Better managed than memorized?

Studying the Impact of Managers on Password Strength and Reuse

Sanam Ghorbani Lyastani, Michael Schilling, Sascha Fahl, Michael Backes, and Sven Bugiel

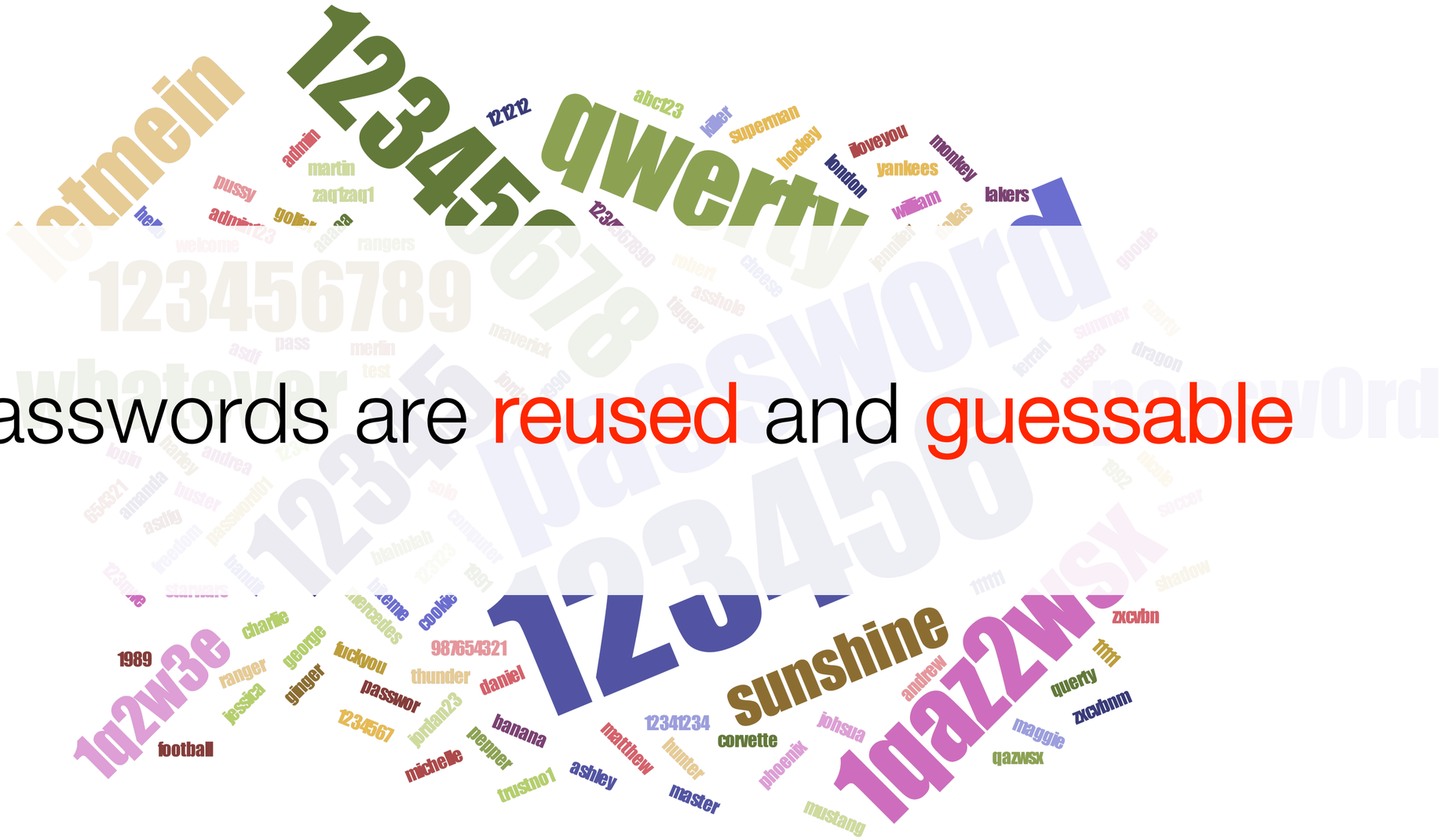
USENIX Security Symposium
Baltimore, August 15th, 2018

UNIVERSITÄT DES SAARLANDES

RUB

CISPA HELMHOLTZ-ZENTRUM i. G.

Where there’s an account there’s a password



Passwords are reused and guessable

Password managers to the rescue!

