Lecture 13: Token-Based Authentication

CS 181W

Fall 2022

Recall: Authentication of humans

- Something you know

  secret information (e.g., a password)

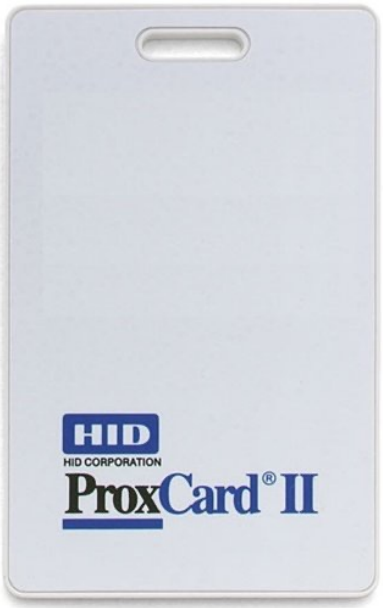
- Something you are

  biometrics (e.g., fingerprints)

- Something you have

  possession of a physical device (e.g., a particular phone)

Authentication tokens

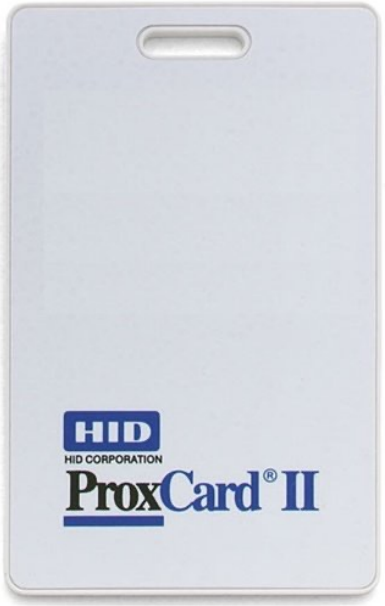


Fixed codes (Keyless Entry)

- Token stores a secret value **`id_T`**
- Lock stores list of authorized ids
- To enter: **`Token->Lock: id_T`**

- **Attack:** replay: thief sits in car nearby, records serial number, programs another token with same number, steals car
- **Attack:** brute force: serial numbers were 16 bits, devices could search through that space in under an hour for a single car (and in a whole parking lot, could unlock some car in under a minute)
- **Attack:** insider: serial numbers typically show up on many forms related to car, so mechanic, DMV, dealer's business office, etc. must be trusted

Fixed codes (RFIDs)



- Token stores a secret value **`id_T`**
- Lock stores list of authorized ids
- To enter: **`Token->Lock: id_T`**

- **Attack:** replay: thief sits nearby, records serial number, programs another token with same number, authenticates
- **Attack:** privacy: adversary tracks token usage across system and learns user attributes and/or behaviors

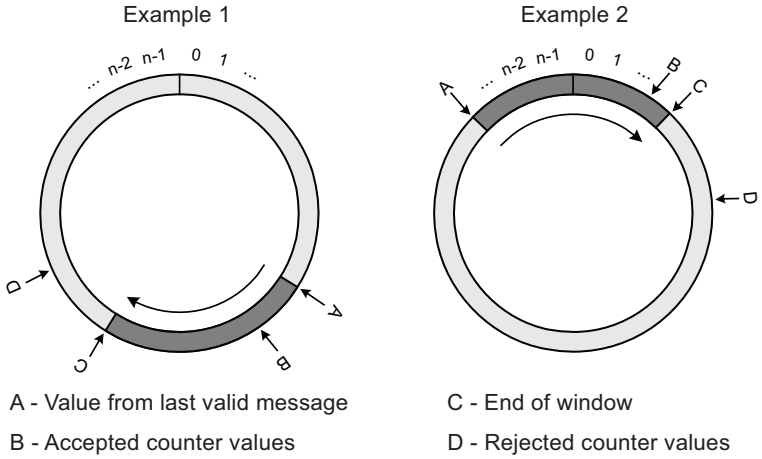
One-Time Passwords

- OTP may be deemed valid only once (the first time)
- Adversary cannot predict future OTPs, even with complete knowledge of what passwords have already been used

