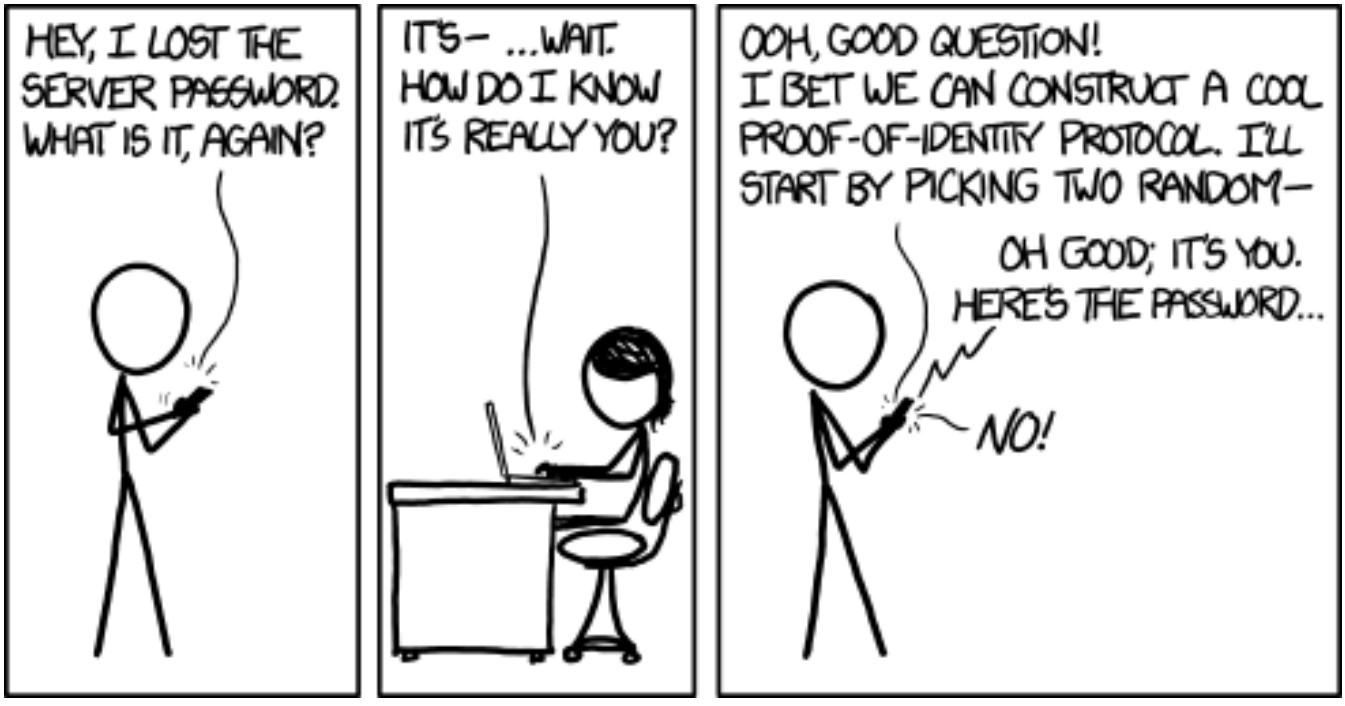
Authentication and ~~Availability~~



https://xkcd.com/1121/

Slides by Prof. Kevin Fu with material from Prof. J. Alex Halderman, Prof. Lorrie Faith Cranor, Prof. Wenyuan Xu

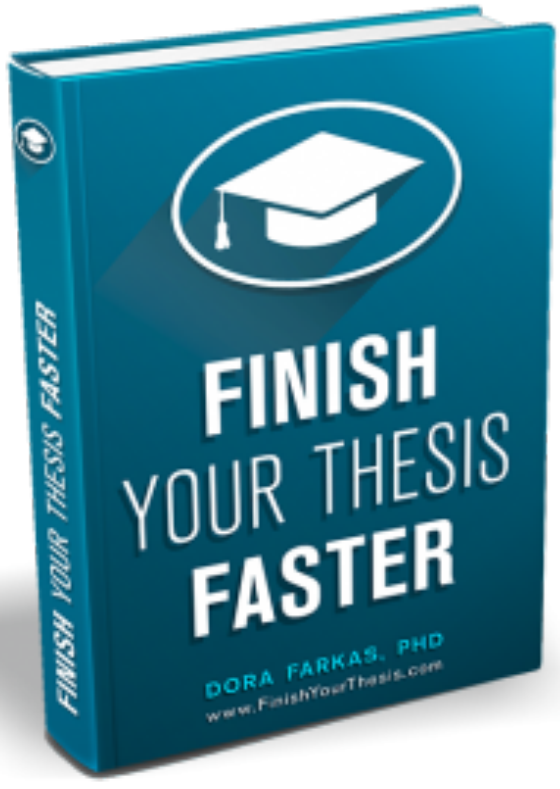
Seniors Considering PhD Programs!