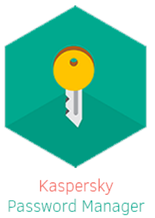




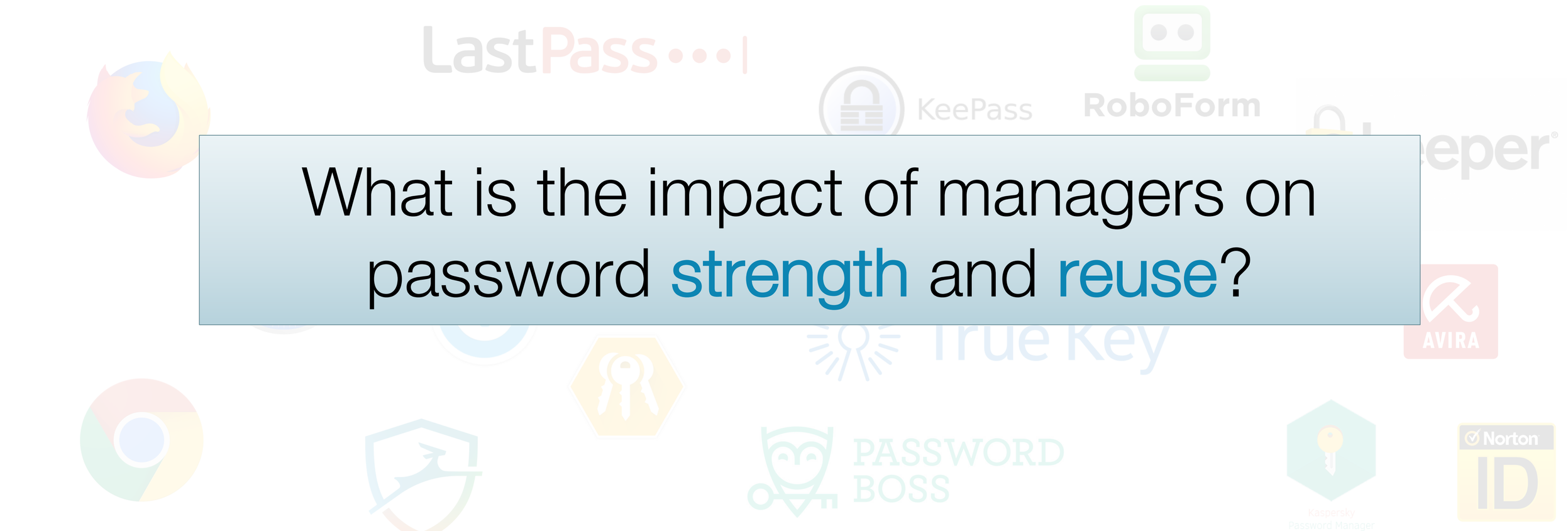






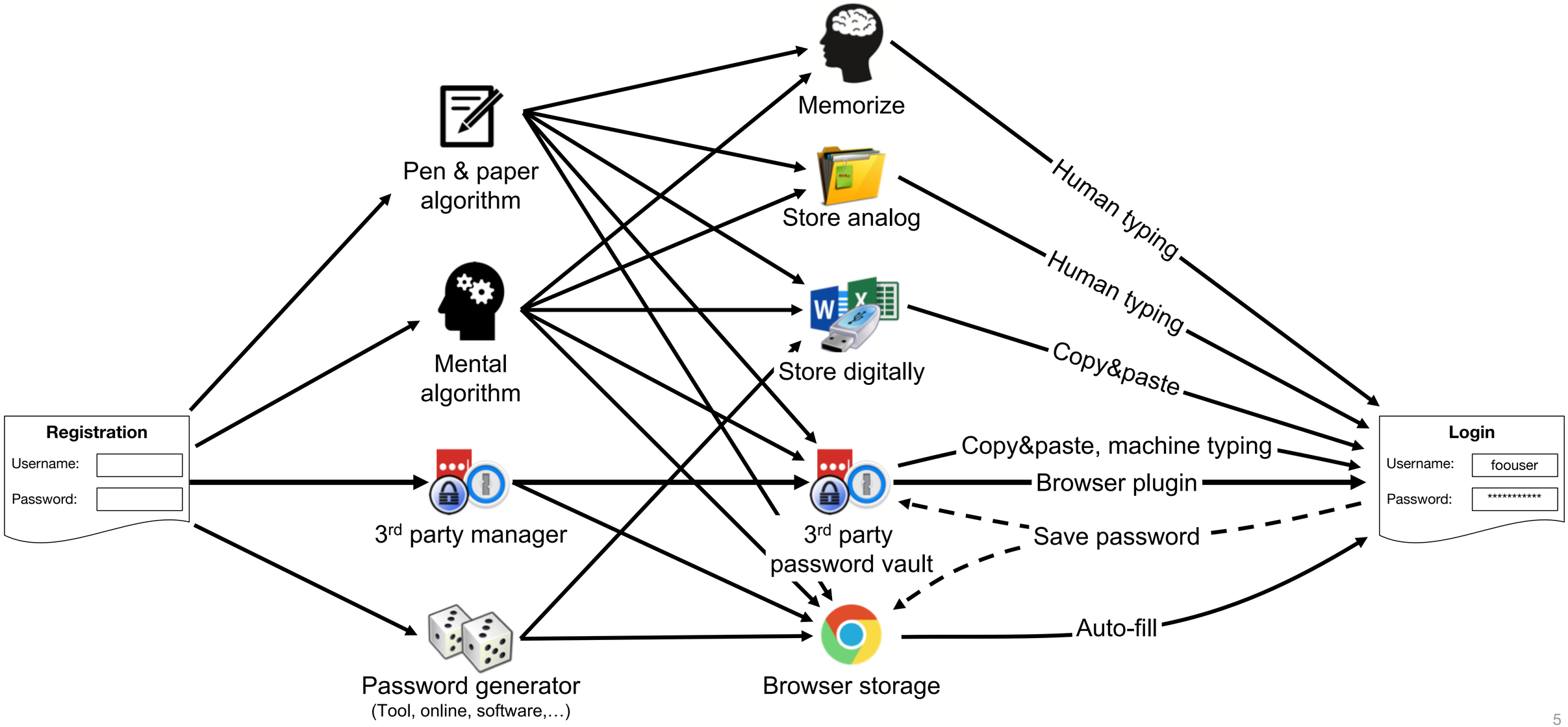




~~Password managers to the rescue!~~ ?

