Rewarding Users for Stronger Passwords: Linking Password Lifetime to Strength

Ingolf Becker, Simon Parkin, M. Angela Sasse

University College London

Old Policy

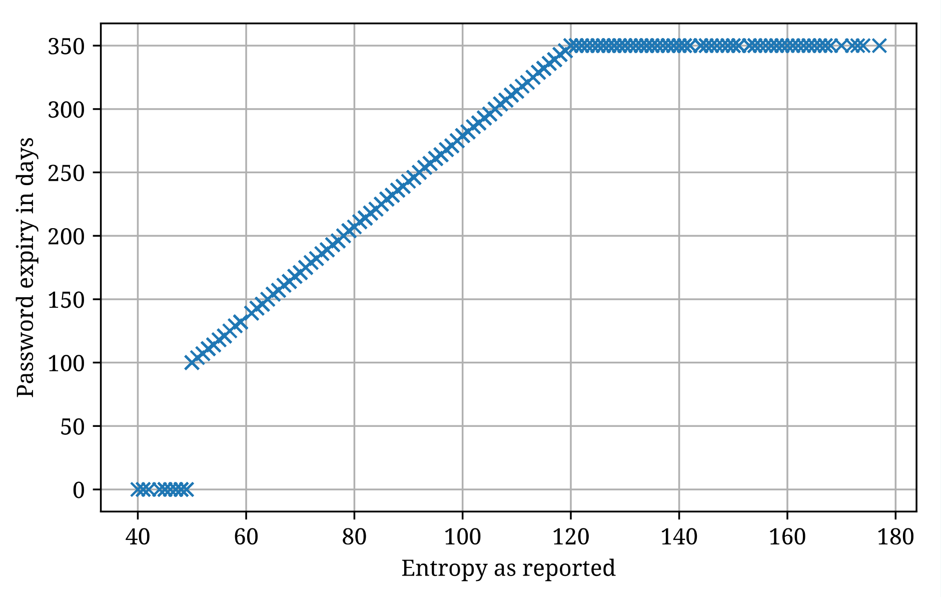
- 150 days fixed expiration
- Exactly 8 characters
- Last 10 passwords are not allowed
- 3 out of:
  - Lowercase character
  - Uppercase character
  - Numbers
  - Symbols

New Policy

- Variable expiration
- 8-30 characters
- Can’t be the same as previous
- 3 out of:
  - Lowercase character
  - Uppercase character
  - Numbers
  - Symbols
- Discount if substring part of a 306k dictionary

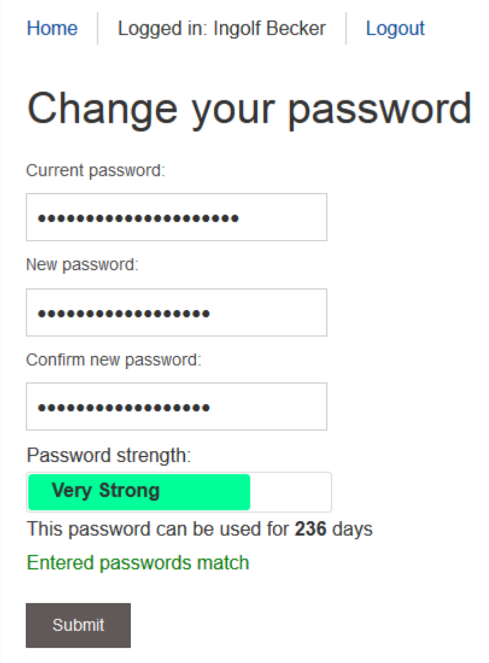
Strength calculation

- Shannon information entropy
  - Not a good measure of guessing resistance (see Weir et al., 2010 and de Carnavalet and Mannan, 2014)
  - But entropy is still widely used!
- 50 bits get you 100 day,
- 120 bits get you 350 days



The environment

- Single Sign On (ish), eduroam, Computer room / library machines
- Large research university
  - 20k undergraduates accounts
  - 30k postgraduate accounts
  - 20k research/admin staff accounts
  - 100k alumni accounts