PhD application essay feedback

Drafts due Monday in gradescope

Or read my classmate's book

web.eecs.umich.edu/~kevinfu/students.html



Today:

- Pa$$w0rdz
- Online and offline guessing
- Multi-Factor Authentication
- Knowledge-Based Authentication
- Denial of service (another day)

Three Ways to Authenticate

1. Something you know

2. Something you have

3. Something you are

How Do Passwords Fail?

Online Password Brute Force Attack

- Submit guesses to website, try to login
- Defenses
  - ✓ Rate limit
  - ✓ Lock account
  - ✓ Captcha
  - ✓ Anomaly detection

Offline Password Brute Force Attack

- Steal encrypted db of passwords
- Server could store:
  - Plaintext passwords (ugh!)
  - Encrypted passwords (hmm!)
  - Hashed passwords (better)
  - ✓ **Salted and hashed password**
    - ➡ Store (salt, H(salt || password)

- Pros and cons?
- Do's and Dont's of Web Authentication
  https://pdos.csail.mit.edu/papers/webauth:sec10.pdf

Prof. Lorrie Faith Cranor on Passwords

http://lorrie.cranor.org/blog/tag/dress/

Julia Angwin
@JuliaAngwin

Follow

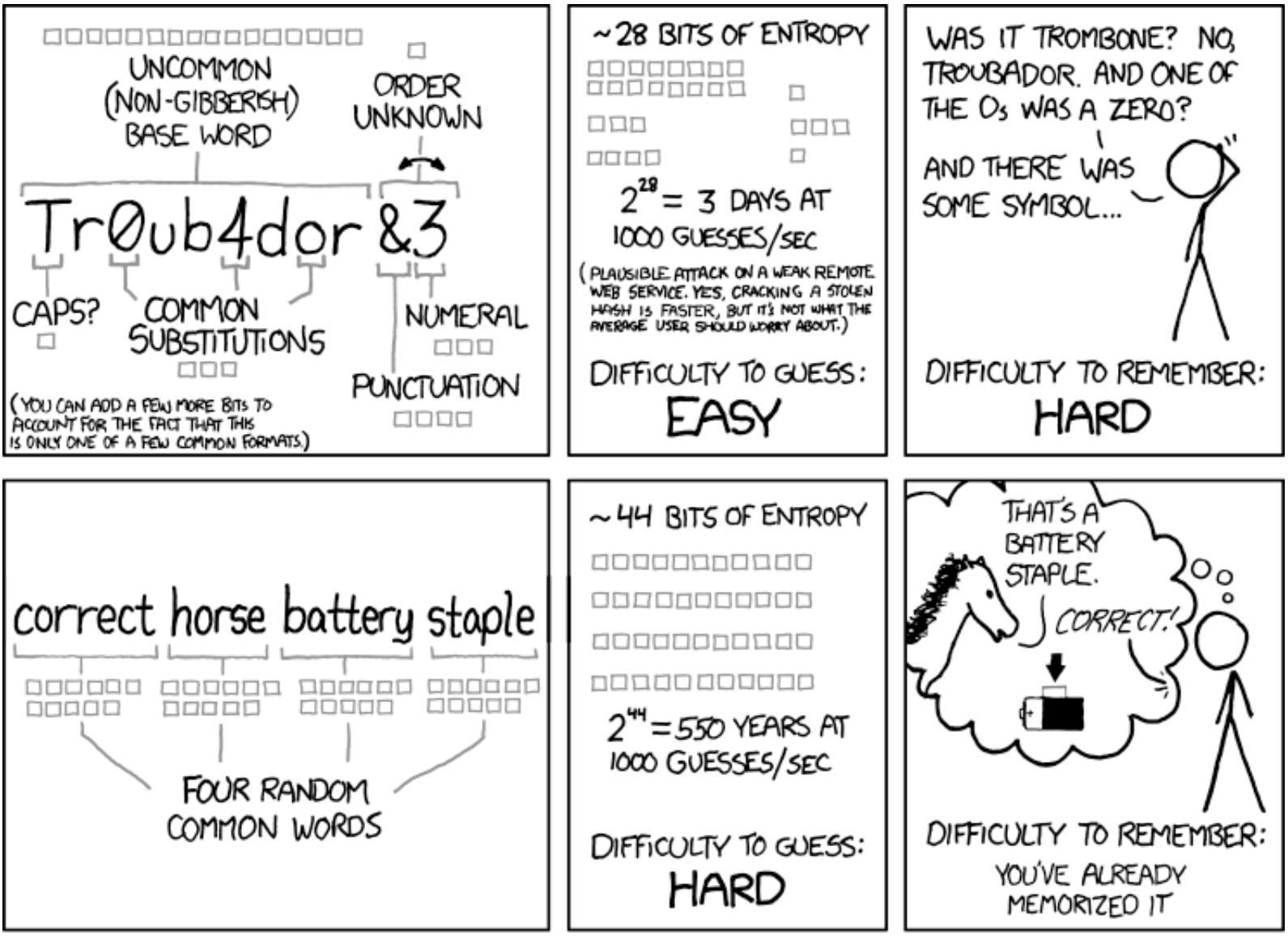
Awesome: @lorrietweet in her dress printed with the most common passwords