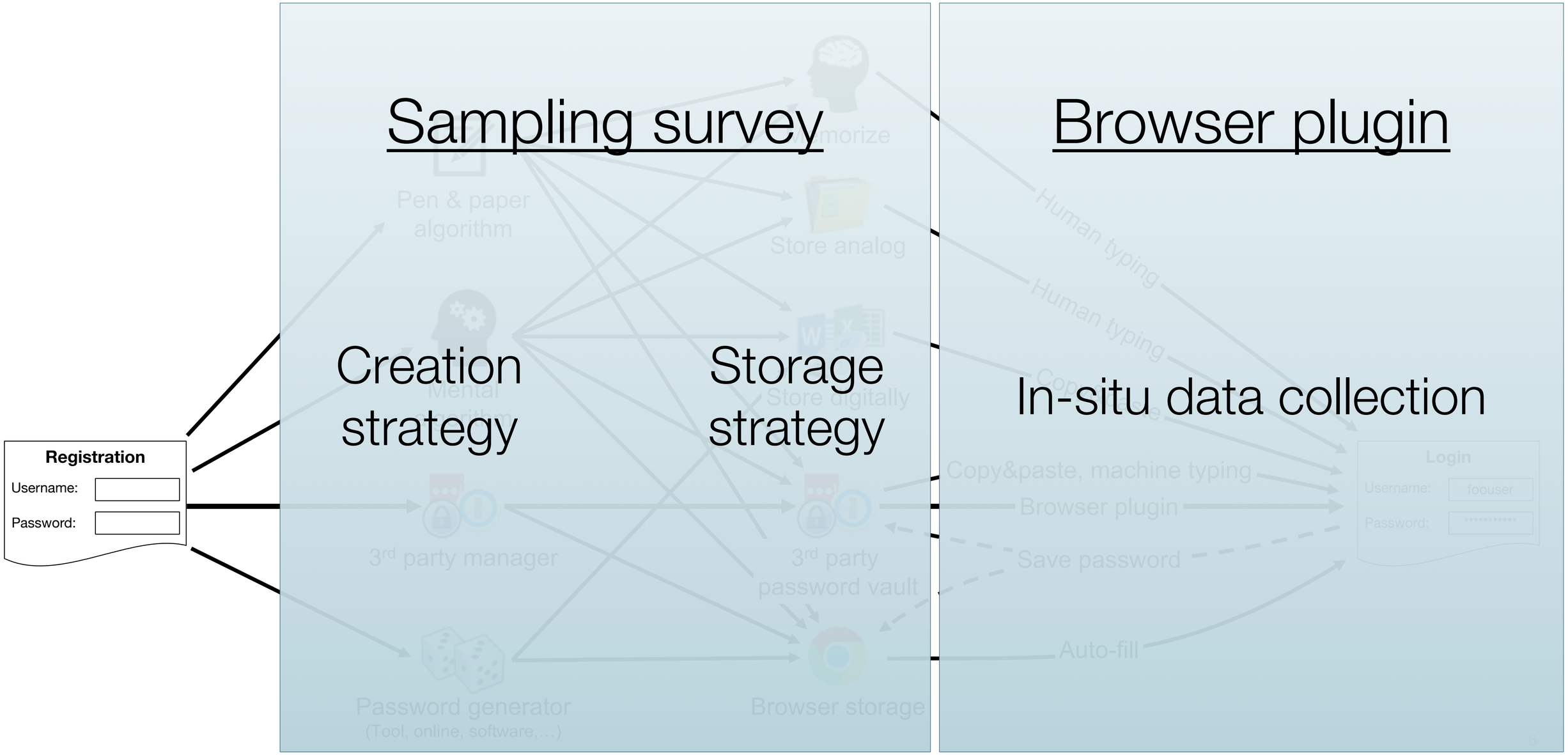


What is the impact of managers on password strength and reuse?

