13- Passwords

Lorrie Cranor

March 1, 2017

05-436 / 05-836 / 08-534 / 08-734 / 19-534 / 19-734
Usable Privacy and Security

Carnegie Mellon University
CyLab

institute for SOFTWARE RESEARCH

Engineering & Public Policy

CyLab Usable Privacy & Security Laboratory
HTTP://CUPS.CS.CMU.EDU

Today's class

- Studying for the midterm
- The continuing quest for secure and usable passwords

Studying for the midterm

- Review quizzes (and missed readings)
- Review lecture notes 2-8 and 10-13
  - Terminology and definitions
  - Questions, reasons, examples, etc., especially those discussed in class
- Review homeworks
- Midterm will be a mix of recognition, recall, and applying what you have learned

The continuing quest for secure and usable passwords

Lorrie Faith Cranor

Carnegie Mellon University
CyLab

institute for SOFTWARE RESEARCH

Engineering & Public Policy

privacy ENGINEERING

Cylab Usable Privacy & Security Laboratory
HTTP://CUPS.CS.CMU.EDU

The CMU passwords research team (2014)

Gates predicts death of the password

Traditional password-based security is headed for extinction, says Microsoft's chairman, because it cannot "meet the challenge" of keeping critical information secure.

Security

February 25, 2004
1:27 PM PST

by Munir Kotadia

SAN FRANCISCO--Microsoft Chairman Bill Gates predicted the demise of the traditional password because it cannot "meet the challenge" of keeping critical information secure. Gates, speaking at the RSA Security conference here on Tuesday, said: "There is no doubt that over time, people are going to rely less and less on passwords. People use the same password on different systems, they write them down and they just don't meet the challenge for anything you really want to secure."

Data and computer security

Will increasing cyber attacks spell the end of username and password security?

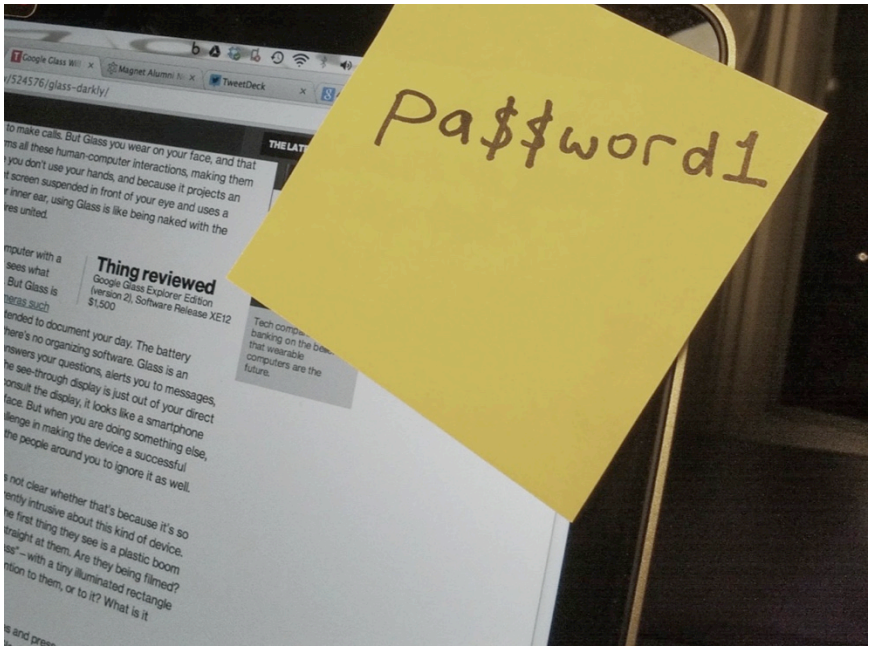
Andy Meek in Memphis

Tuesday 10 February 2015 09.09 EST

Paul Kocher, president and chief scientist at Cryptography Research, a division of Rambus, says the “reports of the death of passwords have been greatly exaggerated”.