Reply Retweet Favorited More

RETWEETS 868 FAVORITES 640

xkcd password generator

good or bad advice? let's see!



xkcd password generator

"Correct horse battery staple: Exploring the usability of system-assigned passphrases" by Shay et al. in Symposium on Usable Privacy and Security (SOUPS) 2012.

- Explore usability of system-assigned passphrases
- Compare to system-assigned passwords of similar security
- System-assigned assures random selection

Methodology

- 1,476-participant Mturk study
- Participants randomly assigned password or passphrase
- Enter password/phrase, take survey, enter it again
- Emailed to come back two days later
- Enter password/phrase, take another survey

Conditions

- 8 passphrase conditions, 3 password conditions
- Varied factors:
  - Size of dictionary words are selected from
  - Whether order matters
  - Parts of speech
  - Number of words
  - Instructions

4 common words

try there three come

one between high tell

Noun verb adjective noun

plan builds sure power

end determines red drug

System-assigned passwords

`@J#8x`

`*2LxG`

Pronounceable passwords

`tufritvi`

`vadasabi`

Empirical results contradict XKCD

- No clear user favorite
- Passphrases are not easier to remember
- Passphrases slower to enter, more mistakes
- Error correction helps passphrase accuracy
- Pronounceable passwords were faster to enter with fewer mistakes than other passwords or passphrases