Change your password

Current password: ••••••••••••••••••••••

New password: •••••••••••••••••••

Confirm new password: •••••••••••••••••••

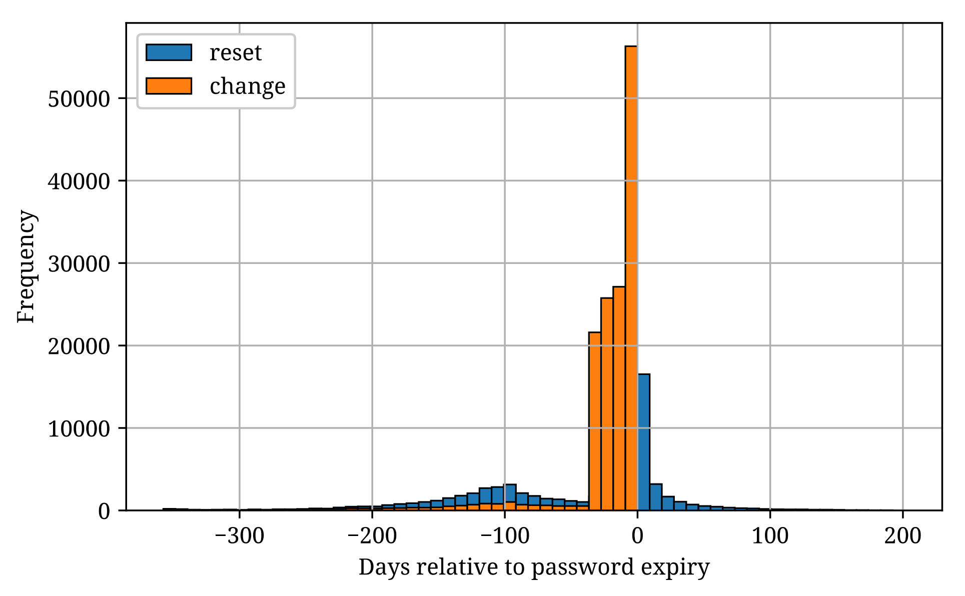
Password strength: Very Strong

This password can be used for **236** days