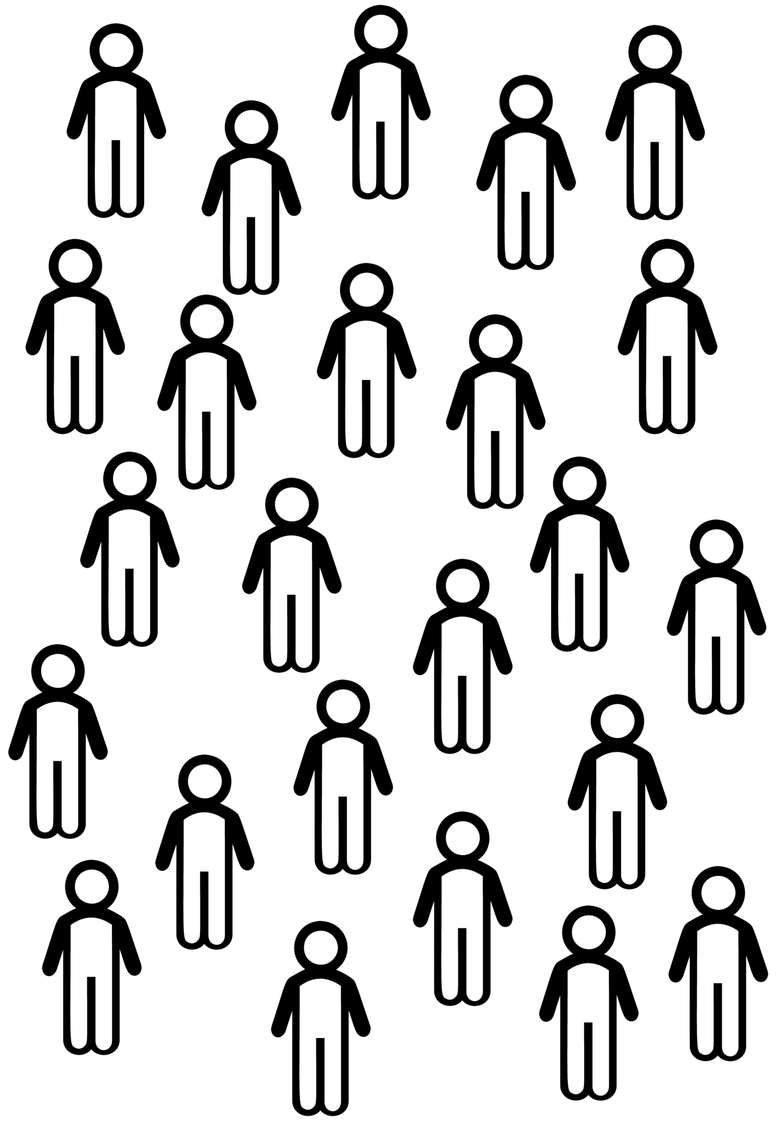
Research Method



Research Method



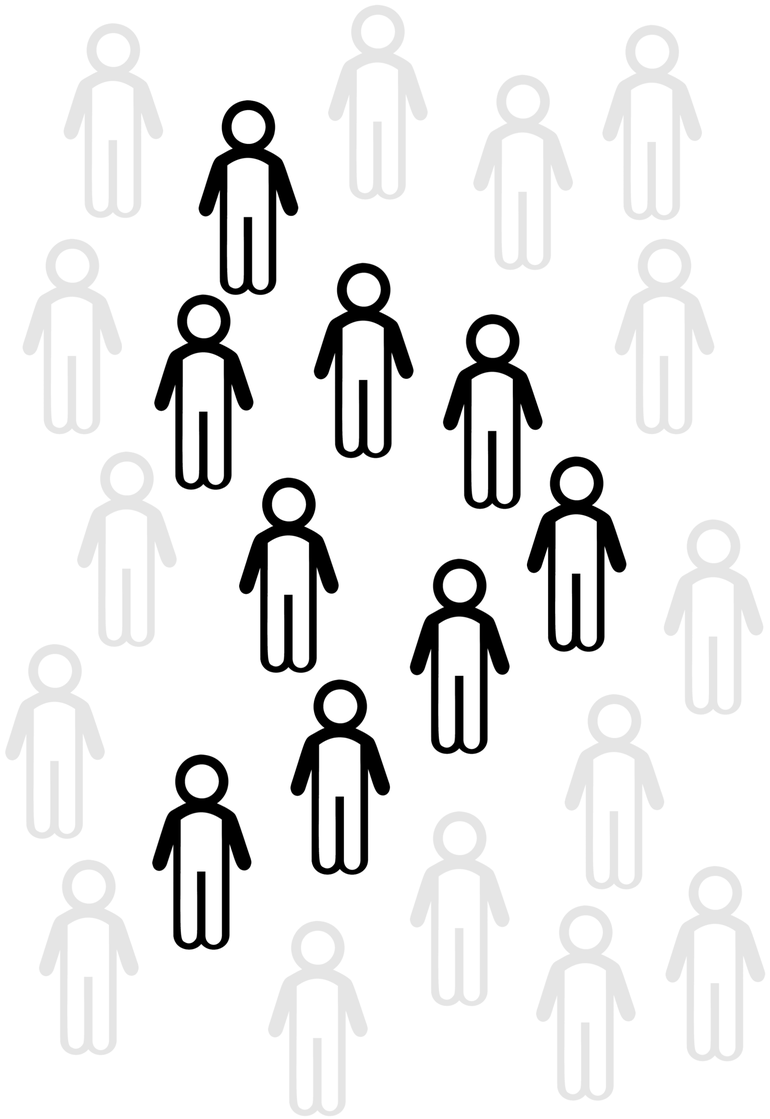
Sampling Survey



Demographics

- 476 participants from Amazon MTurk
- Gender: 57.6% male
- Age: ranges from 18 — ≥71, 75.2% younger than 40
- Education: 44.0% at least bachelor's degree (36.6% bachelor's degree)
- 80.9% use Chrome as primary browser
- Attitude towards passwords: 76.7% believe in importance of passwords
- Prior password leaks: 31.1% experienced password leak (29.0% not aware of)

