Lecture 11: Passwords (cont'd)

CS 181W

Fall 2022

Recall: Authentication of humans

- Something you are

  biometrics (e.g., fingerprints)

- Something you know

  secret information (e.g., a password)

- Something you have

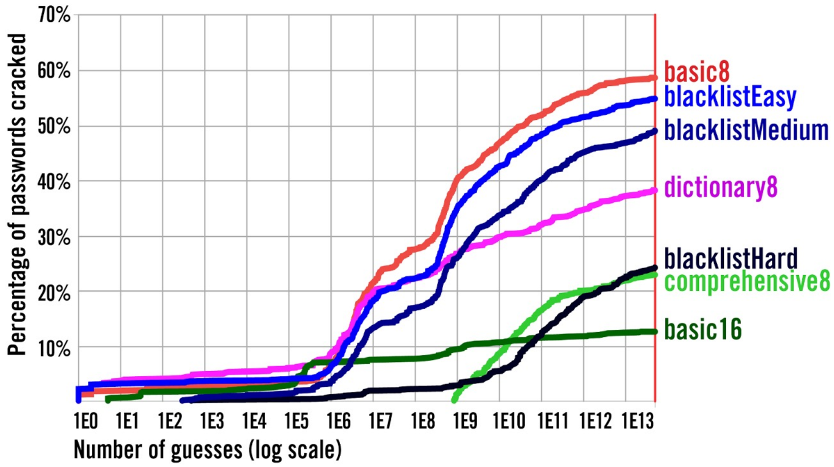
  possession of a physical device (e.g., a particular phone)

Recall: Password lifecycle

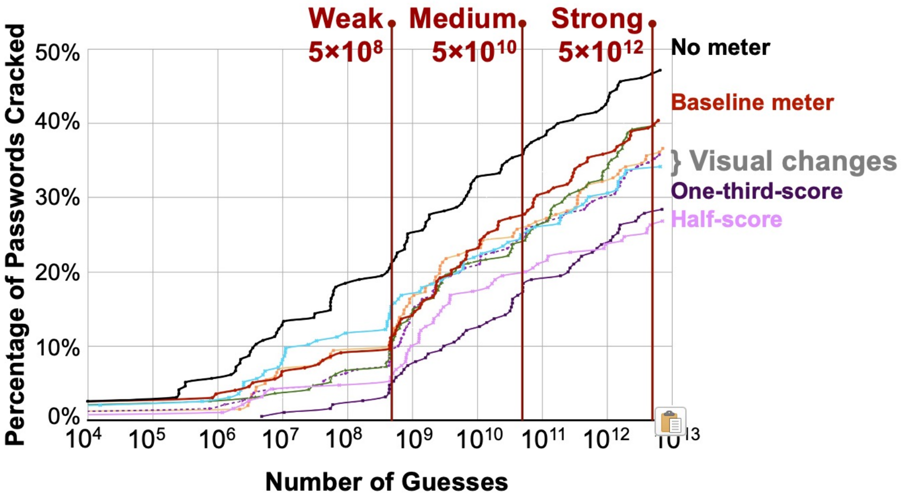
1. **Create:** user chooses password
2. **Store:** system stores password with user identifier
3. **Use:** user supplies password to authenticate
4. **Change/recover/reset:** user wants or needs to change password

Recall: How to get better passwords

Password Policies?



Password Meters?



Password perceptions study

`p@ssw0rd`

`pAssw0rd`

p@ssw0rd much more secure ○ ○ ○ ○ ○ ○ ○ pAssw0rd much more secure

Ur et al. Do users' perceptions of password security match reality? CHI 2016.

Which is more secure?

iloveyou88

ieatkale88

Study participants' perceptions

iloveyou88 = ieatkale88

Reality

iloveyou88

ieatkale88

4,000,000,000 × more secure!

Which is more secure?

brooklyn16

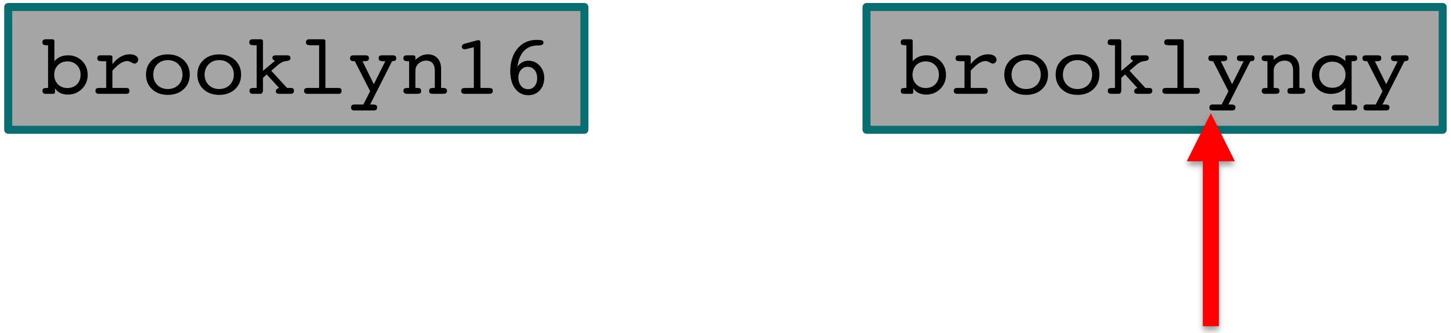
brooklynqy

Study participants' perceptions

[✓ brooklyn16]

brooklynqy

Reality



brooklyn16

brooklynqy

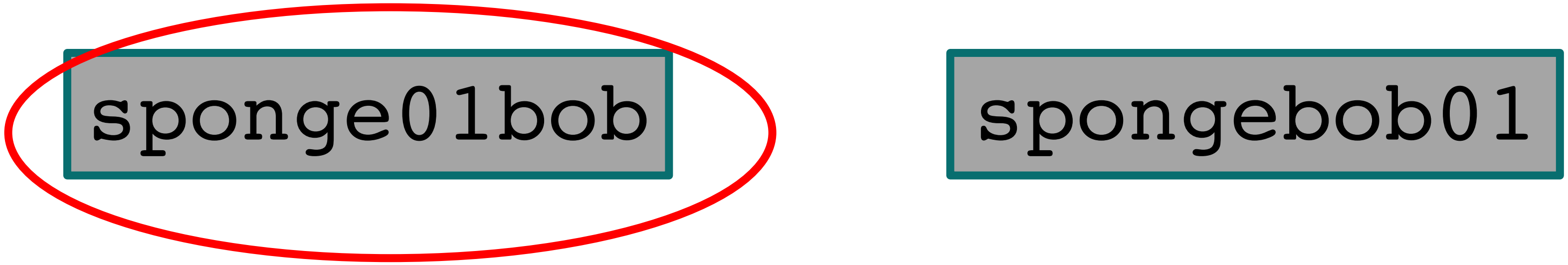
300,000 × more secure!