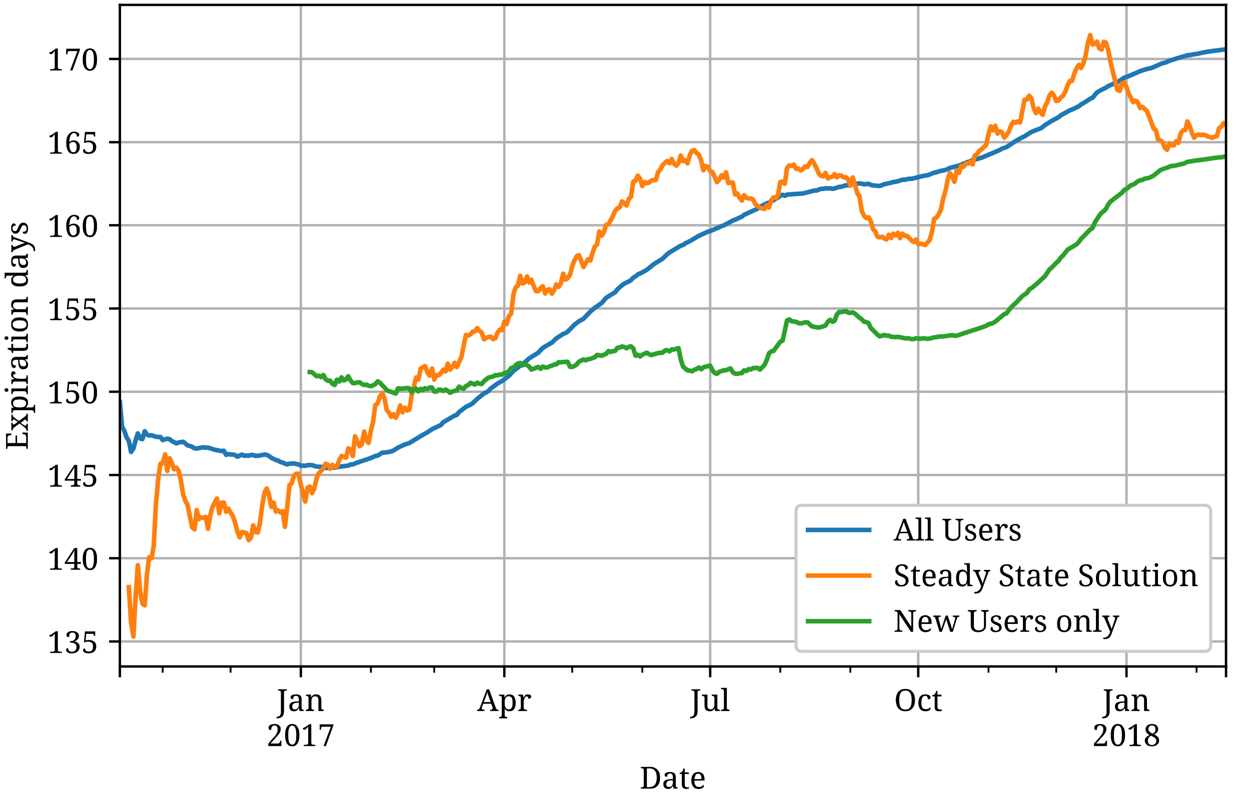
Entered passwords match

The data

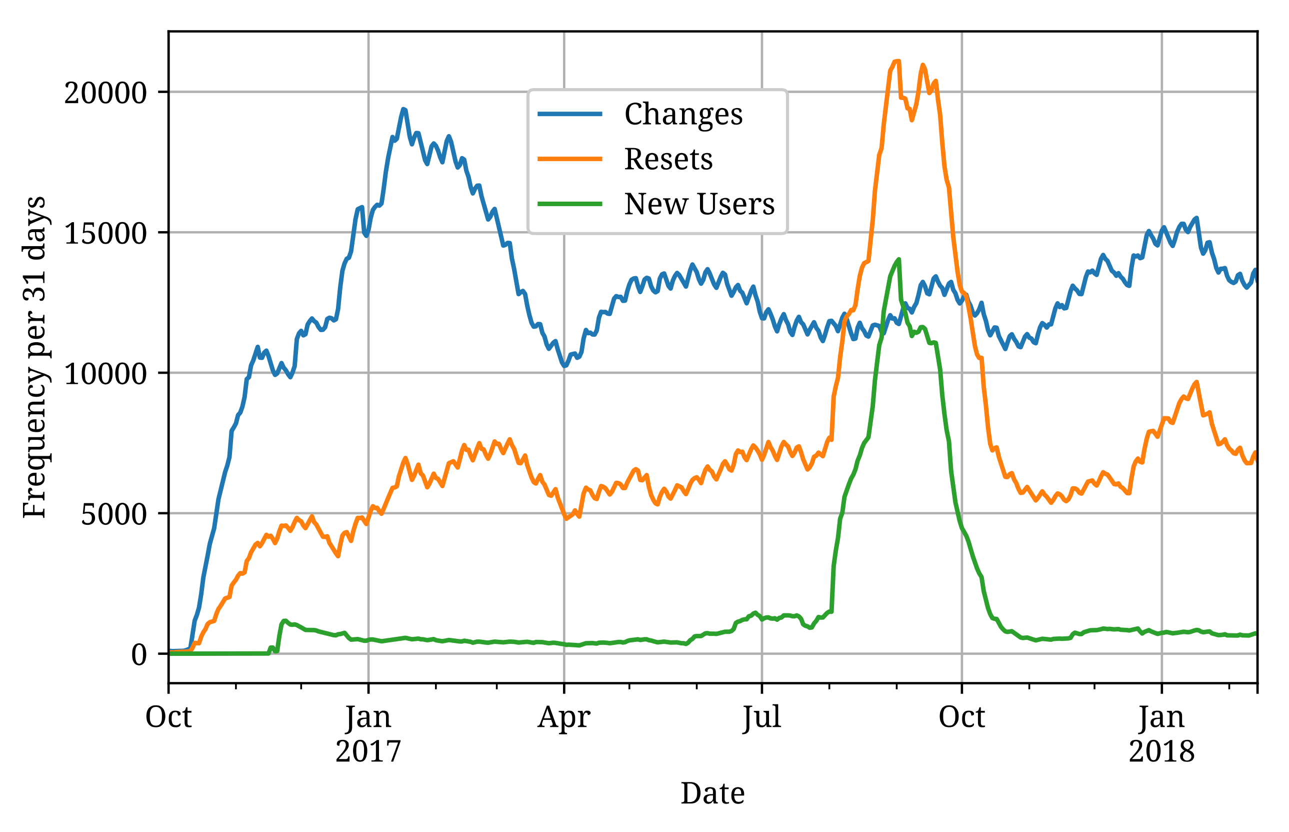
- Pseudo-anonymised log data
- 16 months of data
- 3 million interactions with the password change system
- 200k password changes
- 115k password resets



