Passwords and Tokens and Humans, Oh My!

Usability and user acceptance of FIDO U2F tokens

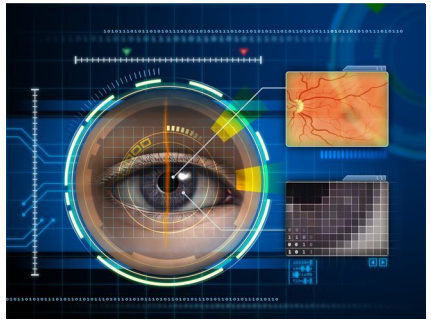
Topics

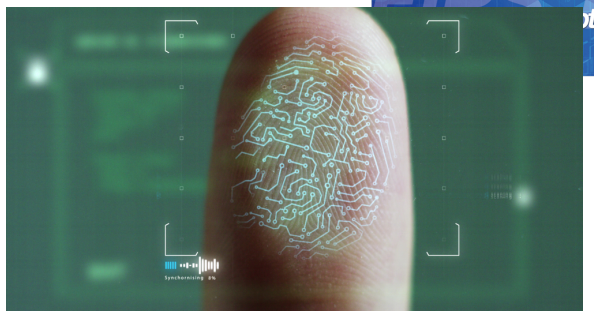
- **Motivation**
- **Background**
  - Authentication factors
  - Token types
- **Our Study**
  - Methods
  - Findings
- **Future Work**

Motivation

- **Passwords stink**
  - Hard to remember
  - Hard to type
  - Easy to guess
  - Easy to steal
  - Easy to share
  - Etc., etc.
- **We still use them**

Motivation (2)





- **Alternatives exist**
  - Biometrics
  - One-time passwords
  - Preference profiles
  - Plenty of weirder ideas
- **Not widely used**
  - Why?

Background: Authentication Factors

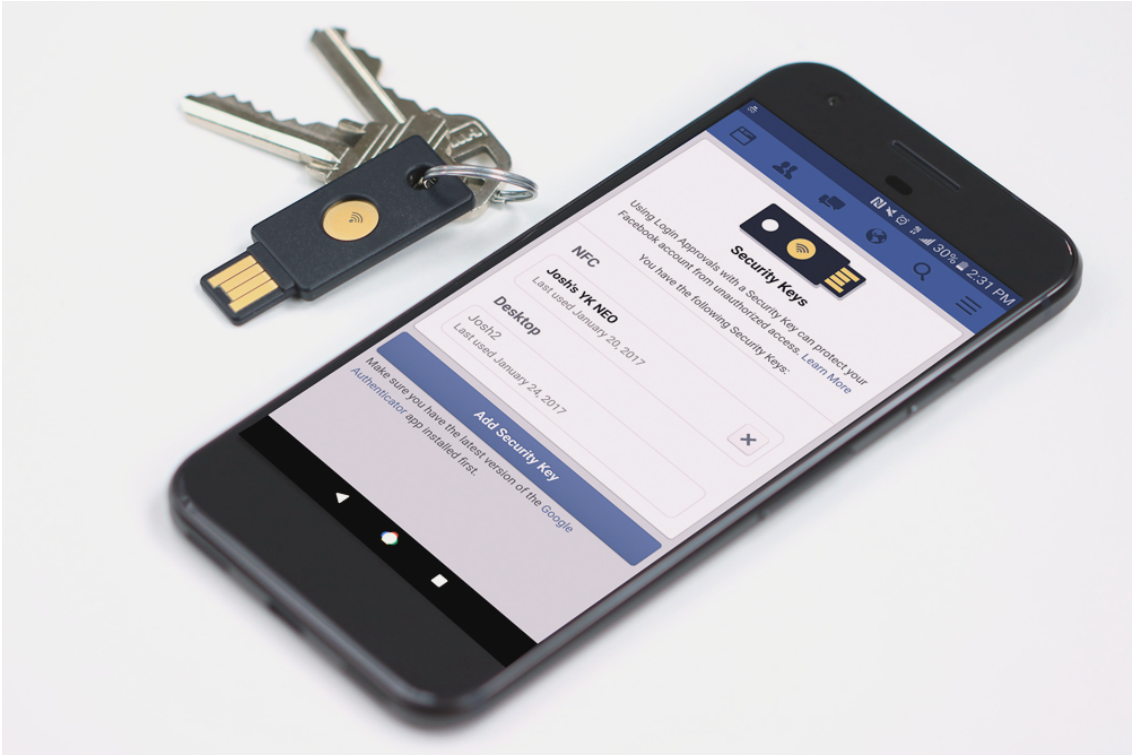
Something you

- **Know**
  - Password/phrase
  - “security question”
  - Secret key
- **Are**
  - Fingerprint
  - Iris patern
  - Gait
- **Have**
  - Key
  - Phone
  - Hardware token