Which is more secure?

sponge01bob

spongebob01

Study participants' perceptions



sponge01bob

spongebob01

Reality

`sponge01bob`

`spongebob01`

900,000 ×
more secure!

Which is more secure?

1qaz2wsx3edc

thefirstkiss

Study participants' perceptions

[✓ `1qaz2wsx3edc`]

`thefirstkiss`

Reality

`1qaz2wsx3edc`

`thefirstkiss`

Both are pretty bad!

300×
more secure!

Participants were not all wrong

- Knew to avoid common words and names
  - But didn't recognize frequently used phrases

~~password~~
~~michael~~
iloveyou

- Knew digits and symbols added strength
  - But thought they provided more strength than they do

password!
michael2015

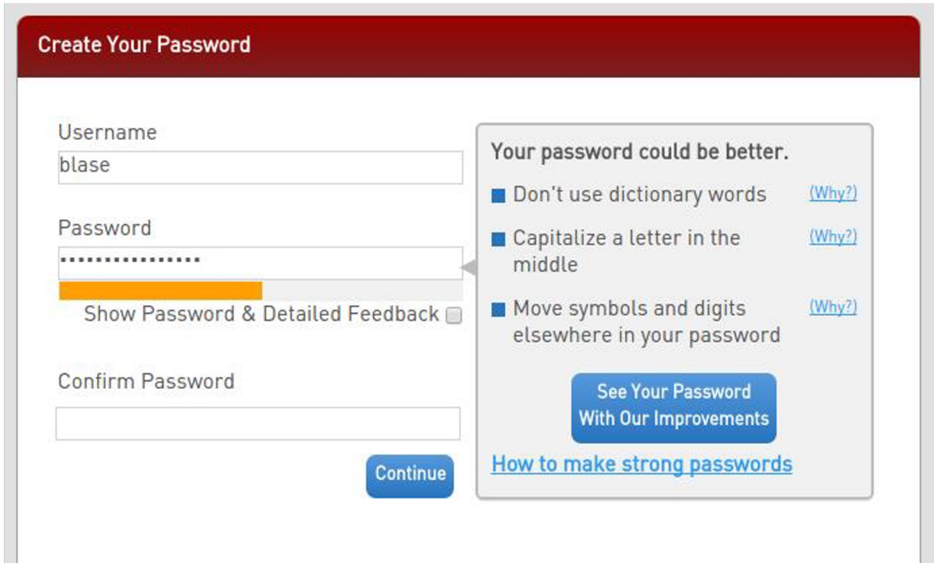
- Perception of attackers varied wildly
  - Many unaware of large-scale attacks

10^{60} guesses?

2 guesses?

Data-driven password meter

General Feedback



Username
blase

Password
••••••••••••••••

Show Password & Detailed Feedback □

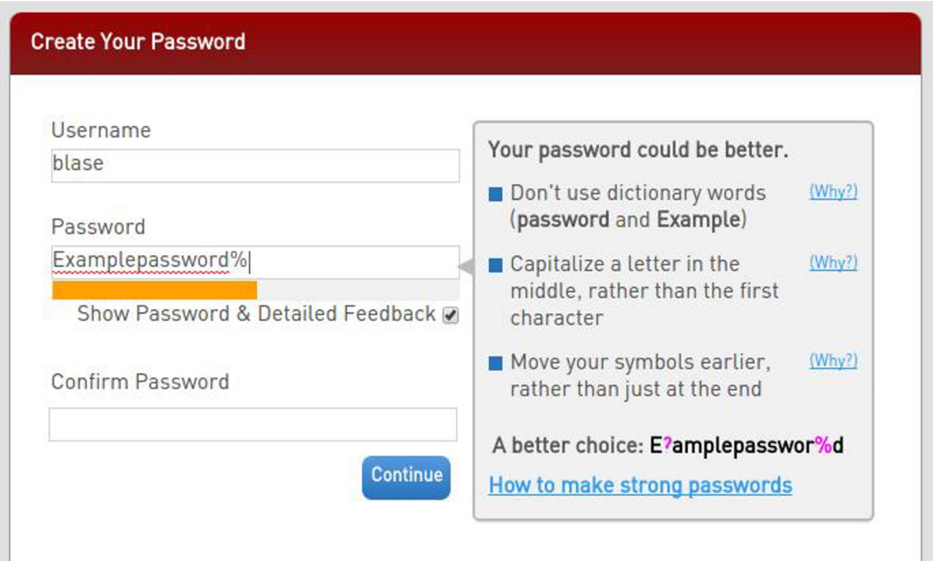
Confirm Password

Your password could be better.

- Don't use dictionary words (Why?)
- Capitalize a letter in the middle (Why?)
- Move symbols and digits elsewhere in your password (Why?)

See Your Password With Our Improvements
How to make strong passwords
Continue

Detailed Feedback



Username
blase

Password
Examplepassword%

Show Password & Detailed Feedback ☑

Confirm Password

Your password could be better.