Password vulnerabilities

- Shoulder-surfing attacks
- Online attacks
- Offline attacks



Recent password breaches

	Affected users	Date
Gawker	1,300,000	2010
Sony	25,000,000	2011
LivingSocial	50,000,000	2013
Sega	1,300,000	2011
Booz Allen Hamilton	90,000	2011
Evernote	50,000,000	2013
Drupal	1,000,000	2013
Ashley Madison	32,000,000	2015

How offline attacks work

- Passwords are leaked hashed or encrypted
- Attackers guess, hash, see whether it matches
- Billions of guesses per second
- Good cracking algorithms guess high-probability passwords first
- Good hash/salt schemes slow guessing

Guessing Strategy

Dumb attacker	Smart attacker
aaaaaaaa	123456789
aaaaaaab	password
aaaaaaac	iloveyou
aaaaaaad	princess
aaaaaaae	12345678
…	…

Smart attacker uses data to crack passwords more quickly

Attackers exploit password reuse

- Guessing leaked passwords doesn't help attacker who already has access to system
- But people reuse passwords
- So attackers guess leaked passwords and try them on other systems

How can we help users pick passwords that are easy to remember, but hard for an attacker to guess?

Password Requirements

Adhere to the following password requirements, when selecting your Andrew account passwor

Must Contain

- At least 8-characters.
- At least one uppercase alphabetic character (e.g., A-Z).
- At least one lowercase alphabetic character (e.g., a-z).
- At least one number (e.g., 0-9).
- At least one special character (e.g., ~!@#$%^&*()_-+=).

Cannot Contain

- Known information (i.e., first name, last name, Andrew userID, date of birth, 9-digit Carnegie Mellon ID number, SSN, job title).
- Four or more occurrences of the same character (e.g., aaaa, 2222, a123a345a678a).*
- A word that is found in a standard dictionary.*
  Note: Verify that the letters within your password do not spell a word after you remove any non-alphabetical or special characters. The system checks all of the letters of the password together. Details...

This requirement does not apply to Andrew account passwords that are more than 19 characters in length (e.g., passphrase).

Additional Policies

- Last five passwords cannot be used.
- Cannot be changed more than four times in a day.

NIST Special Publication 800-63-1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Electronic Authentication Guideline

Recommendations of the National Institute of Standards and Technology

William E. Burr
Donna F. Dodson
Elaine M. Newton
Ray A. Perlner
W. Timothy Polk
Sarbari Gupta
Emad A. Nabbus

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

"Unfortunately, **we do not have much data** on the passwords users choose under particular rules.... NIST would like to obtain more data on the passwords users actually choose, but … system administrators are understandably reluctant to reveal password data to others."

Outline

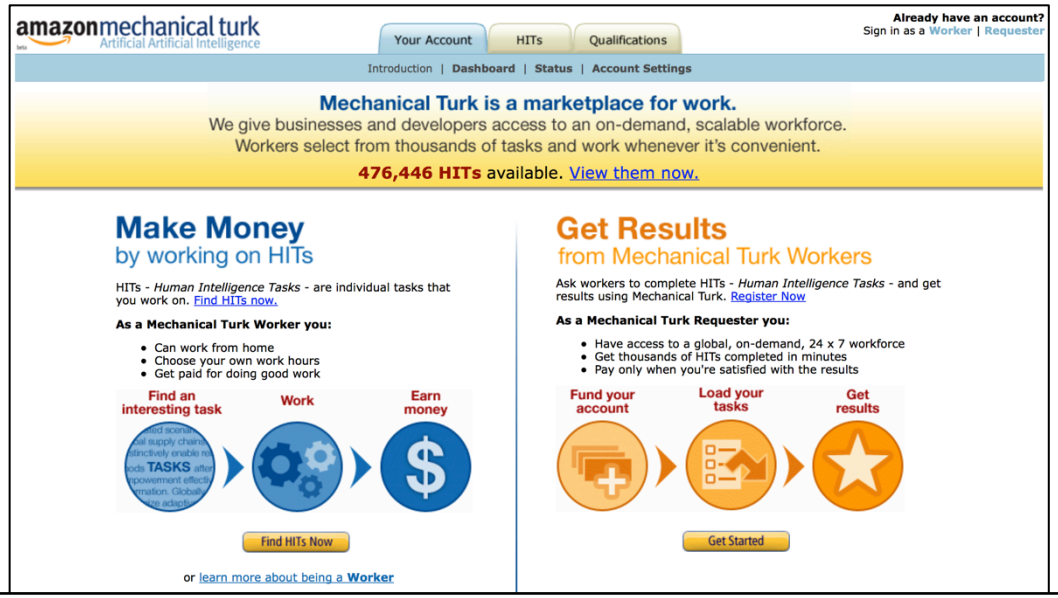
- **Password study methods (applied to CMU passwords) [CCS 2013]**
- Finding good password-composition policies
- Password meters, feedback, and guidance
- Passphrases
- Perceptions
- Expiry
- Conclusions