Browser Plugin Data Collection



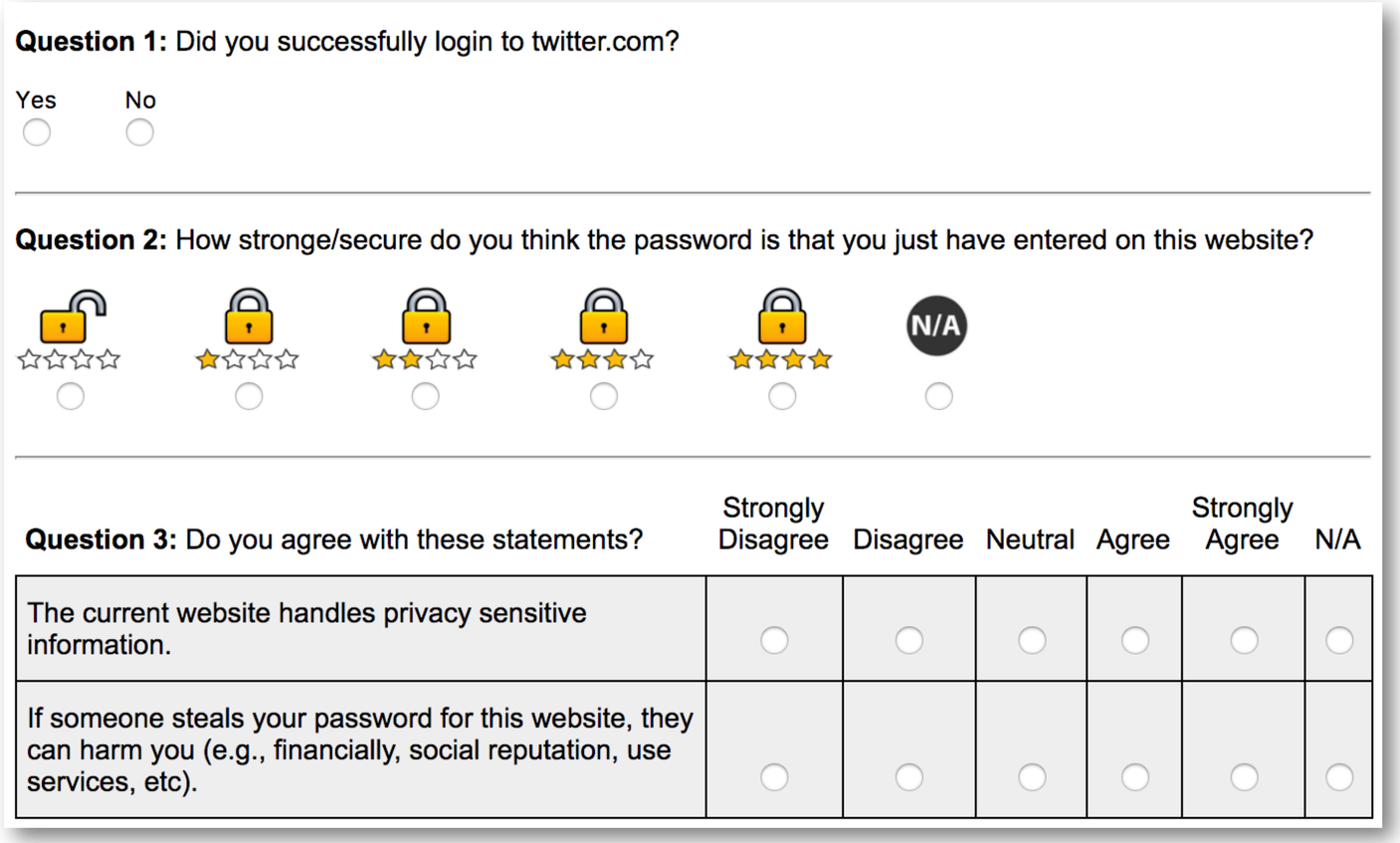
Demographics

- 170 participants completed follow-up study
- No indication of opt-in bias from survey participants

Types of data collected

- Hashes of passwords and 4-character substrings
- Password strength (zxcvbn), length, and composition
- Website category
- Entry method of password
- In-situ questionnaire

In-situ Questionnaire



Question 1: Did you successfully login to twitter.com?

Yes ○ No ○

Question 2: How stronge/secure do you think the password is that you just have entered on this website?

Question 3: Do you agree with these statements?	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	N/A
The current website handles privacy sensitive information.	○	○	○	○	○	○
If someone steals your password for this website, they can harm you (e.g., financially, social reputation, use services, etc).	○	○	○	○	○	○

- Firsthand knowledge about the entered password's value and self-reported strength
- Three-question questionnaire presented to participants one-time on login to a new website

Summary Statistics

- Collected 1,767 passwords (1,045 *unique* passwords)
- Average participant…
  - has 10.39 different accounts
  - has 6.15 distinct passwords
  - reused 70.56% the passwords
    (min: 0% ; max: 100%)