Attacks Against Something You Know

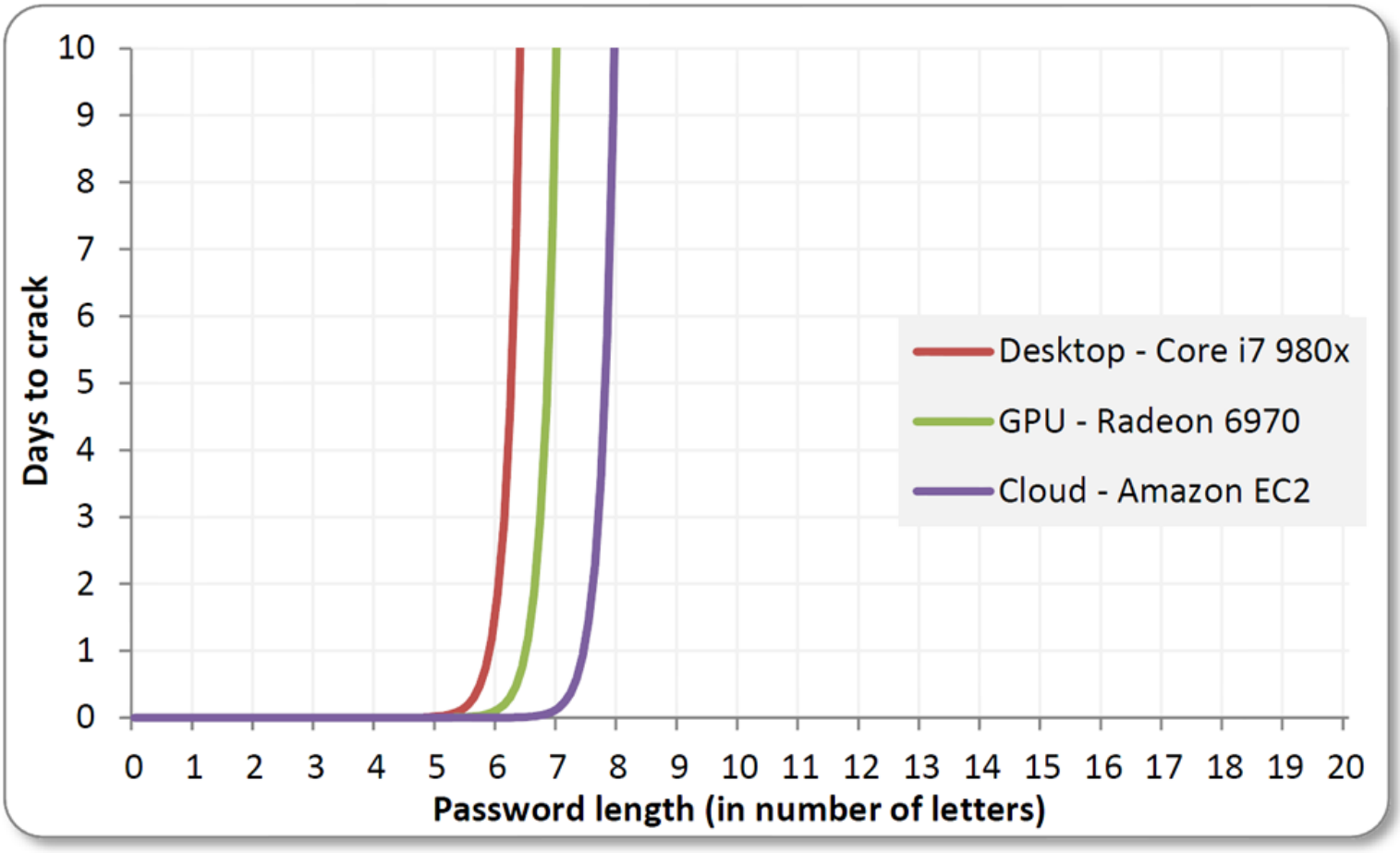
- Online Attacks
  - Detectable, rate limited
- Offline attacks
  - How to securely store passwords?
  - Brute force with Amazon EC2, GPUs
- Dictionary attack
  - Cracked 33% of 36m Ashley Madison Passwords in 10 days
  - Cracked 90% of 6.5m LinkedIn passwords in 6 days

Guessing PINs

	PIN	Frequency
1	1234	10.713%
2	1111	6.016%
3	0000	1.881%
4	1212	1.197%
5	7777	0.745%
6	1004	0.616%
7	2000	0.613%
8	4444	0.526%
9	2222	0.516%
10	6969	0.512%
11	9999	0.451%
12	3333	0.419%
13	5555	0.395%
14	6666	0.391%
15	1122	0.366%
16	1313	0.304%
17	8888	0.303%
18	4321	0.293%
19	2001	0.290%
20	1010	0.285%

DataGenetics

Passwords



http://blog.erratasec.com/2012/08/common-misconceptions-of-password.html

Countermeasures

- Slower hash functions
  (e.g., 10,000 iterations of SHA256)
- Randomized salt for each password
  H(salt, pwd)
  - What attack does this thwart?
- One-Time Passwords
  - k, H(k), H(H(k)), …
- Multi-Factor Authentication

Exercise!

Sketch a one-time password system for client-server authentication using a pre-image resistant hash.