How can you get passwords to study?

- Passwords created for experiments
  - Lab studies
  - Online studies
- Real passwords
  - Stolen passwords
  - Surveys
  - Legitimate access to actual passwords

Large-scale online experiments

- Amazon MTurk for recruitment and payment
- Enabled study of 40,000+ participants
- Email participants without collecting personally identifiable information



Methodology

- Participant tasks
  - Create password under a randomly assigned condition
  - Take a survey
  - Recall password
  - Return two days later to recall password and take another survey
- Data
  - Plaintext passwords
  - Self-reported data about sentiment
  - Measured and self-reported password behavior

Usability metrics

- Creation attempts and time
- Recall attempts
- Reported sentiment
- Write-down rate
- Study drop-out rate

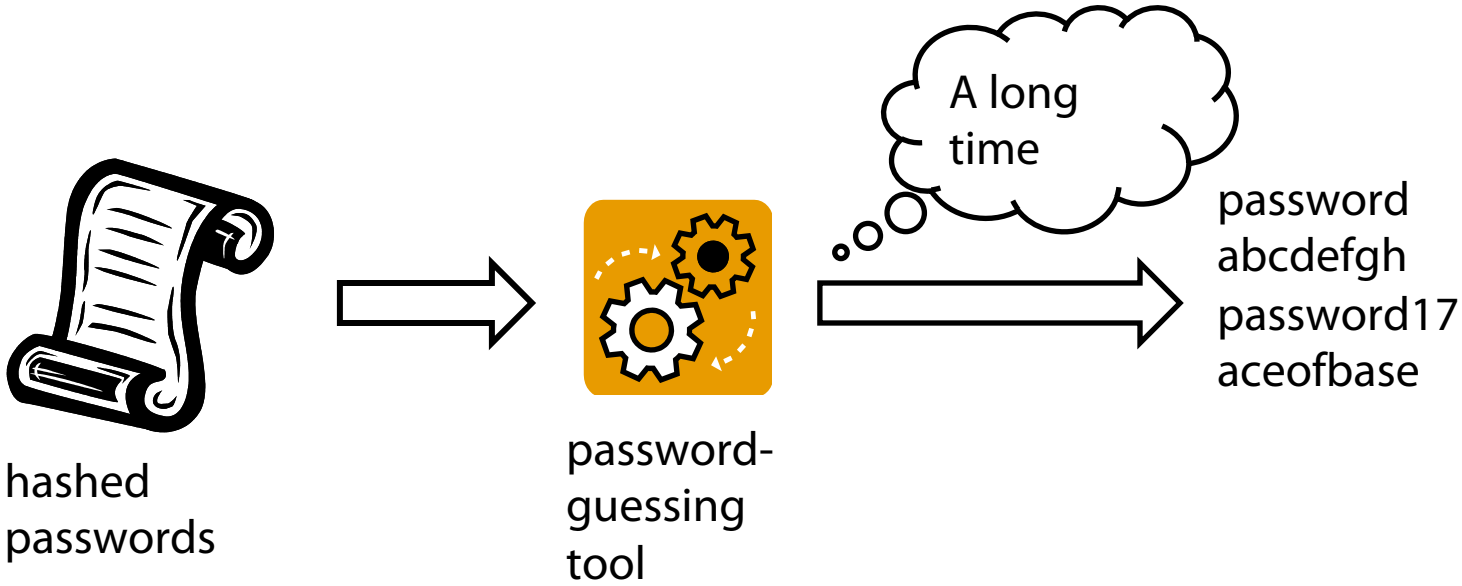
Strength metric: Guessability

- How many guesses to reach each password?
  - Subject to guessing algorithm and training data
- Result: guess number or **beyond the cutoff**
  - Cutoff = 380 trillion guesses (runs in about 1 day)