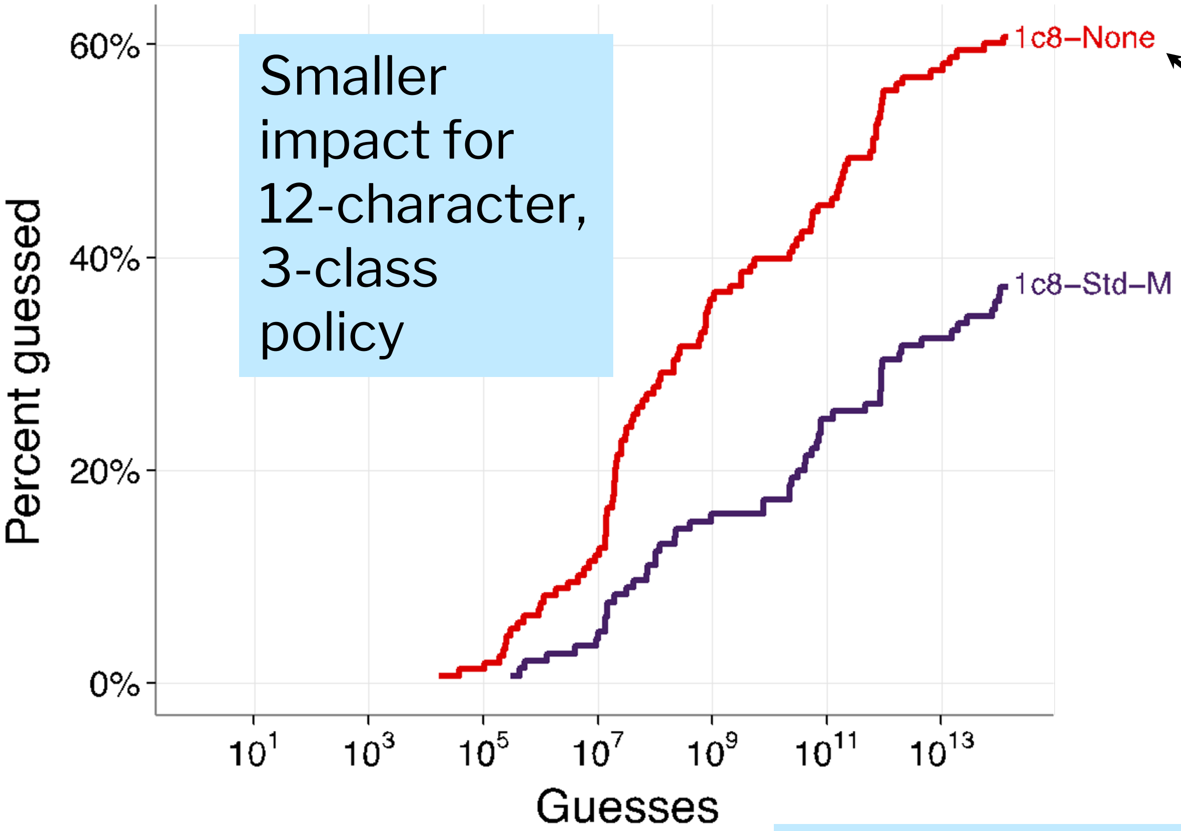
- Don't use dictionary words (**password** and **Example**) (Why?)
- Capitalize a letter in the middle, rather than the first character (Why?)
- Move your symbols earlier, rather than just at the end (Why?)

A better choice: **E?amplepasswor%d**

Ur et al. Design and Evaluation of a Data-Driven Password Meter. CHI 2017

Online Study
Between Subjects
n=4509

Data-driven meter improves strength



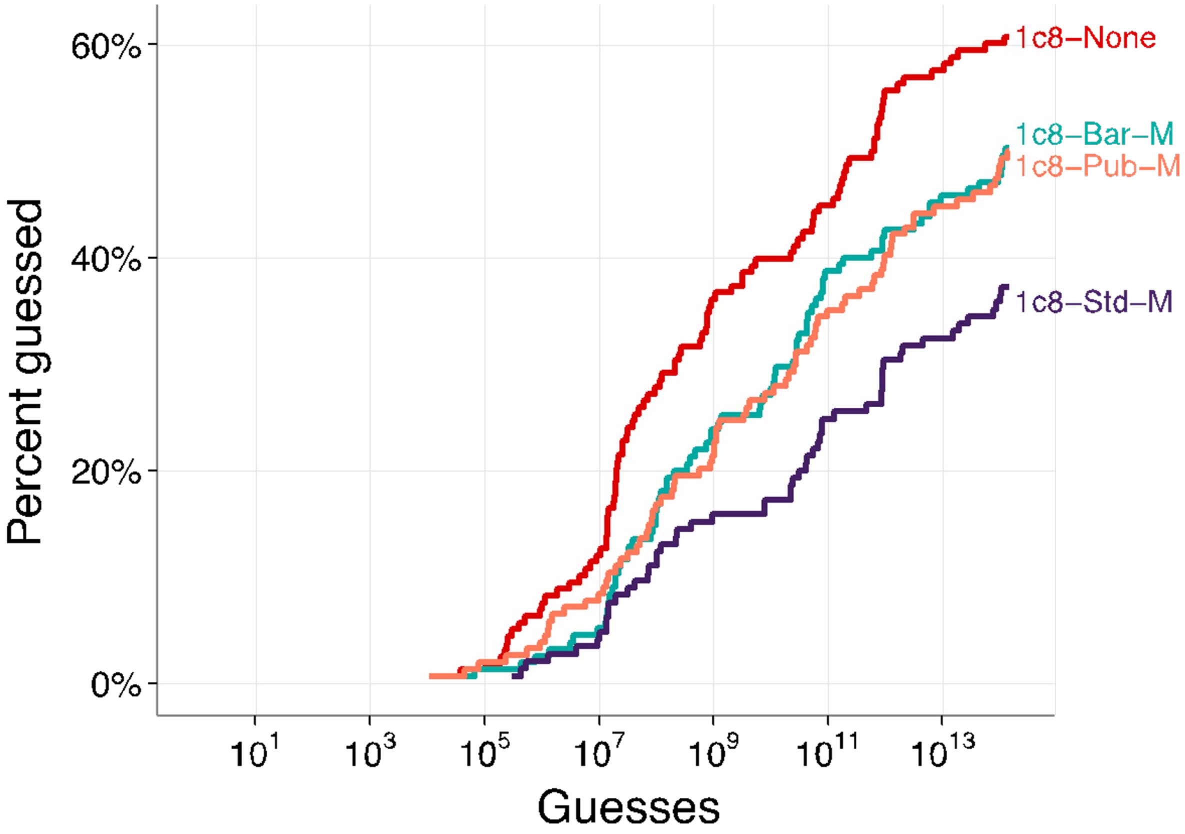
Smaller impact for 12-character, 3-class policy

No meter

Detailed feedback

Passwords created with meter are just as memorable!