Server setup:

- Pick an integer n
- Randomly select last password p_n
- For i=n-1 downto 0, let $p_i=h(p_{i+1})$
- Store p_0 in server password database for a user

Authentication: User presents to server the lowest unused password starting at p_1

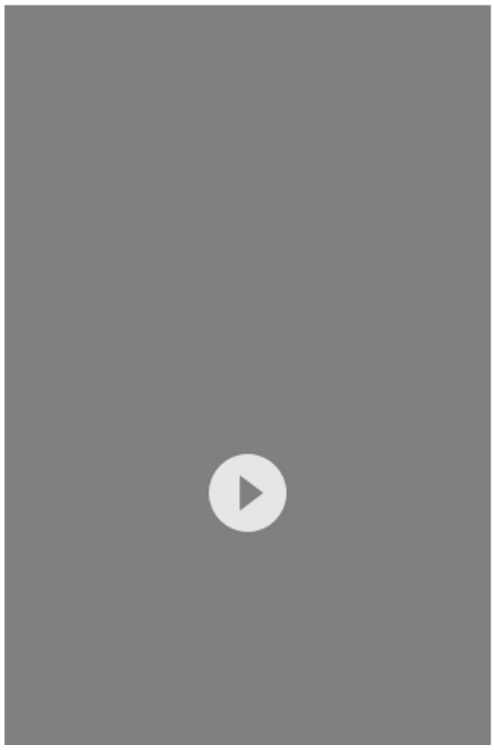
Your exercise:

- What information does the server keep?
- What information does the user keep?
- How does the server verify a OTP?
- What does server do after verification?
- What are the strengths and weaknesses?

Multi-Factor Authentication

- Two-Factor Authentication (2FA)
- A best practice
- U-M moving toward 2FA
- Defense against phishing, keylog, stolen passwords

Ann Arbor–based Duo Security gets $12M in Series B funding led by Silicon Valley VC firm



Multi-Factor Authentication

A local 2FA company started with a guy who worked for Prof. Honeyman

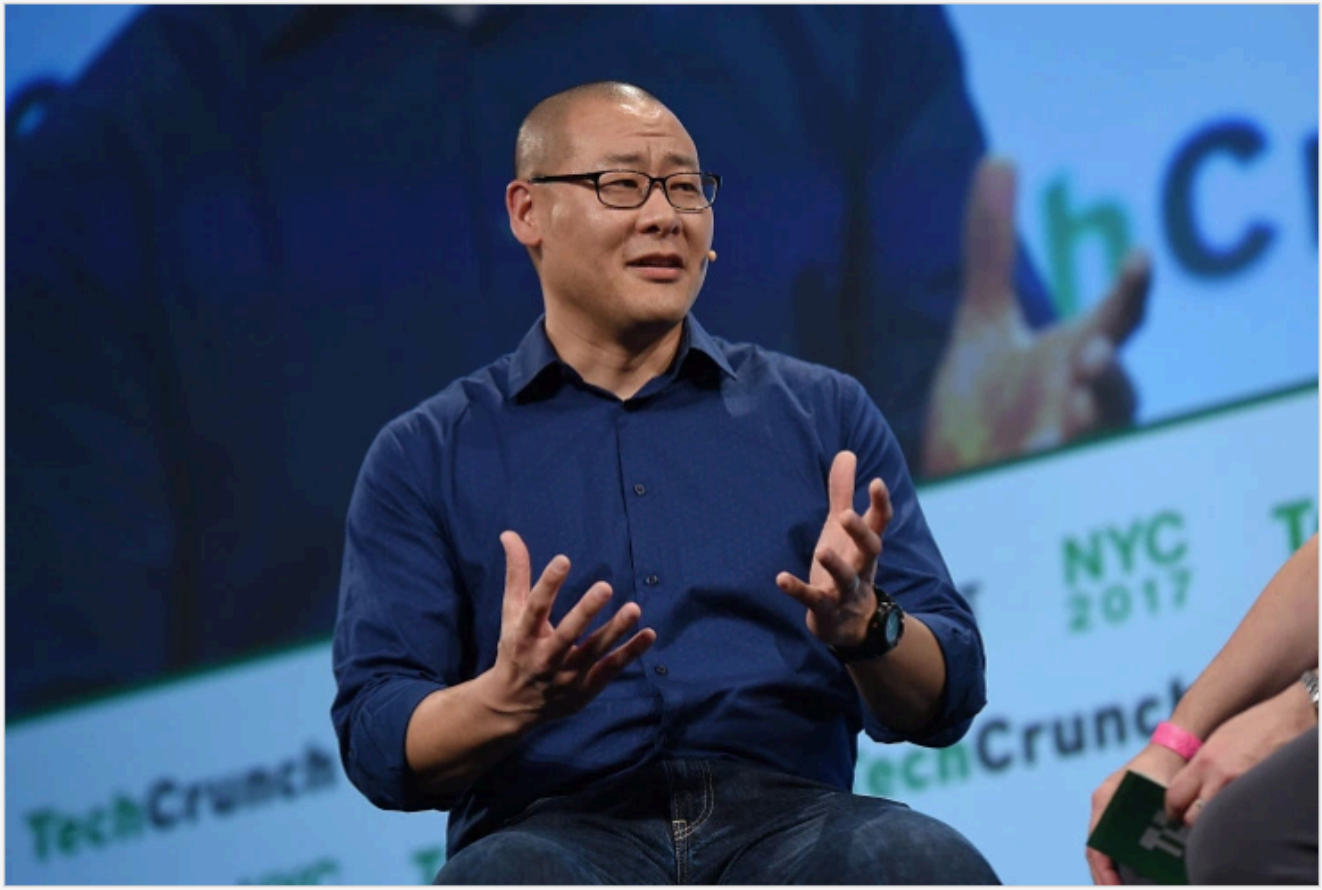
Dug Song (CEO of Duo Security), Prof. Fu, and Prof. Honeyman at USENIX Security in 2001