“Rolling” codes

- Token stores: **`id_T, sk_T, n`**
- Lock stores info for all authorized ids
- To enter: **`Token->Lock: id_T, Hash(id_T, n, sk_T)`**
- Both Token and Lock increment n after each authentication

- **Problem:** desynchronization of nonce



Hacking Rolling Codes

Honda key fob flaw lets hackers remotely unlock and start cars

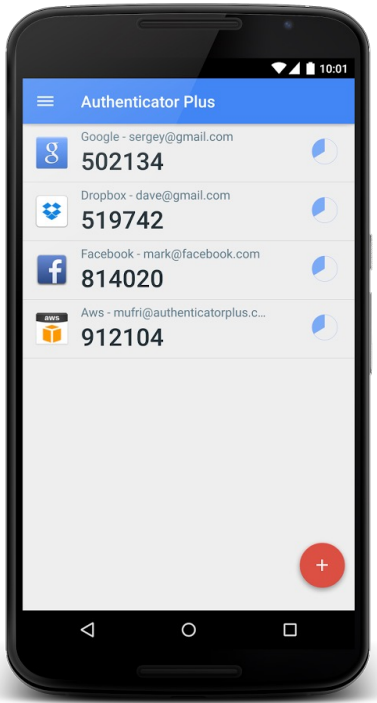
Carly Page @carlypage_ / 7:31 AM PDT • July 12, 2022

Comment

Time-based One-Time Password

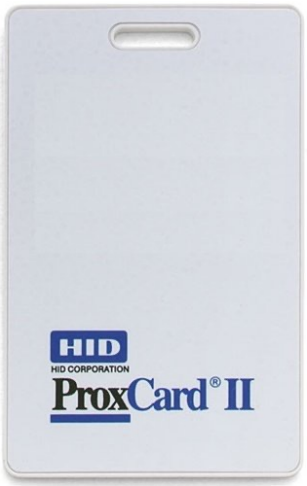
- Token stores: **`id_T, sk_T`**
- Lock stores info for all authorized ids
- To enter: **`Token->Lock: id_T, Hash(id_T, time, sk_T)`**