Password expiration over time for the whole university



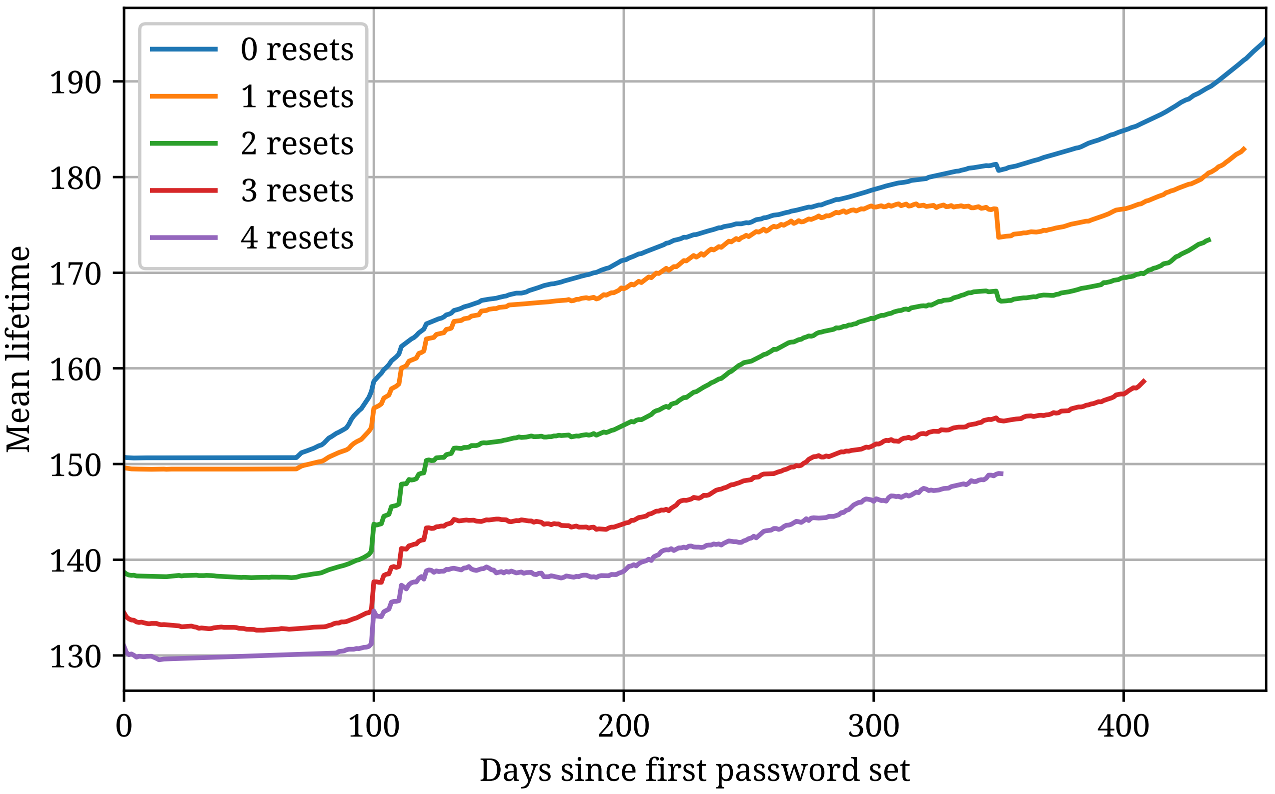
Frequency of changes and resets over time