Background: One-Time Passwords

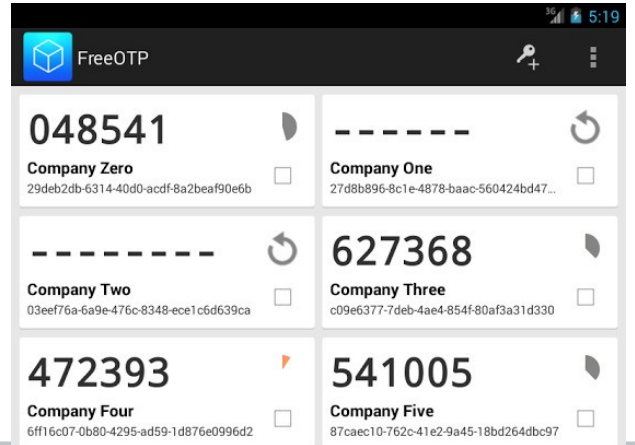
Prove posession of

- **Phone**
  - SMS
  - “Soft” token & key
- **Hardware Token**
  - Tamper-resistant hardware
  - Embedded key
- **Standards**
  - TOTP, HOTP



Background: Deployment

- **Easy front-end**
  - One password box
  - Everyone has a keyboard
- **Easy-ish backend**
  - RADIUS



- **Obnoxious user experience**
  - Must carry token
  - Must transcribe code
  - Often no backup permitted
  - Token proliferation
- **Users find 2X utility to avoid**

Background: FIDO U2F

Introduced in 2012

- **Advantages**
  - One token across all sites
  - Mutual authentication
  - Backup tokens
- **Disadvantages**
  - New protocol
  - Needs client support
  - Needs server support

"We fail if FIDO is not more usable than all the other (hardware token) options you have used before"

– Brett Mcdowell

Looks Cool!

Let’s give these to a bunch of undergrads and see what happens!

Two Phases

What we did:

- **Two-phase study**
  - Same procedures
  - A year apart
- **Some changes between**
  - Validated some recommendations
- **Two cases**
  - Google instructions
  - Yubico instructions
- **Expertise survey**
  - Previously validated
- **Think-aloud observation**
  - Gave keys to undergrads
  - Asked them to set up
  - Tried not to help
    - (or laugh)
- **Follow-up survey**

Phase I participants

- 20 male students, and 7 female students
- Six were between 18 and 20
- Sixteen were between 21 and 23
- Four were 24-26
- One was over 30
- Mean security expertise was 2.96 of 5
- Mean computing expertise was 4.34 of 5

Phase II participants

- 27 male students, and 8 female students
- One were between 18 and 20
- Twenty Nine were between 21 and 23
- Two were 24-26
- One was over 30
- Mean security expertise was 2.95 of 5
- Mean computing expertise was 4.22 of 5

Participants

- 20 male students, and 7 female students
- Six were between 18 and 20
- Sixteen were between 21 and 23
- Four were 24-26
- One was over 30
- Mean security expertise was 2.96 of 5
- Mean computing expertise was 4.34 of 5

- 27 male students, and 8 female students
- One were between 18 and 20
- Twenty Nine were between 21 and 23
- Two were 24-26
- One was over 30
- Mean security expertise was 2.95 of 5
- Mean computing expertise was 4.22 of 5

Recommendations – Phase I

- Finding instructions
- Demo versus reality
- Device identification
- Biometric versus touch
- Confirmation of operation
- Communicate the benefit
- Communicating the risks

Recommendations – Phase II

- Finding instructions
- ~~Demo versus reality~~
- Correctly identifying the device
- Biometric versus touch
- *Confirmation of operation*
- *Communicate the Benefit*
- *Communicating the risk*

Future work

- **Range of tokens**
  - Other hard tokens
  - Soft tokens
- **Different population**
  - Dad?
  - Coworkers?
  - “normal” undergrads?
- **Value communication**
- **Forthcoming standards**
  - More general extension of U2F ideas
  - Extra metadata options
    - Cool soft token possibilities
- **Collaboration with Red Hat**
  - Nathaniel McCallum and FreeOTP

Who we are

Dr. L. Jean Camp

https://www.sice.indiana.edu/all-people/profile.html?profile_id=178

@SanchariDecrypt

sancdas@indiana.edu

https://www.linkedin.com/in/sanchari-das

@acdingman

andrew@dingman.tech

Questions?

Presented at Financial Cryptography and Data Security 2018

Full paper at http://fc18.ifca.ai/preproceedings/111.pdf