https://www.usenix.org/legacy/events/sec01/

Duo Security raises $70 million at a valuation north of $1 billion

Posted 13 hours ago by ***Matt Burns*** *(@mjburnsy)*

Next Story



Duo Security today announced its Series D funding that puts the company in unicorn territory. The company raised $70 million led by Meritech Capital Partners and Lead Edge Capital at a valuation of $1.17 billion. This funding round brings the company's total amount raised to $119 million.

This round included new investors, Index Ventures and Workday, that latter of which joins as a strategic partner, as well as existing investors Redpoint Ventures and True Ventures.

The Michigan-based SaaS company was founded in 2010 in Ann Arbor, Michigan, which it still calls home though it has since opened offices in Austin; San Mateo, Calif.; and London and now employs more than 500 globally. The company says it now works with more than 10,000 companies and has more than doubled its annual recurring revenue for the past four years.

In May 2017 at TechCrunch Disrupt SF Duo Security's founder Dug Song said Duo makes security easy for organizations at scale. The company's main product is a two-factor authentication app — which TechCrunch's parent company uses and I've found it works fine — but Duo also offers other security products to secure users and their devices.

Study of 70 Million Yahoo Passwords

The science of guessing: analyzing an anonymized corpus of 70 million passwords

Joseph Bonneau
Computer Laboratory
University of Cambridge
jcb82@cl.cam.ac.uk

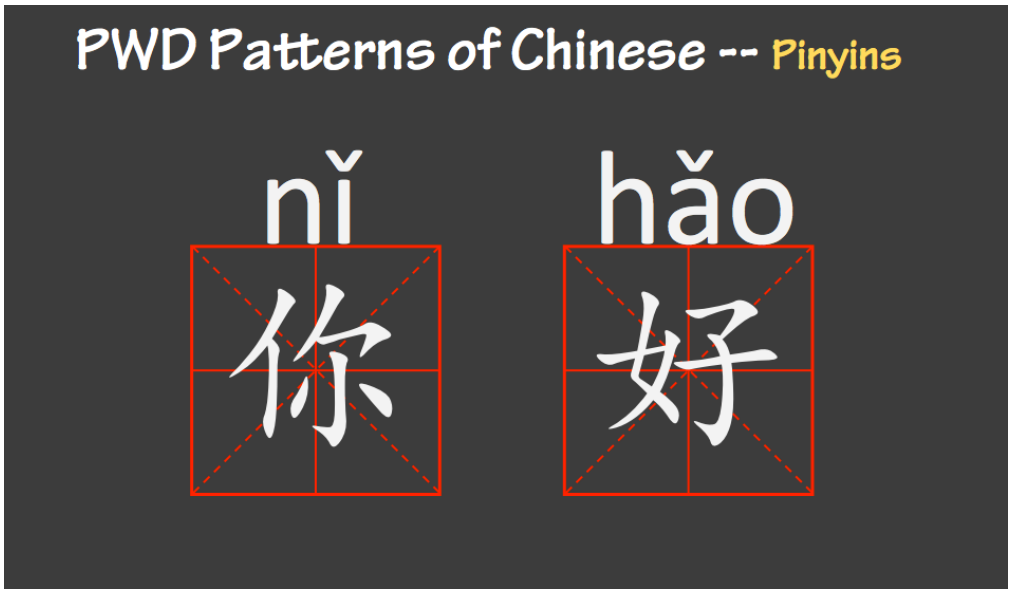
Crackability counterintuitively **increased** after introducing password meters!