Detailed Feedback Matters



No meter

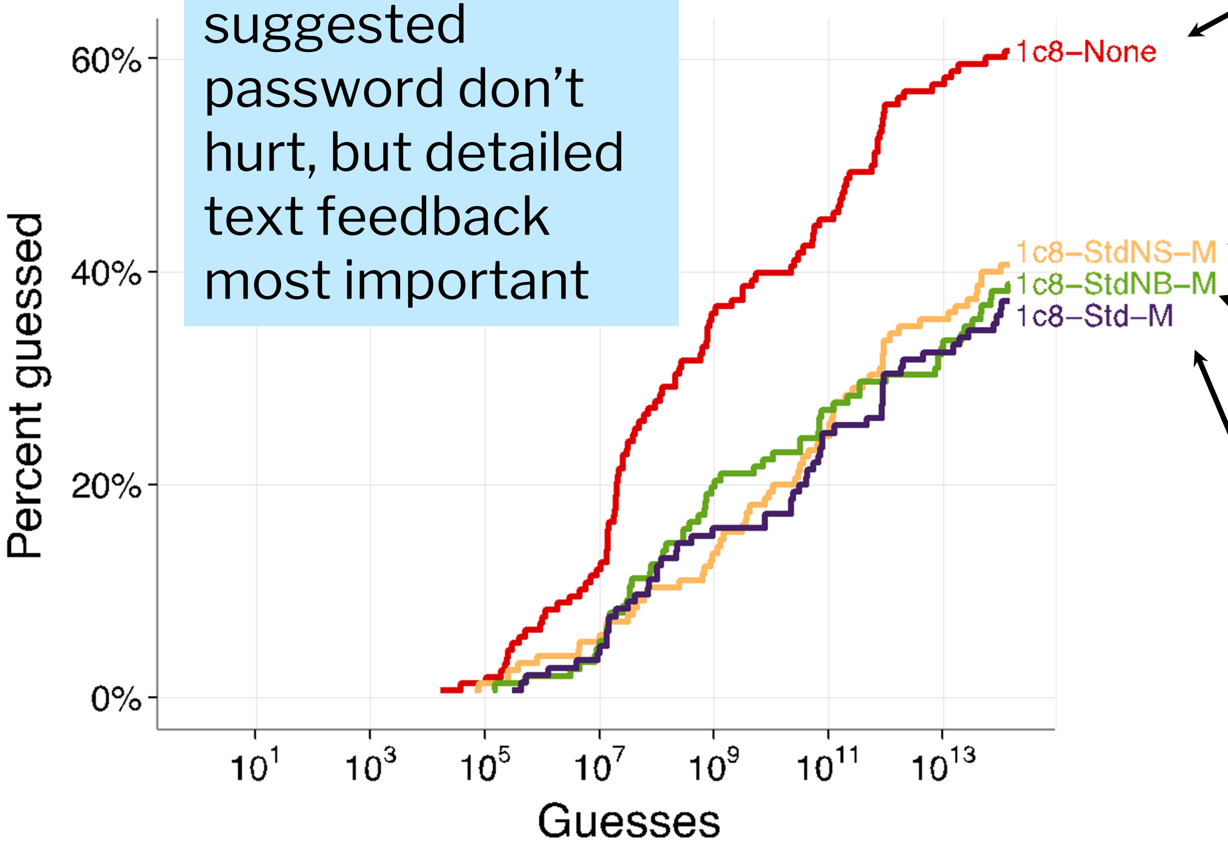
Only bar

No detailed feedback

Detailed feedback

Other factors less critical

Bar and suggested password don't hurt, but detailed text feedback most important



No meter

No suggested password

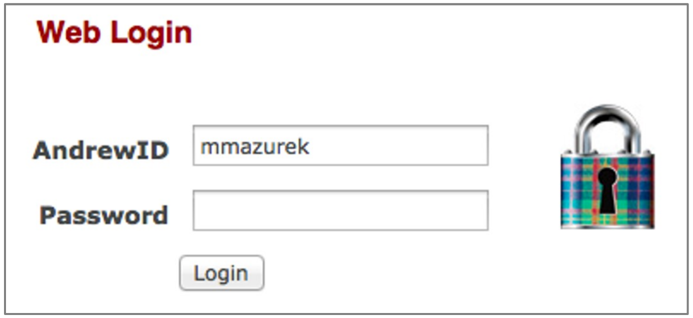
No bar

Detailed feedback

How valid are online studies?

Passwords for an entire university

- 25k+ CMU faculty, staff, and student accounts
  - Plus 17,104 deactivated accounts
- Single-sign-on for email, financial, grades, registration, health, etc.
- Password requirements:
  - Minimum 8 characters
  - Upper, lower, digit, symbol
  - Dictionary check (241,497 words)