  → underlines rampant password reuse in general

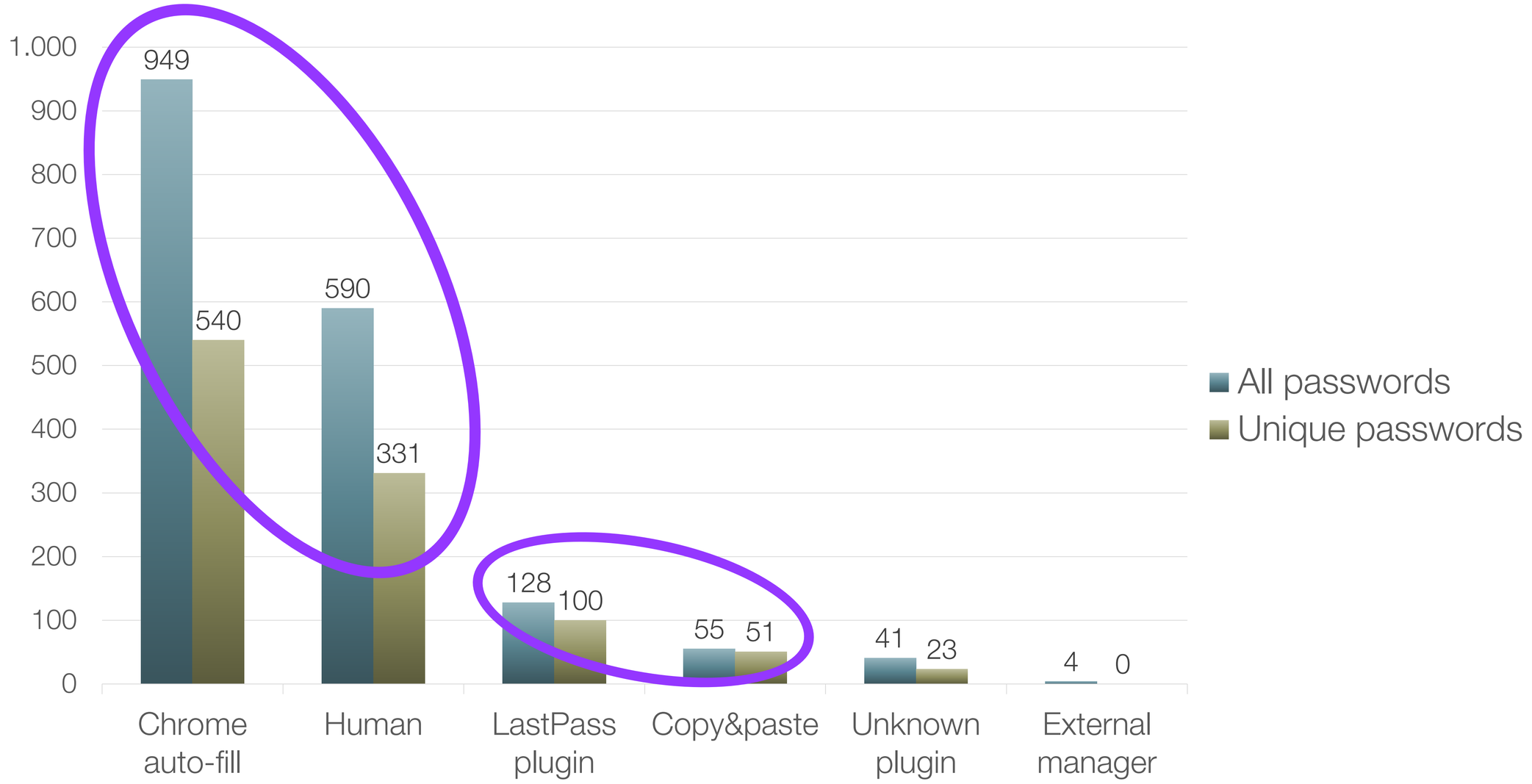
  - has average zxcvbn score of 2.20 (out of 4)
    (min: 0.67 ; max: 4.0)

  → unsatisfying general password strength

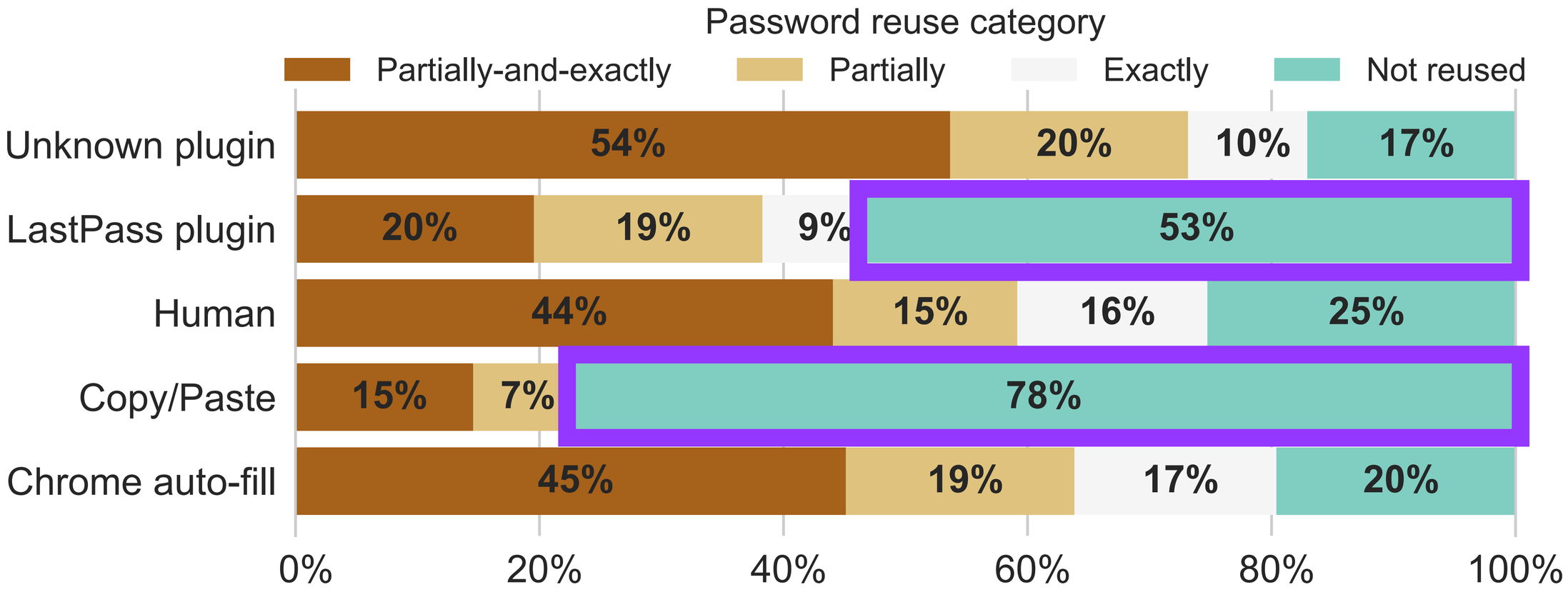
  - entered passwords with 2.24 different entry methods
    (min: 1 ; max: 4)