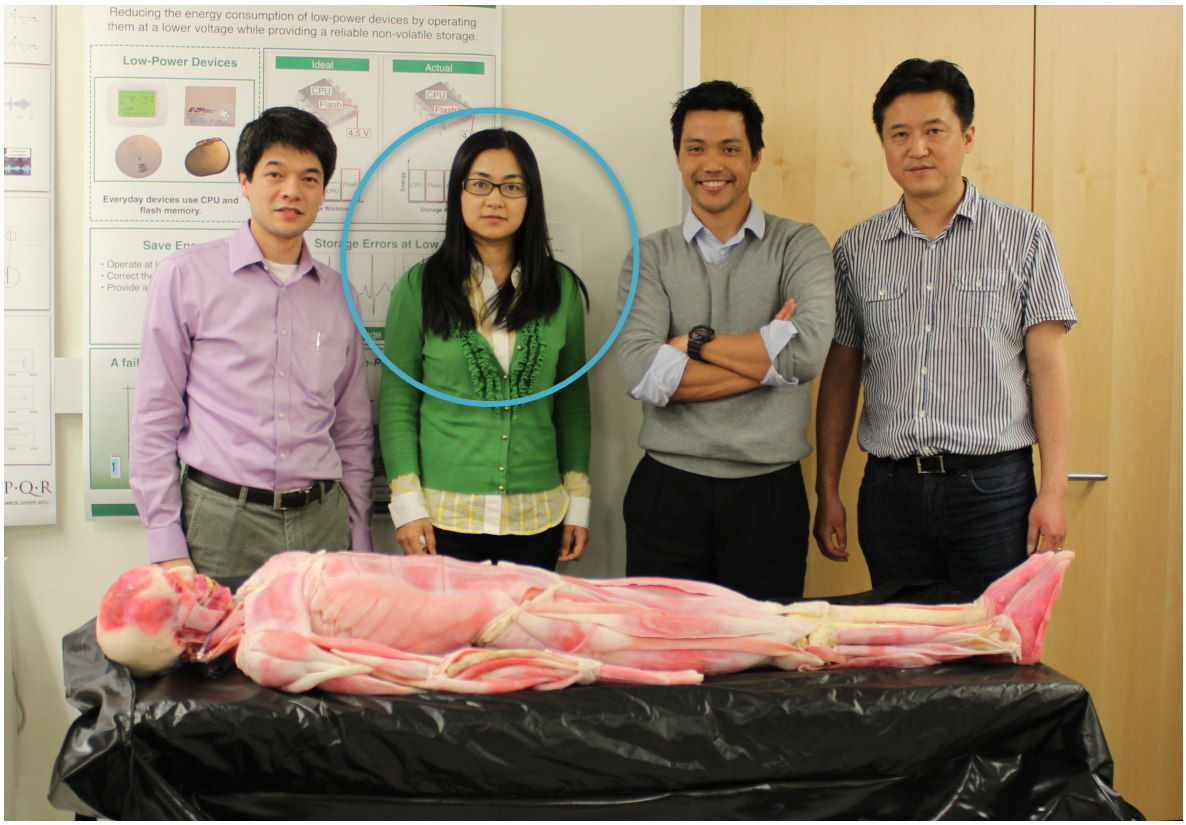
Chinese Passwords Crackable Too

A Large-Scale Empirical Analysis of Chinese Web Passwords

Zhigong Li and Weili Han, *Fudan University*; Wenyuan Xu, *Zhejiang University*

https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/li_zhigong





Chinese Passwords Crackable Too

7

What are the Most Popular Passwords

	Chinese	English
1	123456 (2.17%)	123456 (0.88%)
2	123456789 (0.65%)	12345 (0.24%)
3	111111 (0.59%)	123456789 (0.23%)
4	12345678 (0.39%)	password (0.18%)
5	000000 (0.34%)	iloveyou (0.15%)