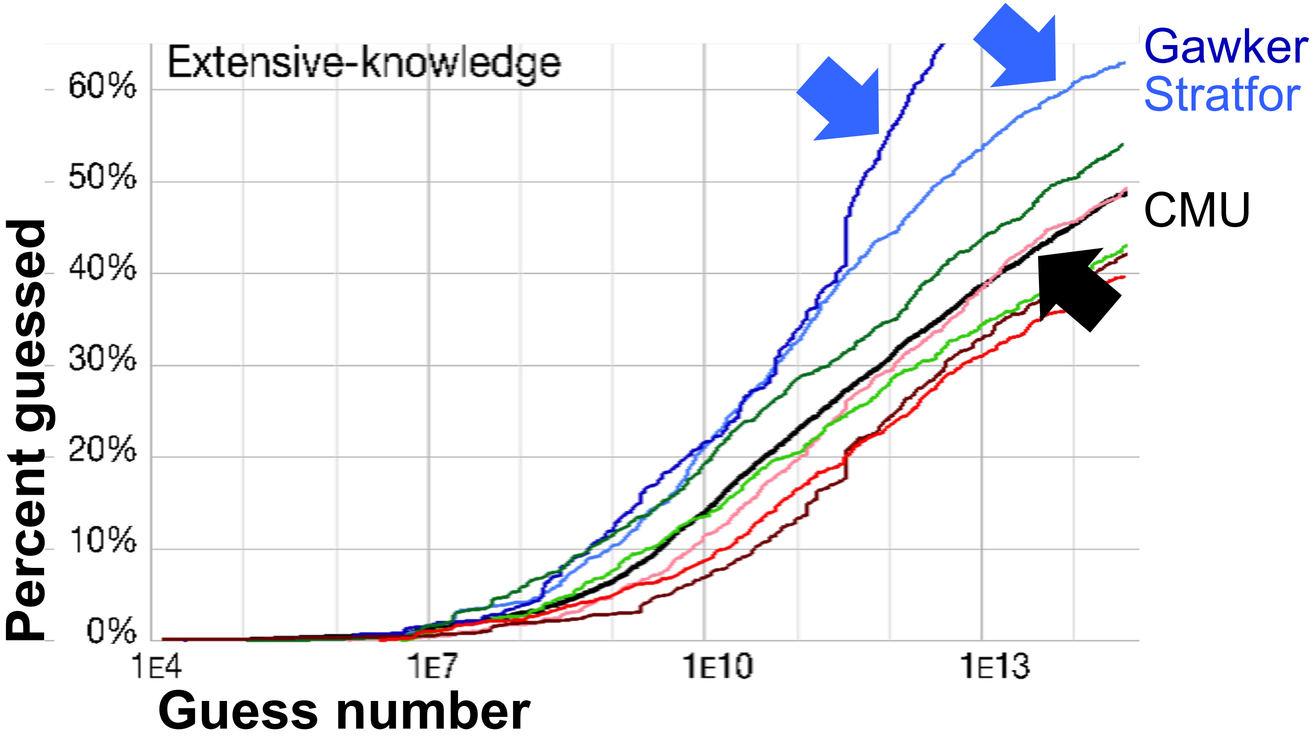
AndrewID mmazurek

Password

- 7 months of authentication logs
- Survey after password change (n=694)

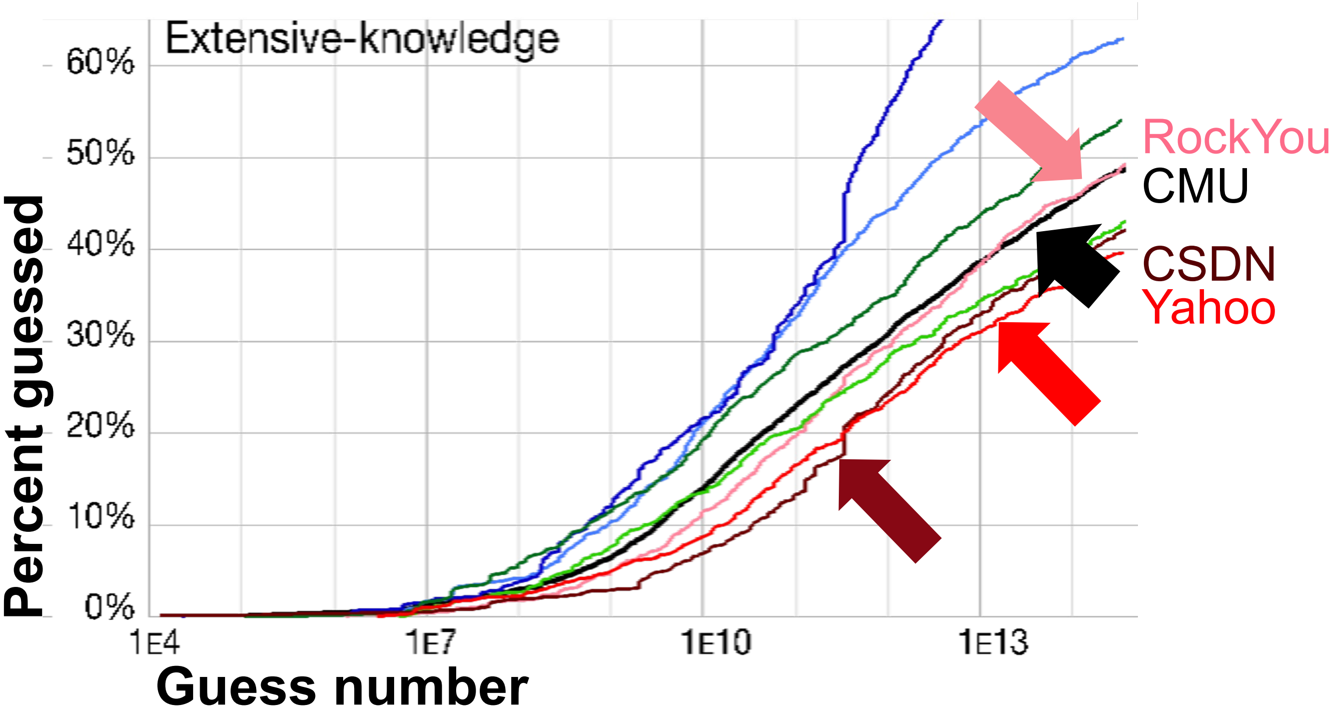
M.L. Mazurek, S. Komanduri, T. Vidas, L. Bauer, N. Christin, L.F. Cranor, P.G. Kelley, R. Shay, and B. Ur. Measuring Password Guessability for an Entire University. ACM CCS 2013.