- 30-60 second valid window



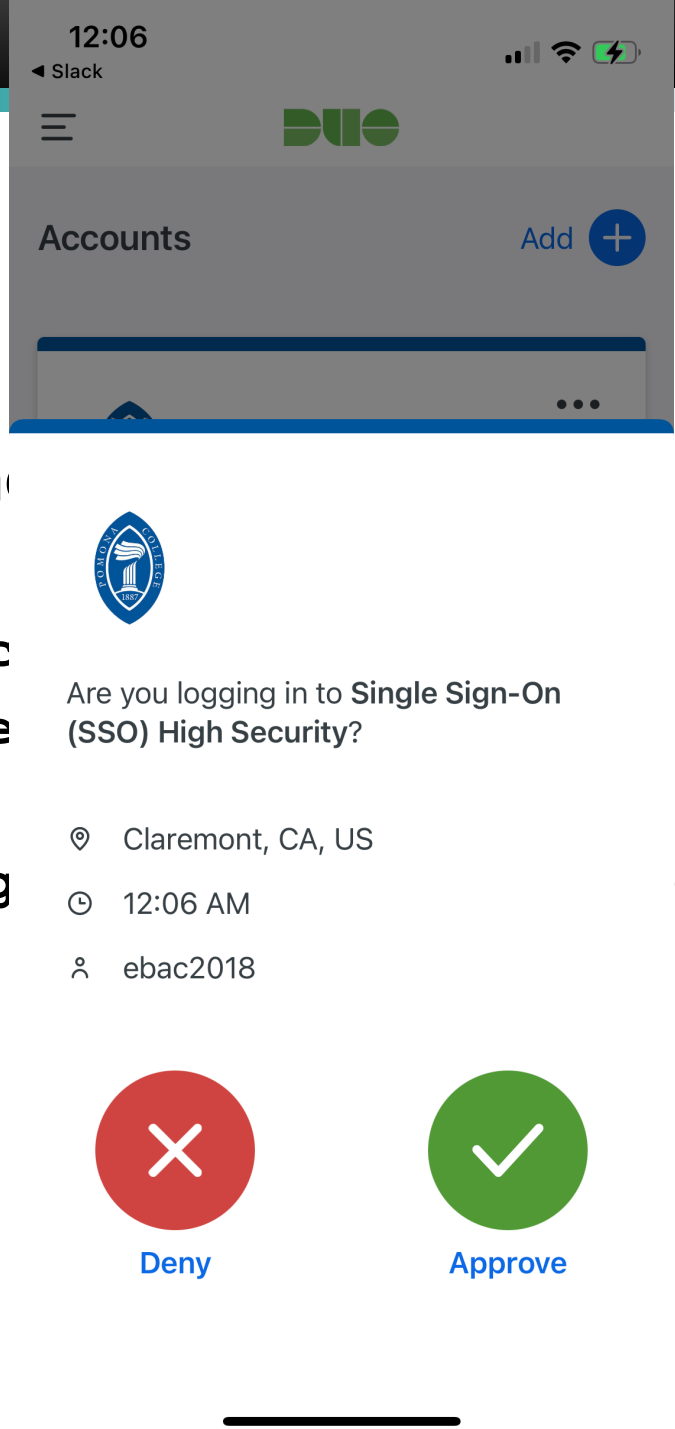
Challenge-based OTPs

- Token stores: **`id_T, sk_T`**
- Lock stores info for all authorized ids
- To enter:
  1. **`Token->Lock: I want to authenticate`**
  2. **`Lock->Token: n (new, randomly chosen number)`**
  3. **`Token->Lock: id_T, Hash(id_T, n, sk_T)`**



Signature-based OTPs

- Token stores: **`id_T, sk_T`**
- Lock stores ids, public keys for all auth
- To enter:
  1. **`User->Lock: I want to authentic`**
  2. **`Lock->Token: auth_details (time`**
  3. **`Token->User: auth_details`**
  4. **`(if yes) Token->Lock: id_T, Sig`**

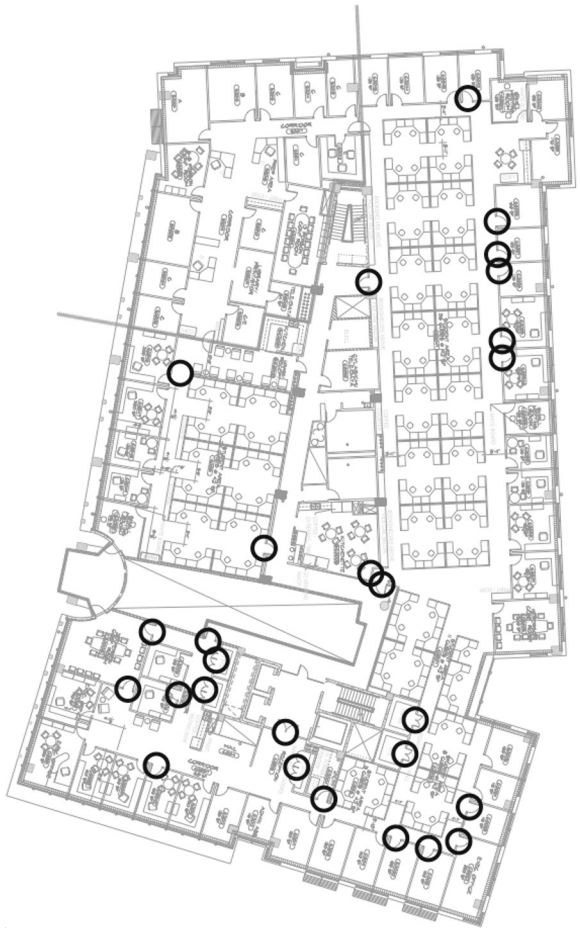


Grey

- Smartphone based access-control system
- Used to open doors in the Carnegie Mellon CIC building
- Allows users to grant access to their doors remotely