Example:

Password	Guess number
12345678	4
Password178	1.4×10^6
jn%fKXsl!8@Df	Beyond cutoff

Measuring Guessability

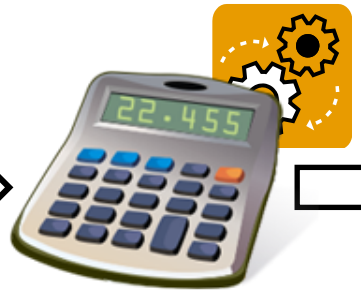


Traditional approach: Run cracking tool

Measuring Guessability

password
abcdefgh
password17
aceofbase
jnfksl834df

plaintext passwords



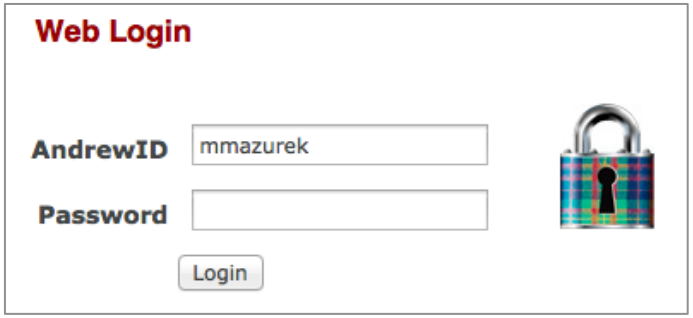
password-guessing *calculator*

password: 2
abcdefgh: 19546
password17: 1.4×10^6
aceofbase: 3×10^4
jnfksl834df: never

Our approach:
Calculate guess numbers directly

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)

