerable passwords, and/or frustrated from character-class requirements.
  – The research is clear, but it looks like practice lags research.
• Future work: understand why system administrators are not following these best practices
Thank you!

Paper, data: passwordpolicies.cs.princeton.edu
Email: kvnl@cs.princeton.edu