Comparing leaked/hashed passwords



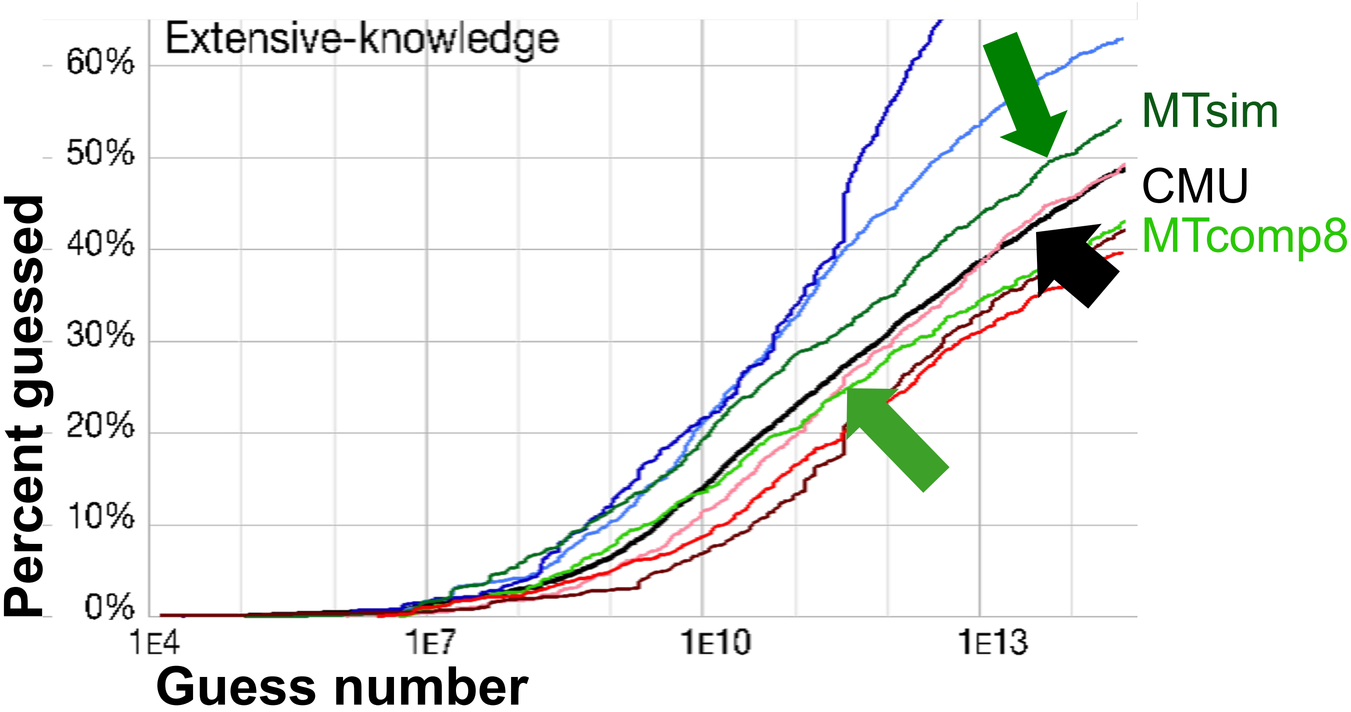
Leaked hashed/cracked: Very easy to guess

Comparing leaked plaintext passwords



Leaked plaintext: RockYou close to CMU, others much tougher

Comparing leaked passwords



Online studies: Closest across all metrics

Password lifecycle

1. **Create:** user chooses password
2. **Store:** system stores password with user identifier
3. **Use:** user supplies password to authenticate
4. **Change/recover/reset:** user wants or needs to change password

Password change

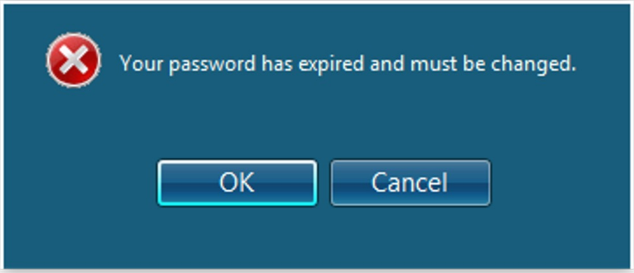
Motivated by...

- **Attacker** learns password
- **System** forces password expiration
- **User** forgets password (maybe just *recover* password)

Does changing your password regularly make accounts more secure?

Testing this theory at UNC

- Mandatory password change every 3 months
- Researchers obtained 4-15 hashed defunct passwords to each account
- Cracked >1 non-last password for 7,752 accounts


Your password has expired and must be changed.

Knowing old password can we predict the new one?

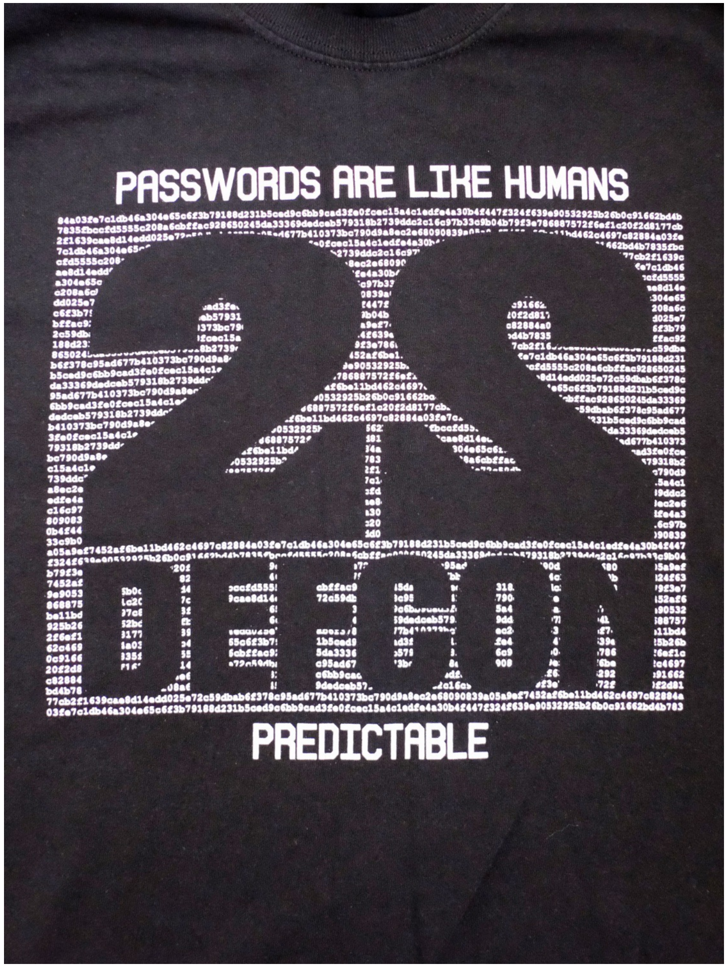
Predictable transformations

Predictable transformations

Capitalization:	`tarheels#1` → `tArheels#1`
Duplication:	`tarheels#1` → `tarheels#11`
Substitution:	`tarheels#1` → `tarheels#2`
Insertion:	`tarheels#1` → `tarheels#12`
Keyboard transform:	`tarheels#1` → `tarheels#!`
Date:	`tarheel#0510` → `tarheel#0810`

