Passwords/multi-factor authentications

Mainack Mondal

CS 60081
Autumn 2020

Roadmap

- Passwords/multi factor authentications
- Usability for security developers
- Online tracking
- Privacy notices/dark patterns
- Temporal aspect of privacy

Roadmap

- Passwords/multi factor authentications
- Usability for security developers
- Online tracking
- Privacy notices/dark patterns
- Temporal aspect of privacy

Good authentication system should be …

- User friendly
  - Memorable, scalable, physically no/little effort, easy to learn, infrequent errors, easy to recover from fault
- Ease of implementation
  - Accessible, negligible cost per user, server deployable, browser deployable, free
- Protection against
  - Targeted impersonation, throttled guessing, unthrottled guessing

Passwords

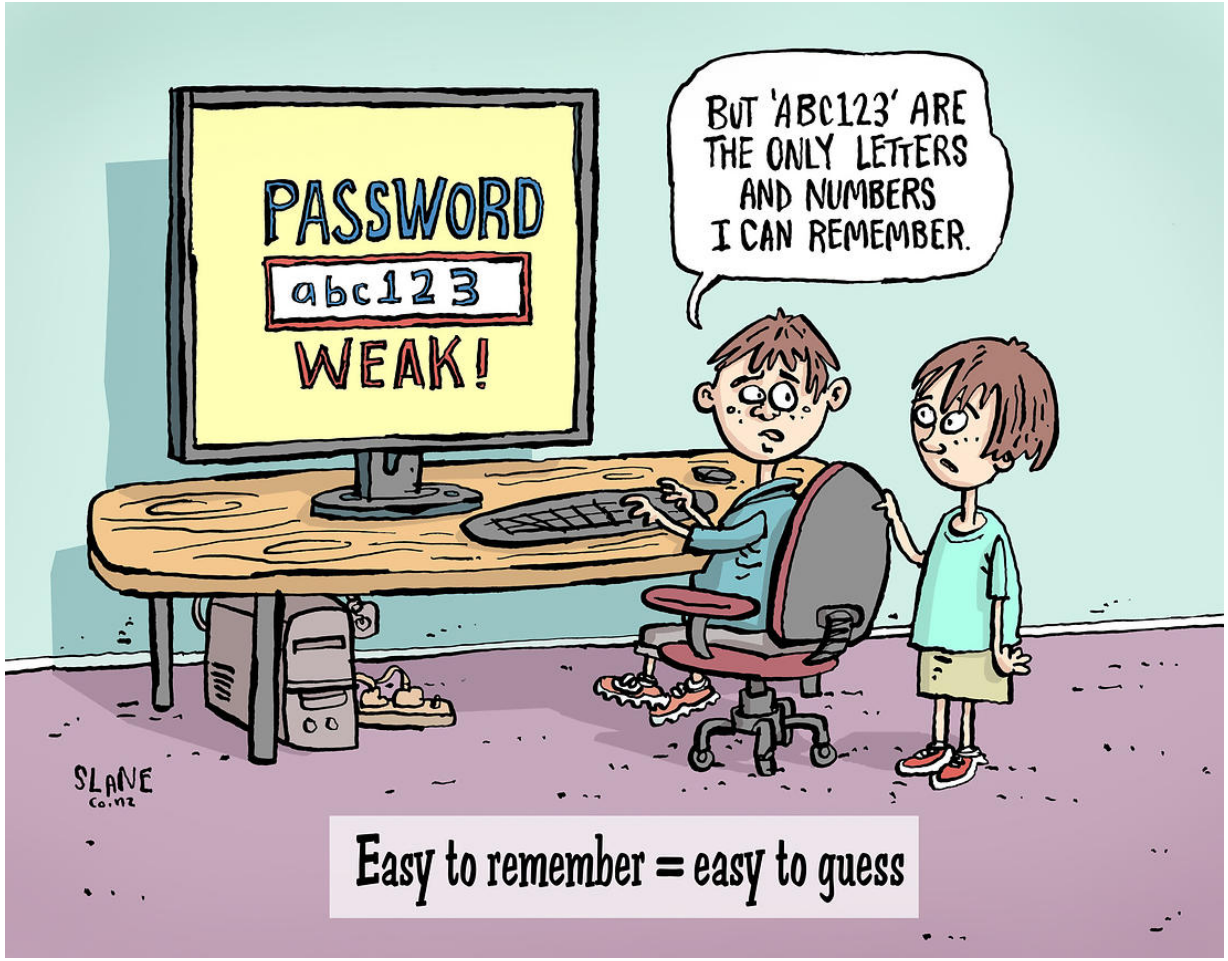
Word/phrase only known by user. User authenticates herself by providing passwords to the server which then verifies that it is the correct one

Password expectation

Roger Buffle Jr. supplies his father with yet another computer password.