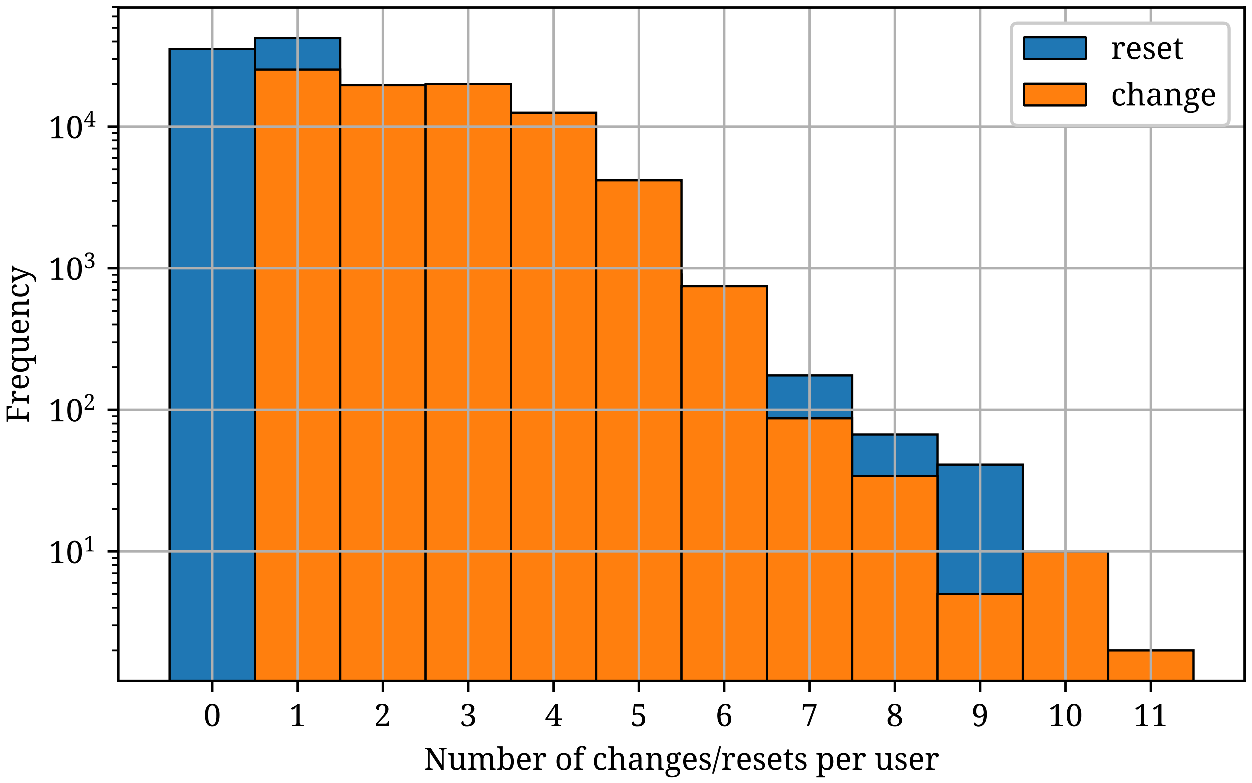
Changes and Resets

- 66% of users had to reset their passwords
- On average, 1.1 resets per user, 2.4 changes per user
- Reasons for resetting:
  - Forgotten password; expired password
- Cost of a reset is significantly higher than a change
  - requires either physical presence at help desk or using a phone-based reset system
- Strong positive correlation between password strength and likelihood of reset before expiration (Spearman's $\rho = 0.95$, $p<10^{-15}$)
  - A user with 300 days lifetime is 4 times as likely to forget their password than a user with a lifetime of 100 days
- The more password resets, the weaker the password choice.