Data collection

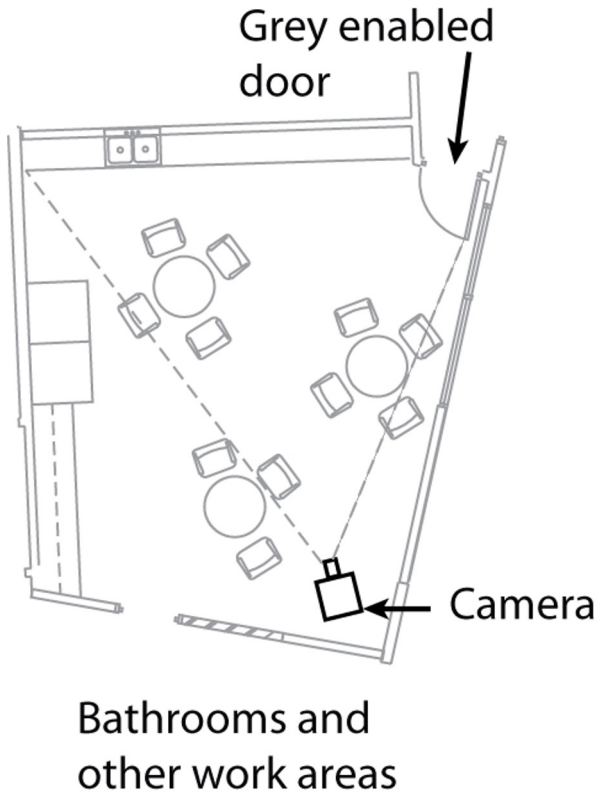
- Year long interview study
- Recorded 30 hours of interviews with Grey users
- System was actively used: 19 users x 12 accesses per week



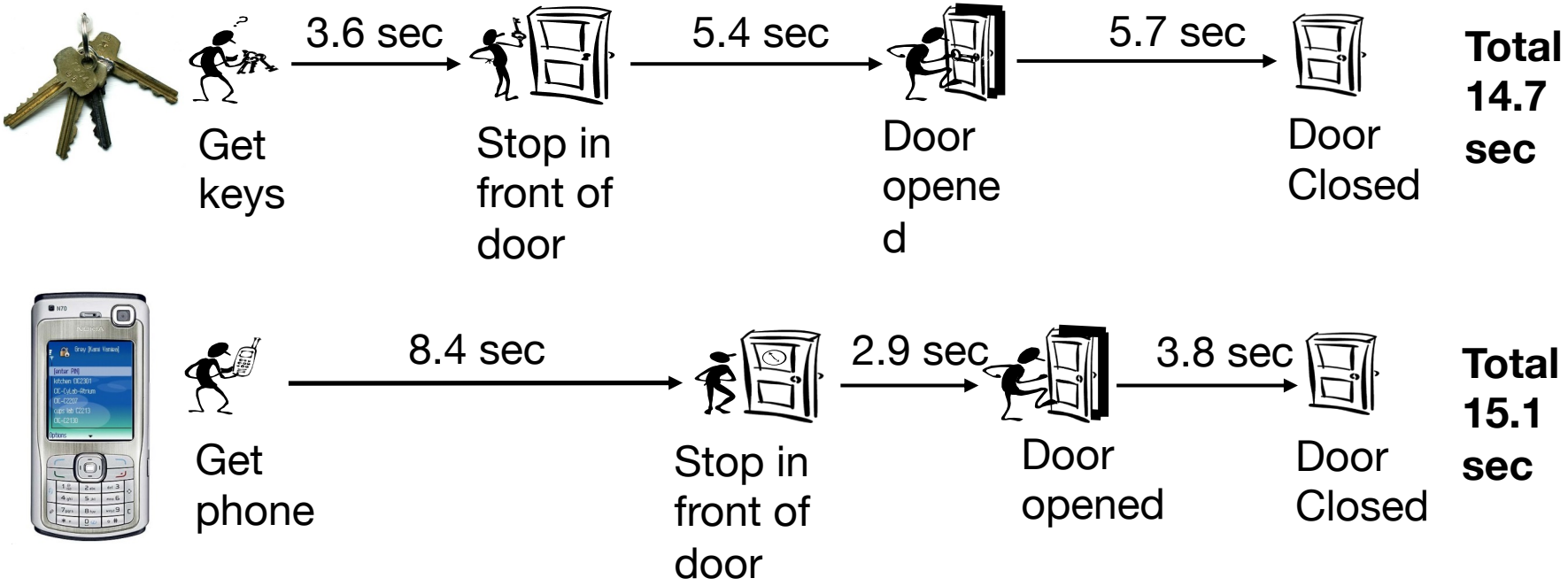
L. Bauer, L. F. Cranor, M. K. Reiter, and K. Vaniea. **Lessons Learned from the Deployment of a Smartphone-Based Access-Control System.** SOUPS 2007. http://cups.cs.cmu.edu/soups/2007/proceedings/p64_bauer.pdf