Results

- Online attack
  - 17% of accounts cracked in <5 guesses
- Offline attack
  - 41% of accounts cracked within 3 seconds



Survey evidence

- Frequent password expiry → users create weaker passwords
  (Adams & Sasse, 1999)
- Annoyed at password change → users create weaker passwords
  (Mazurek et al., 2013)

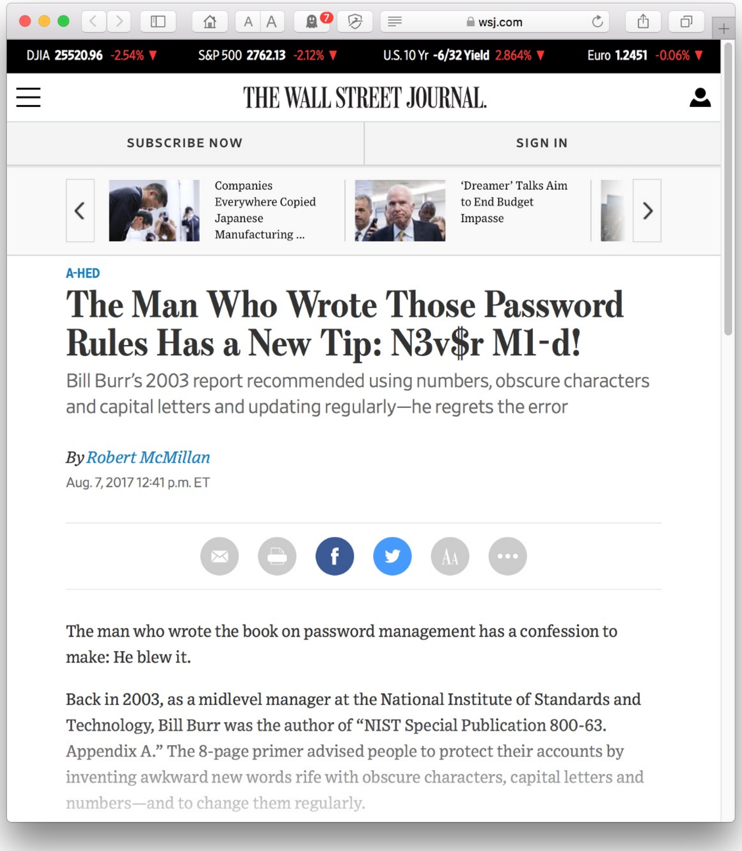
WORLD
PASSWORD
DAY 2016

**** When is the last time you **changed** yours?

New guidance

Our research was cited by NIST in June 2017 *NIST Special Publication 800-63B Digital Identity Guidelines*

- Emphasis on length rather than complexity
- Don’t require periodic password changes


wsj.com
DJIA 25520.96 -2.54% ▼
S&P 500 2762.13 -2.12% ▼
U.S. 10 Yr -6/32 Yield 2.864% ▼
Euro 1.2451 -0.06% ▼
THE WALL STREET JOURNAL.
SUBSCRIBE NOW
SIGN IN
Companies Everywhere Copied Japanese Manufacturing ...
‘Dreamer’ Talks Aim to End Budget Impasse

A-HED

The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1-d!

Bill Burr’s 2003 report recommended using numbers, obscure characters and capital letters and updating regularly—he regrets the error

By *Robert McMillan*

Aug. 7, 2017 12:41 p.m. ET

The man who wrote the book on password management has a confession to make: He blew it.

Back in 2003, as a midlevel manager at the National Institute of Standards and Technology, Bill Burr was the author of “NIST Special Publication 800-63. Appendix A.” The 8-page primer advised people to protect their accounts by inventing awkward new words rife with obscure characters, capital letters and numbers—and to change them regularly.

Password change

Motivated by...

- **Attacker** learns password

- ~~**System** forces password expiration~~

- **User** forgets password (maybe just *recover* password)

Change mechanisms

- Tend to be **more vulnerable** than the rest of the authentication system
  - Not designed or tested as well
  - Have to solve the authentication problem without the benefit of a password

- Two common mechanisms:
  - Security questions
  - Emailed passwords

Security questions

- Something you know: attributes of identity established at enrollment
- **Pro:** you are unlikely to forget answers
- **Assumes:** attacker is unlikely to be able to answer questions
- **Con:** might not resist targeted attacks
- **Con:** linking is a problem; same answers re-used in many systems

Secret questions

- How secure are secret questions against random guessing?
- Can acquaintances guess secret questions?
- Can users remember their own secret questions?

Stuart Schechter, A. J. Bernheim Brush, and Serge Egelman. It's No Secret: Measuring the Security and Reliability of Authentication via 'Secret' Questions. IEEE Security and Privacy 2009.

130 participants, recruited in pairs

- Move to room separate from partner
- Answer personal questions for top four webmail services
- Guess partner’s answers to personal questions
- Attempt to recall answers to own personal questions
- Second chance to guess partner’s questions using online research
- 3-6 months later: Attempt to recall answer to own questions in online survey

AOL Questions

Aol Mail.

- What is your pet’s name?
- Where were you born?
- What is your favorite restaurant?
- What is the name of your school?
- Who is your favorite singer?
- What is your favorite town?
- What is your favorite song?
- What is your favorite film?
- What is your favorite book?
- Where was your first job?
- Where did you grow up?

Google Questions

- What is your primary frequent flier number?
- What is your library card number?
- What was your first phone number?
- What was your first teacher’s name?

Microsoft Questions

Windows Live

Hotmail

The efficient way to do email

- Mother’s birthplace
- Best childhood friend
- Favorite teacher
- Favorite historical person
- Grandfather’s occupation

Yahoo! Questions

- Where did you meet your spouse?
- What was the name of your first school?
- Who was your childhood hero?
- What is your favorite pastime?
- What is your favorite sports team?
- What is your father’s middle name?
- What was your high school mascot?
- What make was your first car or bike?
- What is your pet’s name?