Password creation

Password reality



Why passwords?

- Password related issues are identified as one of the top ten security related problems

- Password == often only barrier an attack needs to cross
  - Frequently misused
  - Hard to create and memorize passwords

Most popular passwords of 2020

- 123456
- 123456789
- qwerty
- password
- 1234567
- 12345678
- 12345
- iloveyou
- 111111
- 123123

The problem: Users are not the enemy

- **Users are not the enemy** (Adams and Sasse, 1999)
  - https://discovery.ucl.ac.uk/20247/2/CACM%20FINAL.pdf
  - Studied factors impacting compliance with password policies at 2 organizations
    - Many people wrote their passwords down
    - Struggling to cope with having to frequently change and remember – results in simpler passwords
    - Users don't understand what makes a password secure
  - Part of the problem is users don't know security risks and rationale for security procedures

The method

- Web-based questionnaire
  - Focused on password related behaviors
  - Then 30 semi-structured in-depth interviews
- Analysis technique
  - Grounded theory
  - Build concepts based on data

Problems of passwords

- 1) multiple passwords
  - Hard to remember
- 2) password content
  - Created password based on what they know
- 3) perceived compatibility with work practices
  - Shared password within a team vs. individual passwords
- 4) users' perceptions of organizational security and information sensitivity

Organizational problem

Communication between security departments and users is therefore often restricted to “ticking off” users caught circumventing the rules … Users have to be treated as partners in the endeavor to secure an organization’s systems, not as the enemy within. System security is one of the last areas in IT in which user-centered design and user training are not regarded as essential; this has to change.

A good solution: password managers

Password creation rules

- NIST in 2003 invented rules of how to create *good* passwords
  - letters, numbers, and symbols
  - changing every 90 days

How to enforce it? Strength meters

- Paper: "How does your password measure up? The effect of strength meters on password creation.", Usenix 2012
- RQ
  - What kinds of meters are being used by websites right now?
  - What are “good” measures of password quality?
  - How do different meter designs impact the passwords created? If so, which meters perform best?

RQ 1: What kinds of meters are being used by websites right now?

- How would you do it?

RQ 1: What kinds of meters are being used by websites right now?

- Reviewed login pages of Alexa top 100 most popular websites
  - 96 allowed a login
  - 70 gave some type of password feedback
  - Common types of meters
    - Bar-like (50%)
    - Checkmark or X system (41.3%)
    - Text indicating problems (21.2%)

RQ 2: Good measures of password quality

- How would you solve it?

RQ 2: Good measures of password quality

- Look at earlier scientific literature to *borrow* ideas
- Basic16
  - Password contains >= 16 characters
- Comprehensive8
  - at least eight characters, uppercase letter, lowercase letter, a digit, and a symbol.
  - Not in a wordlist of common passwords

RQ3: How do different meter designs impact the passwords created?

- Online survey study using Amazon Mechanical Turk (AMT)
  - Shown15 different types of password meter
  - 2931 participants

- Study phases
  - Setup a password
  - 2 days later, log in using the original password