Users complained about speed

- Users said Grey was slow
- But Grey was as fast as keys
- Videotaped a door to better understand how doors are opened differently with Grey and keys



Similar average access times



“I find myself standing outside and everybody inside is looking at me standing outside while I am trying to futz with my phone and open the stupid door.”

Nobody wants to have to reboot their door

Unanticipated uses can bolster acceptance

Convenience always wins

Comparing 2FA Methods

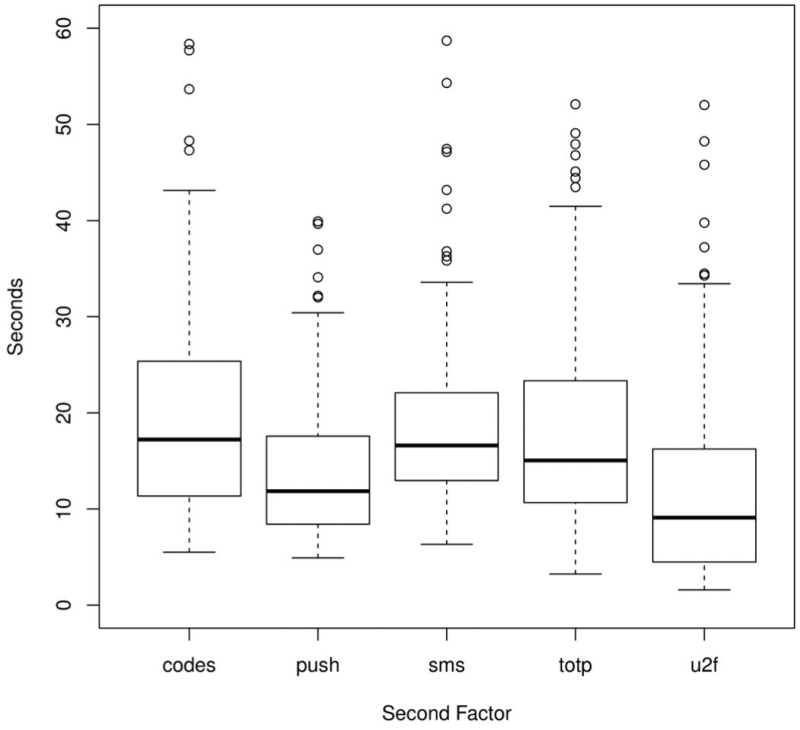
- SMS code
- TOTP (Google Auth)
- pre-generated codes
- Duo Push
- U2F security keys