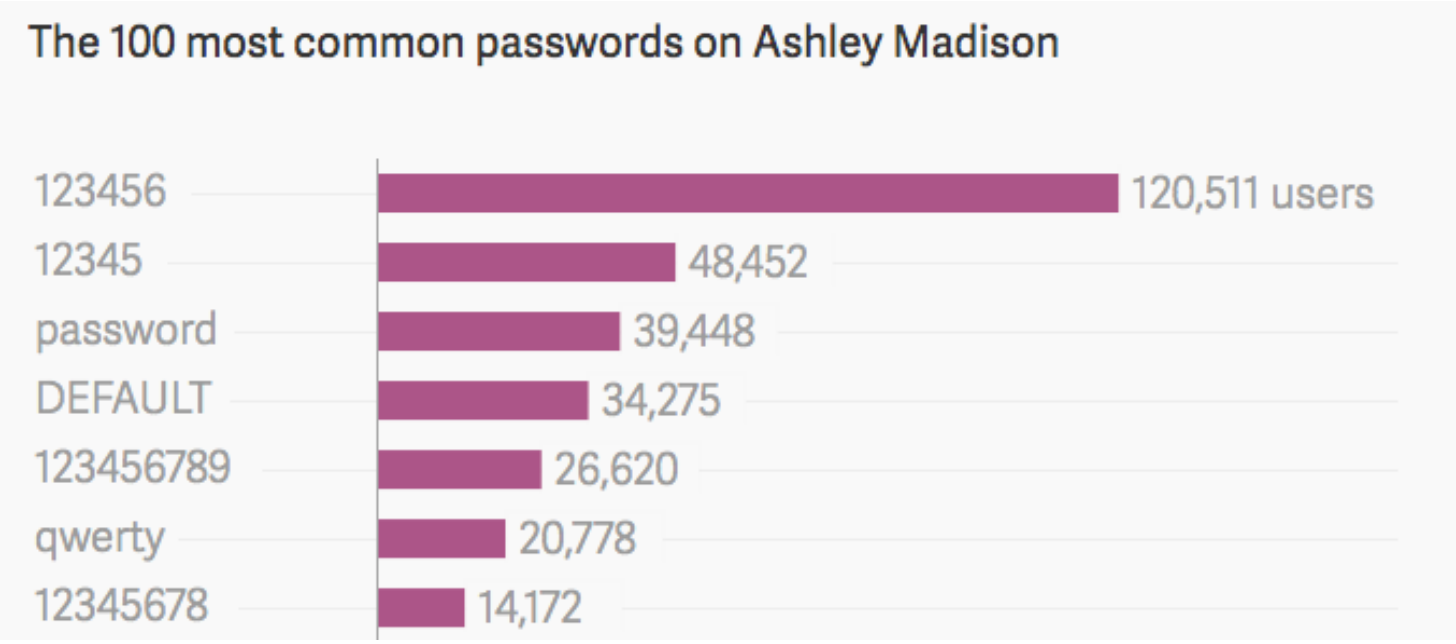
16

Special Passwords -- Love

	Top Chinese Pinyins	Top English Words
1	woaini (1.47%)	password (1.28%)
2	li (1.06%)	iloveyou (0.98%)
3	wang (0.97%)	love (0.76%)
4	tianya (0.89%)	angel (0.59%)
5	zhang (0.84%)	monkey (0.45%)

11 Million Ashley Madison Encrypted Passwords Cracked in 10 Days

- Passwords hashed with Bcrypt
- But some protected with MD5



http://qz.com/501073/the-top-100-passwords-on-ashley-madison/

http://thehackernews.com/2015/09/ashley-madison-password-cracked.html

Knowledge-Based Authentication

http://www.hsgac.senate.gov/hearings/the-irs-data-breach-steps-to-protect-americans-personal-information

So Far:

Crypto

Web Security

Network Security

Authentication

Next:

Control hijacking