Meters tried

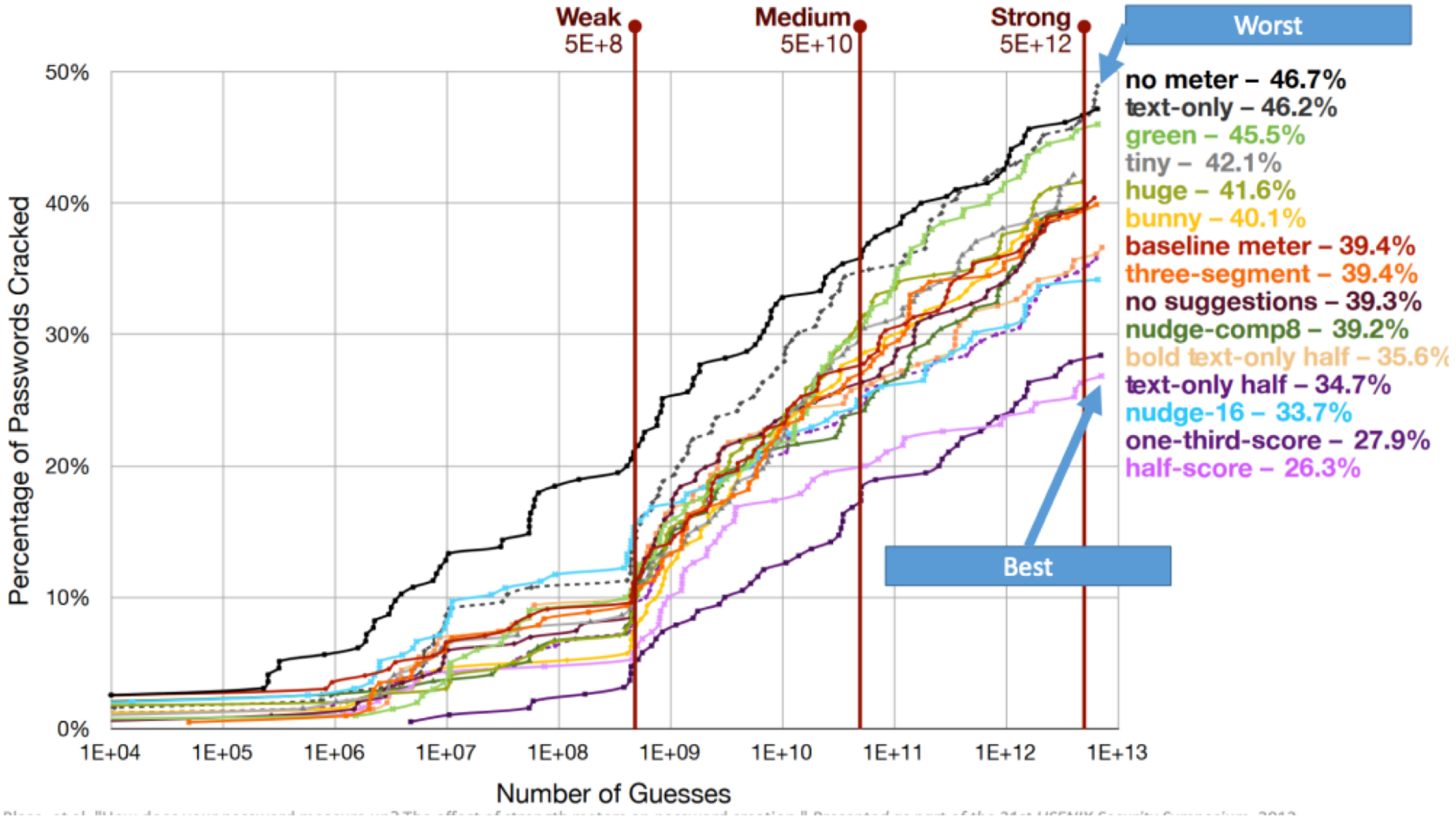
- Control: No meter
- Appearance variations: 3 segment, always green, tiny, huge ..
- Scoring: half-score (always half full), nudge-16, nudge-comp8
- Variation: Running bunny instead of a bar

Anything left in the design?

Anything left in the design?

- What is the attack model?

Results


Weak
5E+8
Medium
5E+10
Strong
5E+12
Worst
Best
no meter – 46.7%
text-only – 46.2%
green – 45.5%
tiny – 42.1%
huge – 41.6%
bunny – 40.1%
baseline meter – 39.4%
three-segment – 39.4%
no suggestions – 39.3%
nudge-comp8 – 39.2%
bold text-only half – 35.6%
text-only half – 34.7%
nudge-16 – 33.7%
one-third-score – 27.9%
half-score – 26.3%
Percentage of Passwords Cracked
50%
40%
30%
20%
10%
0%
1E+04
1E+05
1E+06
1E+07
1E+08
1E+09
1E+10
1E+11
1E+12
1E+13
Number of Guesses

Question

- Is there any shortcoming in the design?
  - Validity point of view?

Two factor authentication

- Something you know
  - Your password

- Something you have
  - Your device

Two factor authentication

- Something you know
  - Your password

- Something you have
  - Your device

Question: Is getting an OTP more secure than passwords?

Question: Is getting an OTP more secure than passwords?

- User friendly
  - Memorable, scalable, physically no/little effort, easy to learn, infrequent errors, easy to recover from fault
- Ease of implementation
  - Accessible, negligible cost per user, server deployable, browser deployable, free
- Protection against
  - Targeted impersonation, throttled guessing, unthrottled guessing

Question: Is getting an OTP more secure than passwords?

- User friendly
  - Memorable, scalable, physically no/little effort, easy to learn, infrequent errors, easy to recover from fault
- Ease of implementation
  - Accessible, negligible cost per user, server deployable, browser deployable, free
- Protection against
  - Targeted impersonation, throttled guessing, unthrottled guessing

Question: Is getting an OTP more secure than passwords?

- User friendly
  - Memorable, scalable, physically no/little effort, easy to learn, infrequent errors, easy to recover from fault
- Ease of implementation
  - Accessible, negligible cost per user, server deployable, browser deployable, free
- Protection against
  - Targeted impersonation, throttled guessing, unthrottled guessing

Roadmap

- Passwords/multi factor authentications
- Usability for security developers
- Online tracking
- Privacy notices/dark patterns
- Temporal aspect of privacy