In person/Remote study
Between subjects
n=72

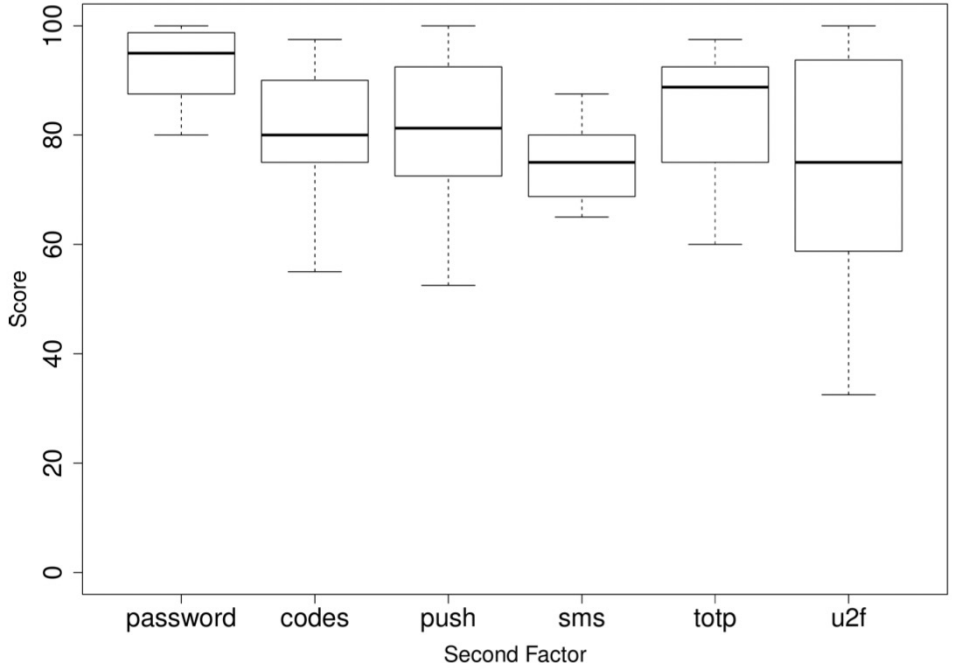
Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. **A Usability Study of Five Two-Factor Authentication Methods.** SOUPS 2019.
https://www.usenix.org/system/files/soups2019-reese.pdf

Comparing 2FA Methods

Time to Login



Usability Score (SUS)



Comparing 2FA Methods

“In my opinion, it may be a little obsessive for everything, but for banking it’s something that I actually do want some authentication. I almost wish that it was a requirement"

“I guess maybe because it’s that I don’t have anything to protect. . . I’m at a stage in my life where nothing I own is that valuable"

“Honestly, once I’m home I kind of just set my phone down and forget where I put it sometimes, so that was a little bit hard ...I needed to go find my phone and pull up the app.”

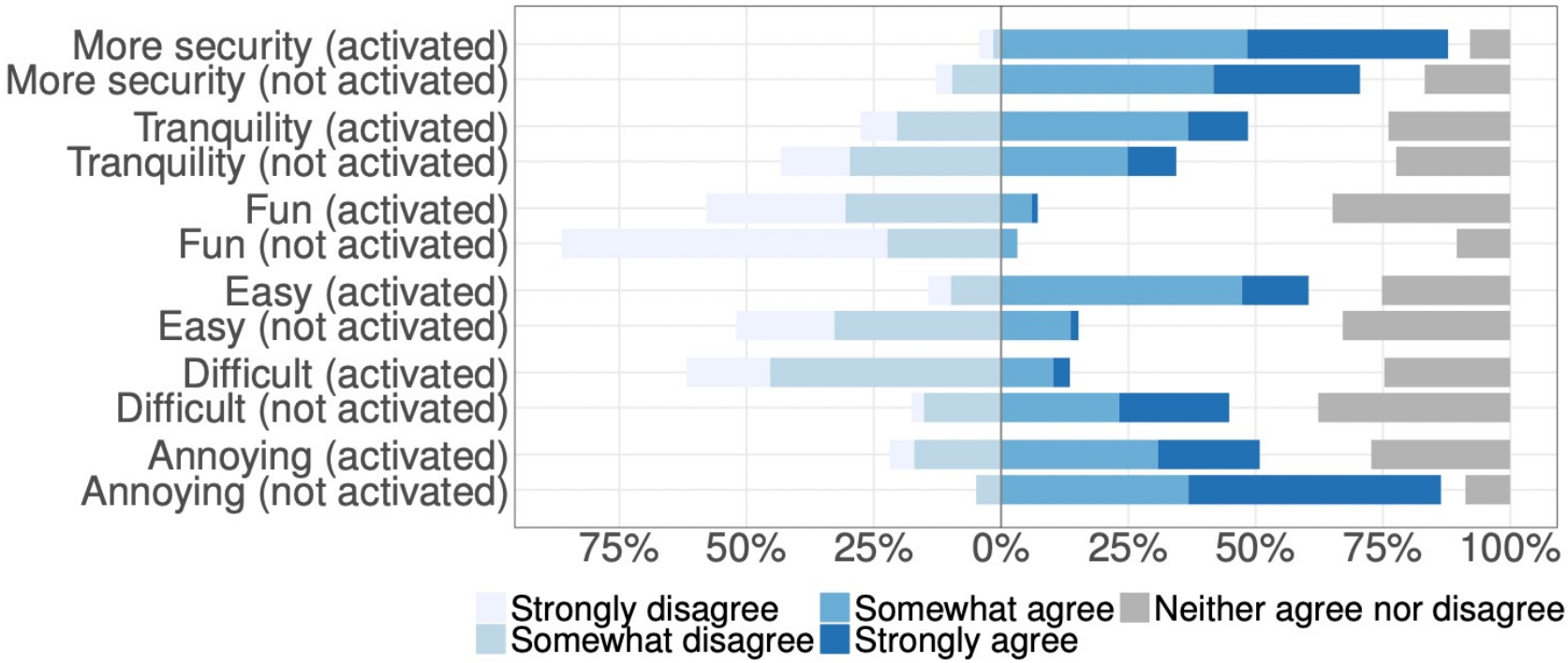
[about TOTP] “I have to type in these numbers so fast or else it’s going to go away.”