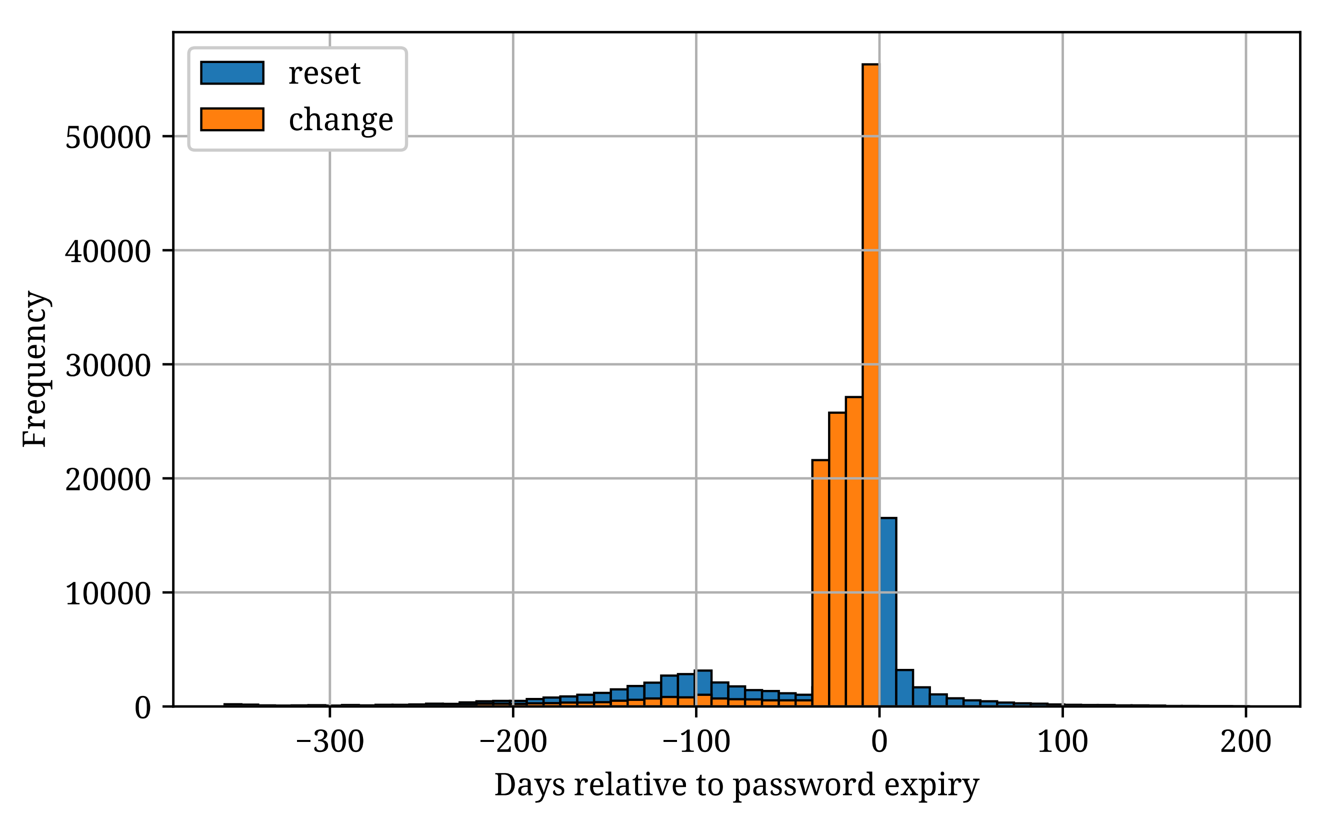
Password lifetime by number of resets

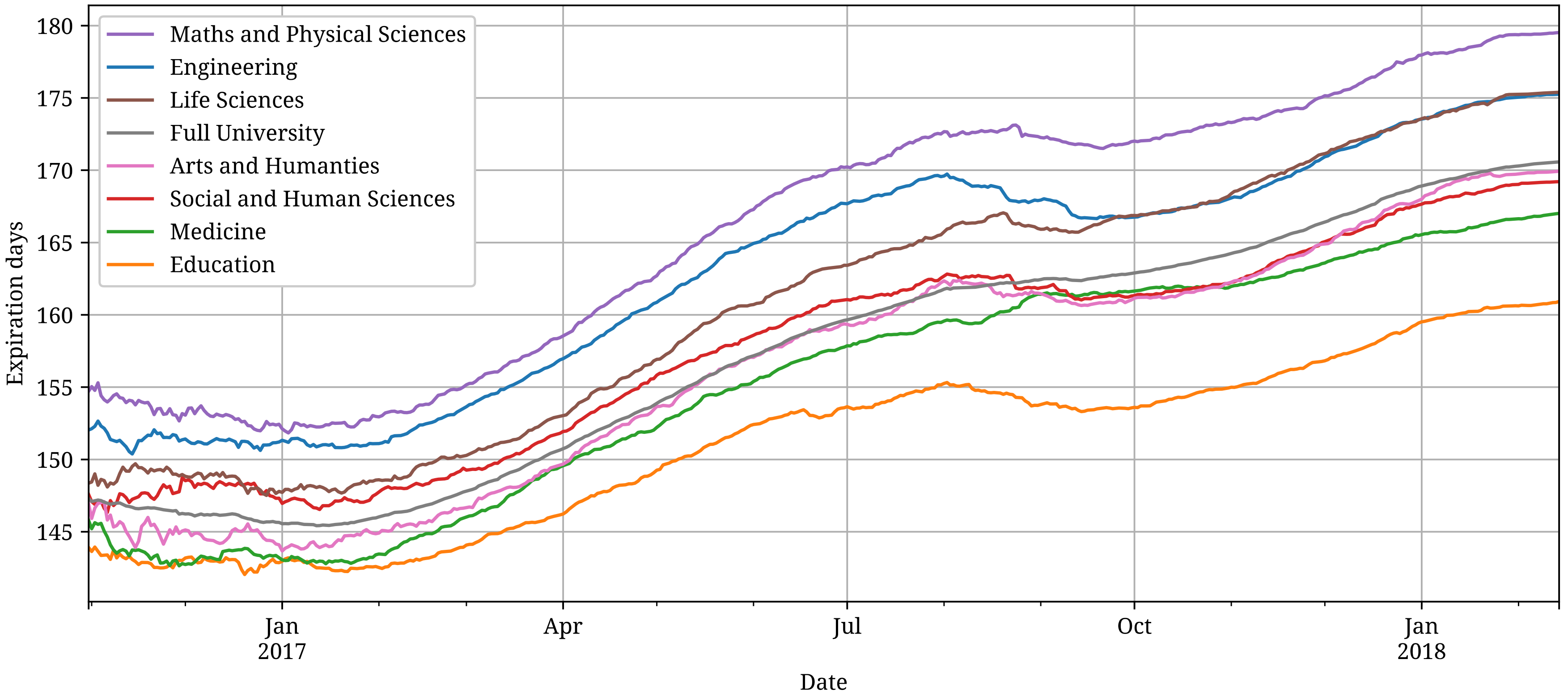


Frequency of changes and resets per user

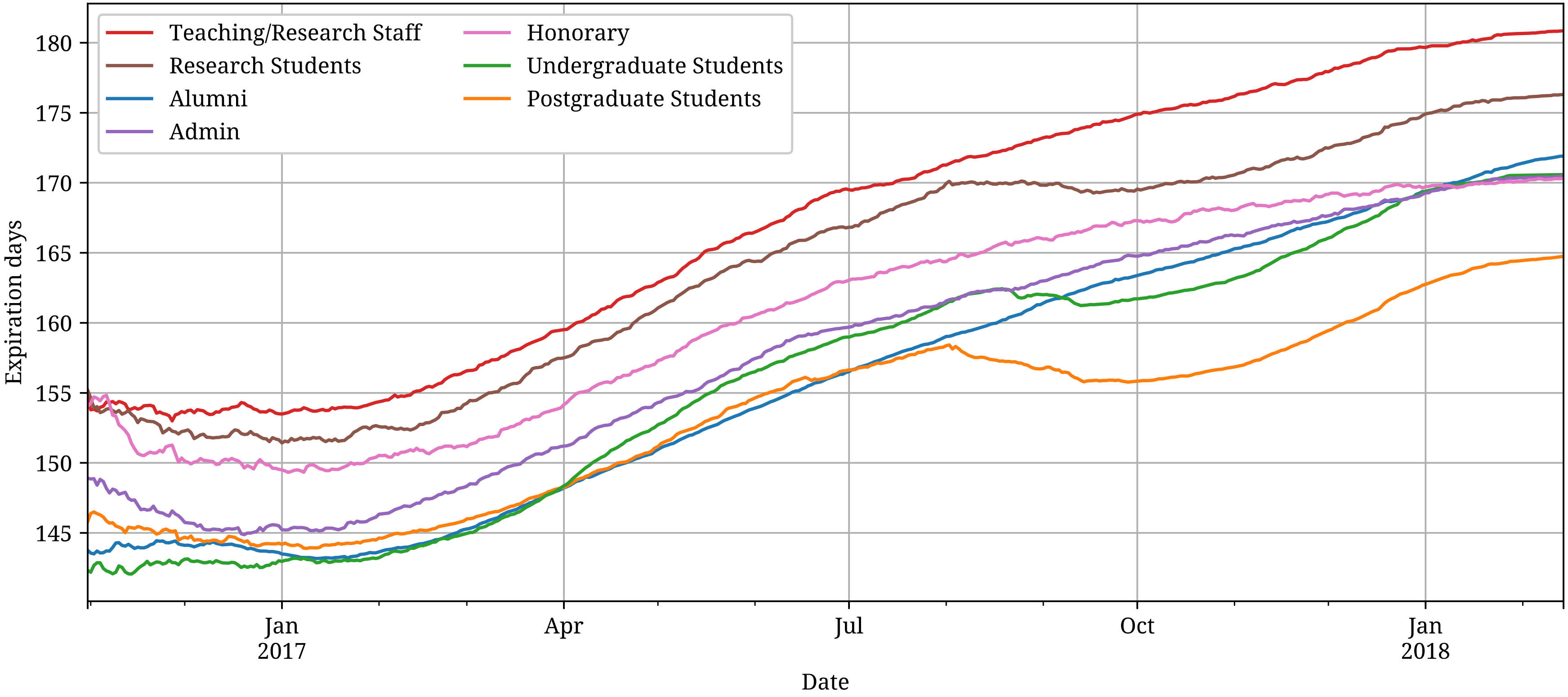


Frequency of password changes relative to password expiration (day 0)




Maths and Physical Sciences
Engineering
Life Sciences
Full University
Arts and Humanties
Social and Human Sciences
Medicine
Education
180
175
170
165
160
155
150
145
Expiration days
Jan
2017
Apr
Jul
Oct
Jan
2018
Date

By Faculty



By Relationship

User feedback

- Qualitative feedback from 93 users in early 2017
- Users:
  - Appreciated the flexibility of the new system
  - If they noticed the change in policy
  - Difficult to create a password that is not “weak”

‘Even though I could remember it wasn’t practically very helpful if you have to put in you know twenty characters. It’s not great. So then I changed it to something that was shorter and last a little less time I just could remember that.’

Discussion

- Intervention clearly successful – users choose stronger passwords
- How long should one measure an intervention?
  - Took a long time to gain traction, still ongoing
- Not a useful intervention:
  - 100 day password is already strong enough to withstand an online attack (10^6 guesses)
  - 350 day password is not strong enough to withstand an offline attack (10^{14} guesses)
    - (Florêncio, Herley and Van Oorschot 2014)
  - Stronger passwords -> higher reset frequency

Conclusions

- Studied a novel password policy:
  ‘Stronger password longer lifetime’
  at a University with 100k users for over 16 months
- Users ‘play the game’: all user groups choose stronger passwords over time
- More than 1 reset / year costs password strength
- Security benefit negligible
  - Maybe dynamic lifetime for online attackable passwords (<10^6 guesses), but no expiration for stronger passwords
- We are continuing to work with our IT services