Findings

- Many bogus answers (e.g., 13% for hotmail)
- After 3-6 months, 20% of answers forgotten
- Answer statistically guessable if in top 5 guesses for that question from other participants (excluding partner)
  - 13% total statistically guessable
- 17-28% guessed by acquaintance

NIST recommendations

- Don’t use secret questions

Emailed password

- new temporary password
  - one-time password: valid for single use only, maybe limited duration

- **Assumes:** attacker is unlikely to have compromised your email account
- **Assumes:** email service correctly authenticates you

Password lifecycle

1. **Create:** user chooses password
2. **Store:** system stores password with user identifier
3. **Use:** user supplies password to authenticate
4. **Change/recover/reset:** user wants or needs to change password

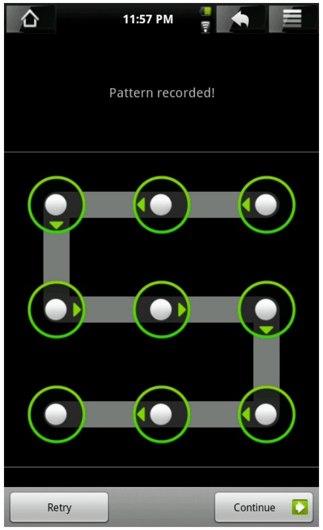
Beyond passwords?

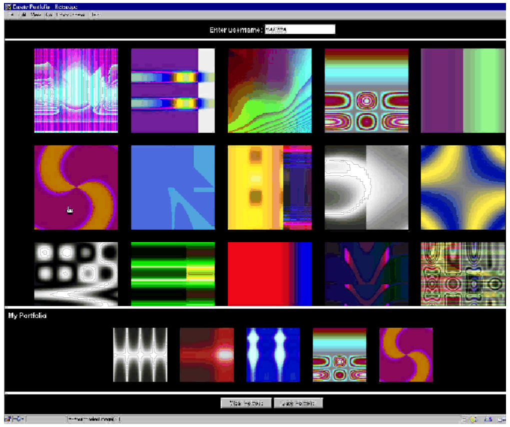
- Passwords are tolerated or hated by users
- Passwords are plagued by security problems
- **Can we do better?**
- Criteria:
  - Security
  - Usability
  - Deployability

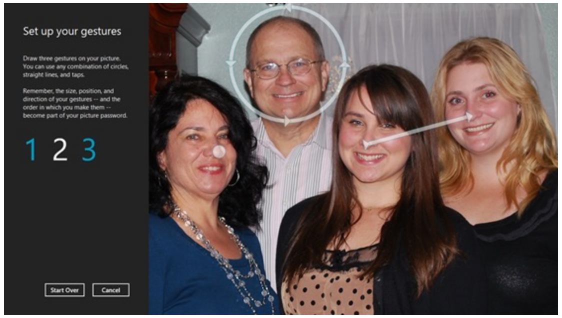
Schemes to replace passwords

- Graphical
- Cognitive
- Visual cryptography

- Password managers
- Single Sign-On
- Two-factor authentication






Set up your gestures

Draw three gestures on your picture. You can use any combination of circles, straight lines, and taps.

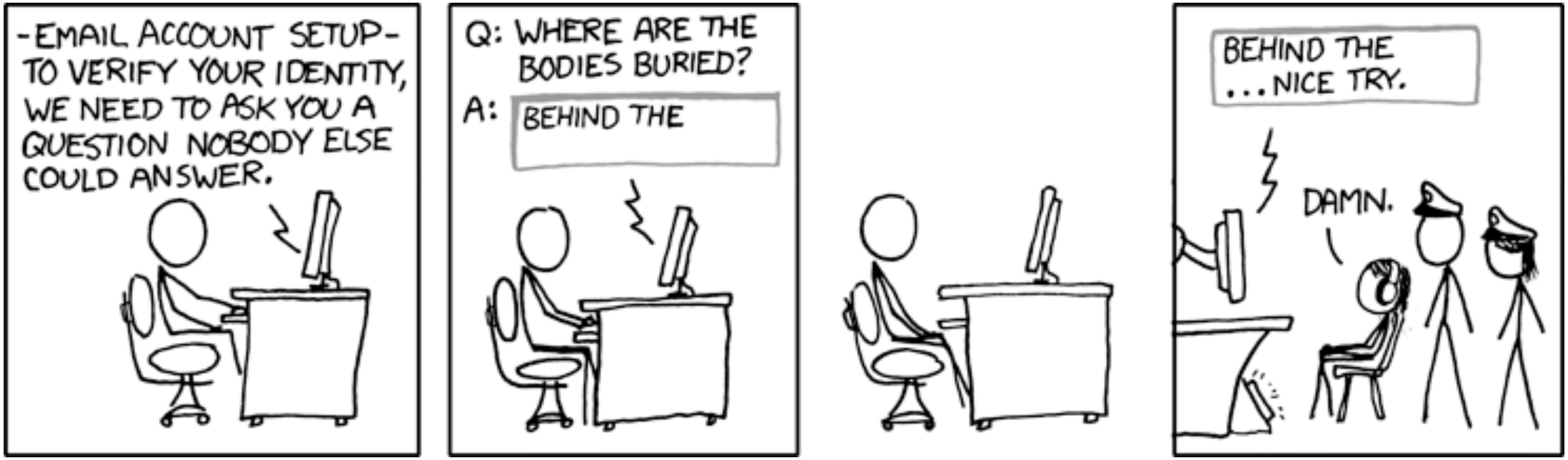
Remember, the size, position, and direction of your gestures -- and the order in which you make them -- become part of your picture password.

- **Passwords are here to stay, for now**

A5

- Password Readings
- Project IRB Proposal

Something you know


-EMAIL ACCOUNT SETUP-
TO VERIFY YOUR IDENTITY, WE NEED TO ASK YOU A QUESTION NOBODY ELSE COULD ANSWER.
Q: WHERE ARE THE BODIES BURIED?
A: BEHIND THE
BEHIND THE
...NICE TRY.
DAMN.