Observing 2FA in the wild

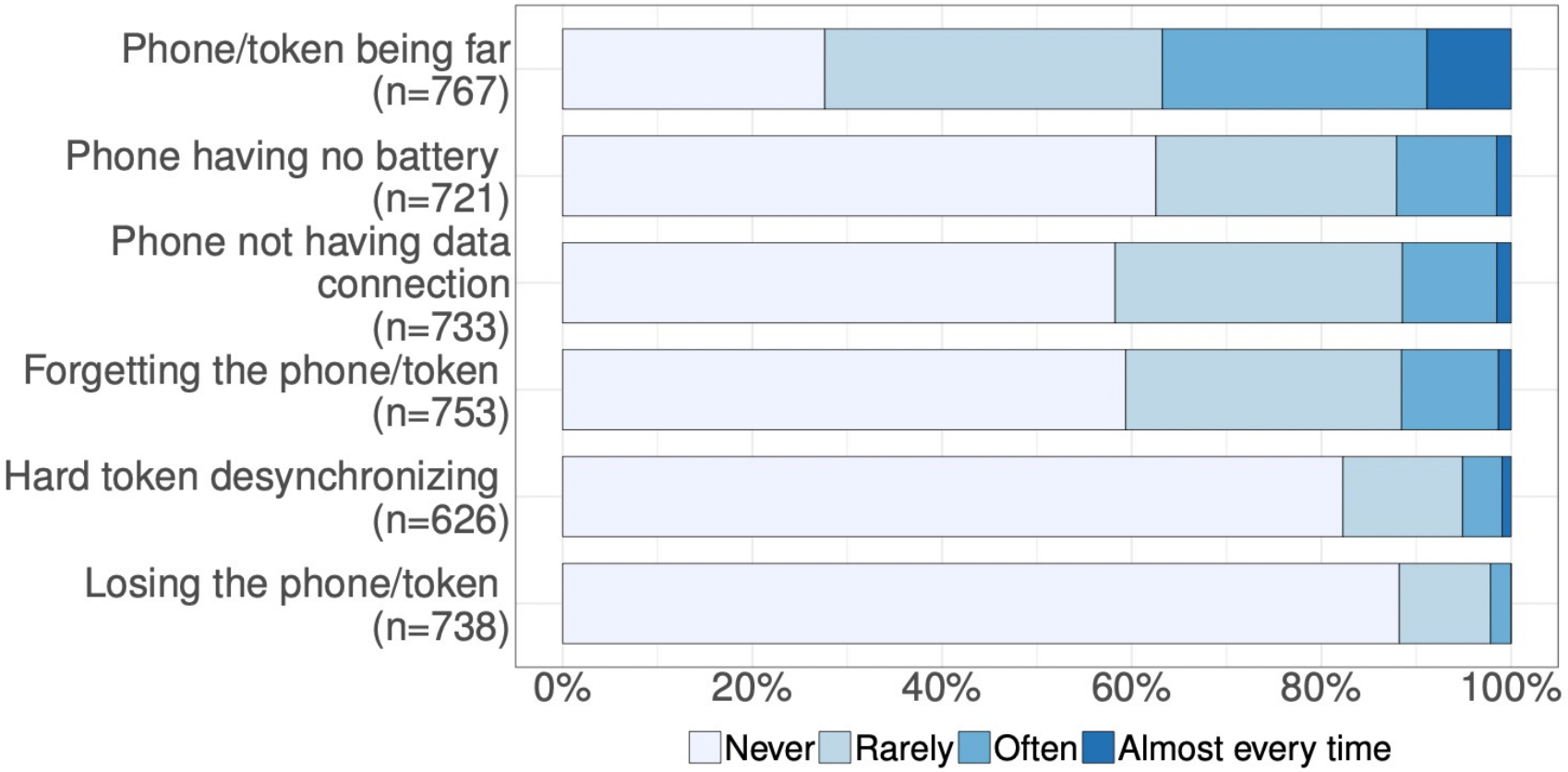
- Log records containing over over one million authentication attempts from over 13,000 users between September 2016 - July 2017
- Survey 1-3 weeks before mandatory (n = 1,251)
- Survey 3 months after mandatory (n = 796)