  → mixed storage strategies

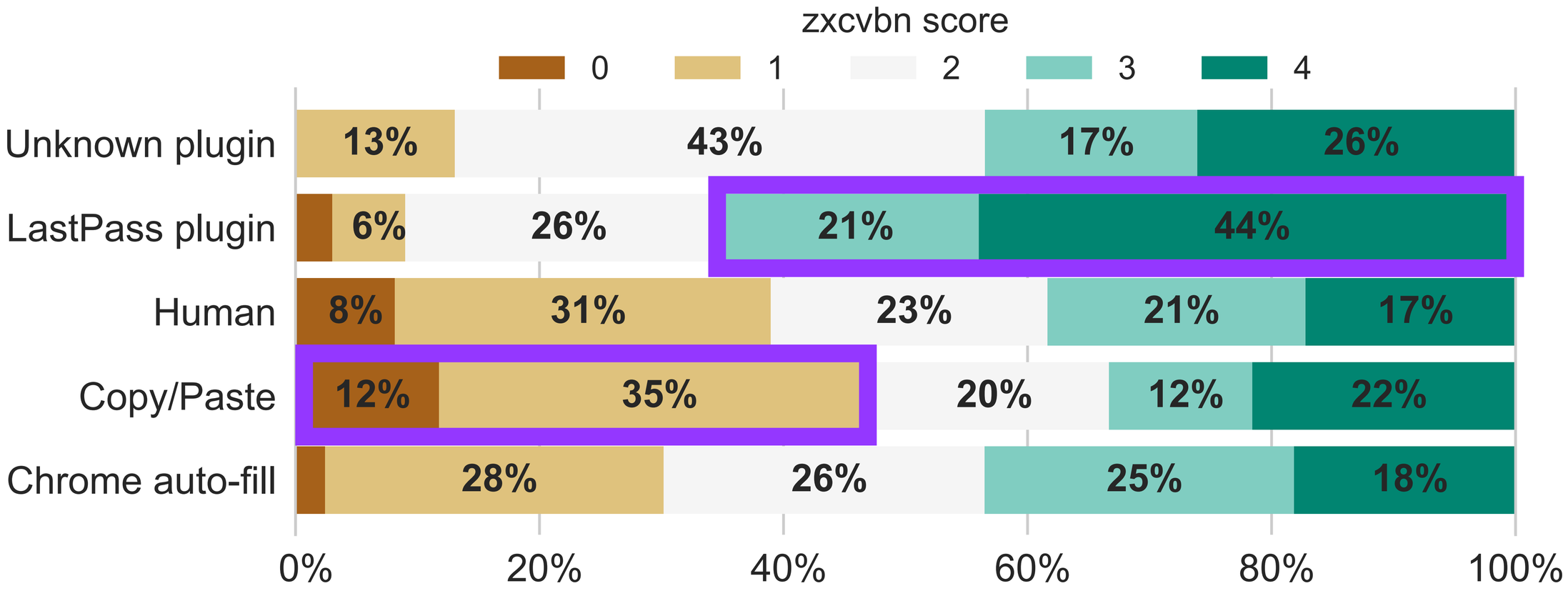
Entry Methods



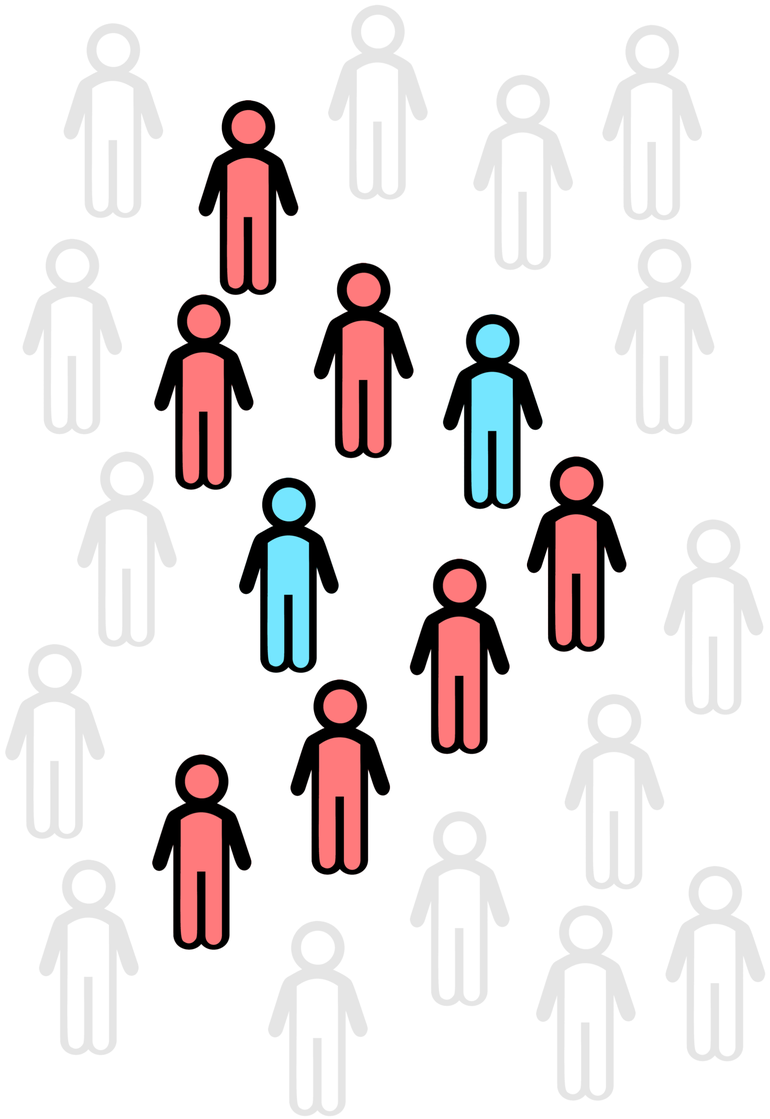
General Password Reuse



General Password Strength



Participant Groups



Grouping based on self-reported creation strategy

Group 1: Password managers
(45 or 26.5%)

“I use lastpass.com, which automatically creates and saves very strong passwords.”