Jessica Colnago, Summer Devlin*, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, Nicolas Christin. "It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University. CHI 2018.

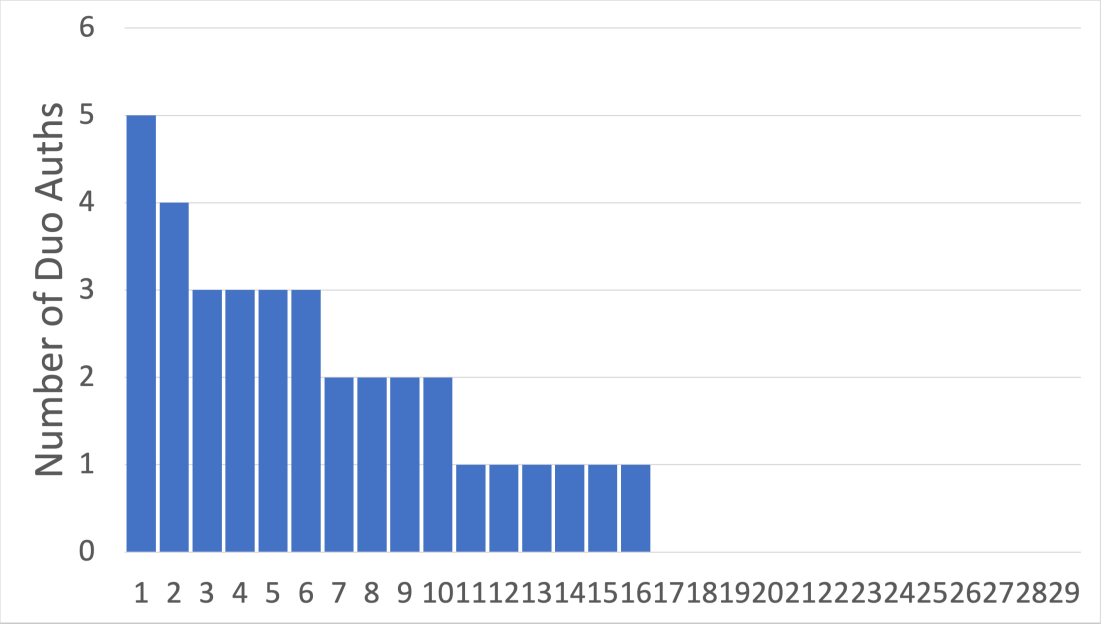
Observing 2FA in the wild



Observing 2FA in the wild



Our Diary Study



Most common:

- Sakai (15)
- VPN (6)
- Others (course sites, zoom, college portal, etc)

- 1 failed (Sakai down)

Remote/online
Diary study
n = 29

Token-based Authentication