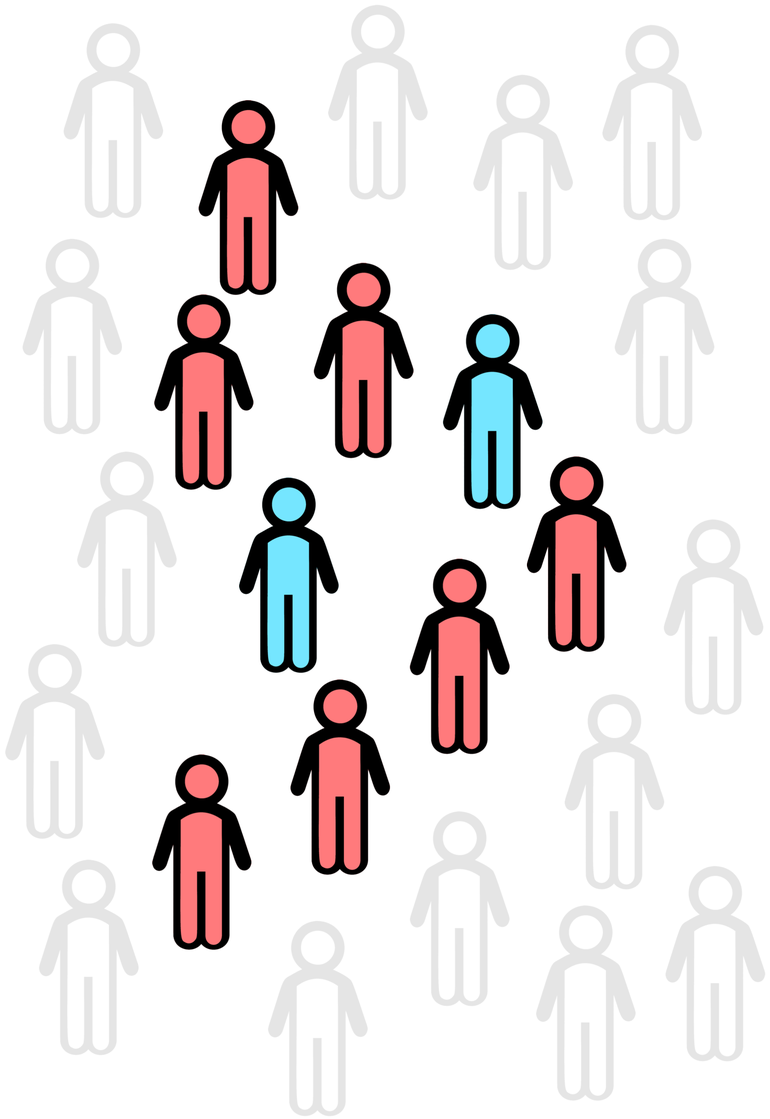
“I use a password creation and storage-related browser extension that also is related to an installed password manager application in my personal computer.”

Group 2: Human-generated
(121 or 71.2%)

“try to come up with a (random) combination of numbers, letters, characters”

“I think of a word I want to use and will remember like. mouse. I then decide to capitalize a letter in it like mOuse. I then add a special character to the word like mOuse@. I then decided a few numbers to add like mOuse@84”

Participant Groups



Grouping based on self-reported creation strategy

Group 1: Password managers
(45 or 26.5%)

Group 2: Human-generated
(121 or 71.2%)

Both groups entered weak and reused passwords

More balanced distribution of password strength

Clear tendency towards weak passwords

High fraction of not-reused passwords

Low fraction of not-reused passwords

Regression Models

- Based on password metrics, answer to in-situ questionnaire, entry method, user variables from sampling survey

- Ordinal multi-level model predicting the zxcvbn score of a password
- Logistic multi-level mode predicting if a password is reused or not

Regression Models — Summary

“Creation strategy is key”

Use of a password generator in combination with Chrome auto-fill, LastPass plugin, and Copy&paste lead to stronger passwords

Use of a password generator reduced chance of password reuse independently of the entry method

Passwords entered with Chrome auto-fill were more likely to be reused independently of creation strategy

Regression Models — Additional Results

“In-situ user reports differ from lab studies”

Self-reported, in-situ password strength was significant predictor for measured password strength
(Participants had a clear view on their entered passwords’ strength)

Better generated and managed ~~than memorized~~?

- Measuring impact of password managers requires a broader view including user strategies and detailed detection of password entry methods
- Users of password generators are closer to a desirable situation, but still far from ideal

Where can we go from here?

- Extend study to walled garden ecosystems (Apple) and mobile domain
- Where do weak and reused passwords in managers come from
  (default passwords, pre-existing, required on devices not managed by the user,…)
- Users of copy&paste strategy warrant further investigation

Questions?