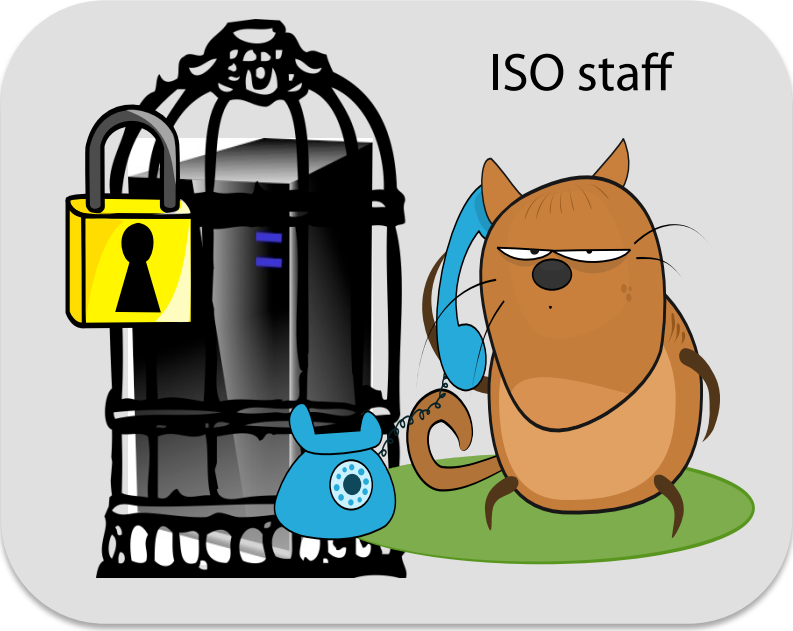


Other CMU data

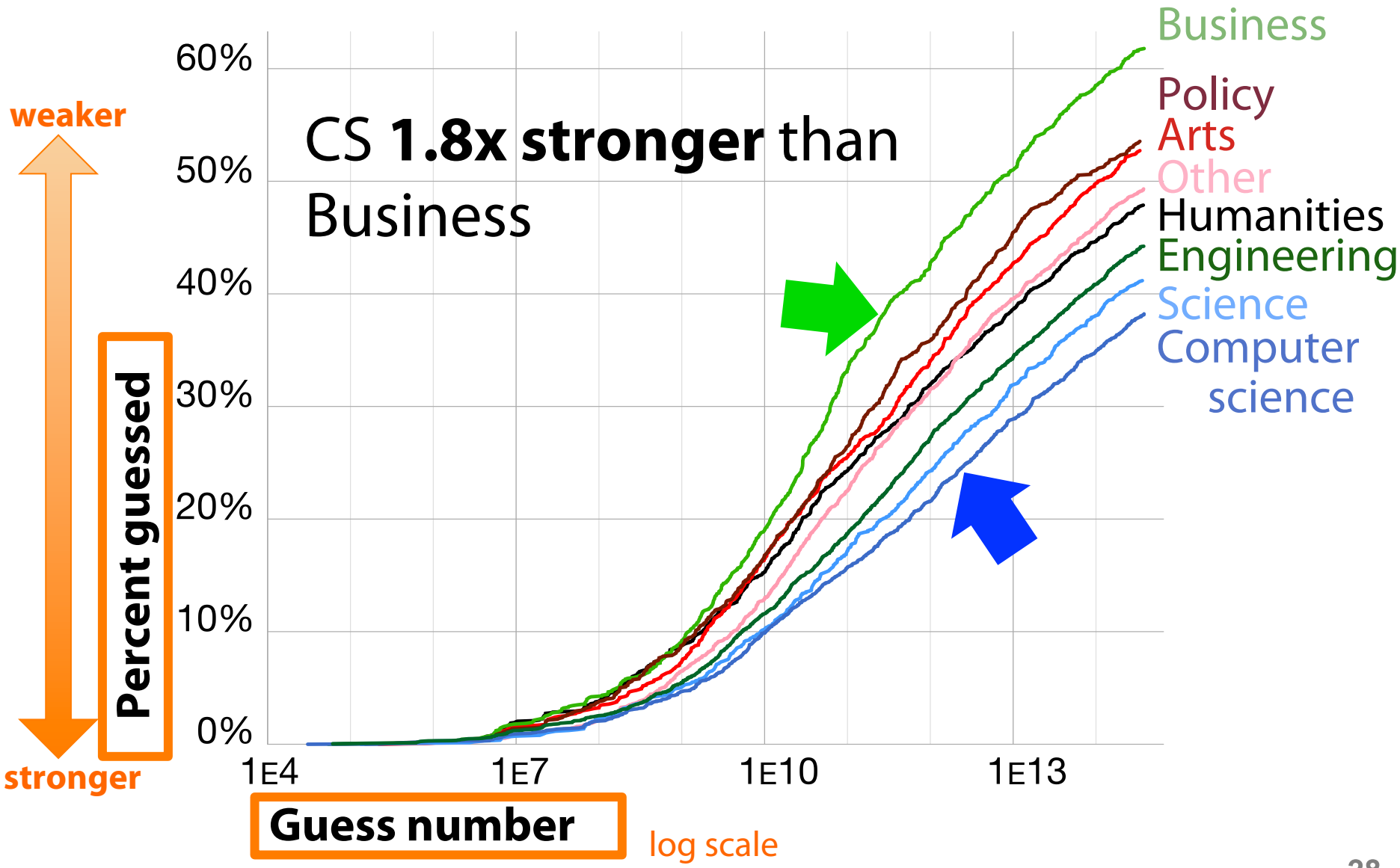
- Web authentication logs (7 months)
  - Login rate, error rate, etc.
  - 1 to 3,595 logins per user (median 55)
- Personnel records: age, gender, affiliation, etc.
- Survey administered after password change
  - Why did you change your password?
  - Password creation strategies
  - 694 participants

Handling real data securely

- Legacy system stored passwords reversibly
- ISO personnel audited and ran code on isolated machine
- Aggregated outputs only, reviewed by ISO director



College affiliation

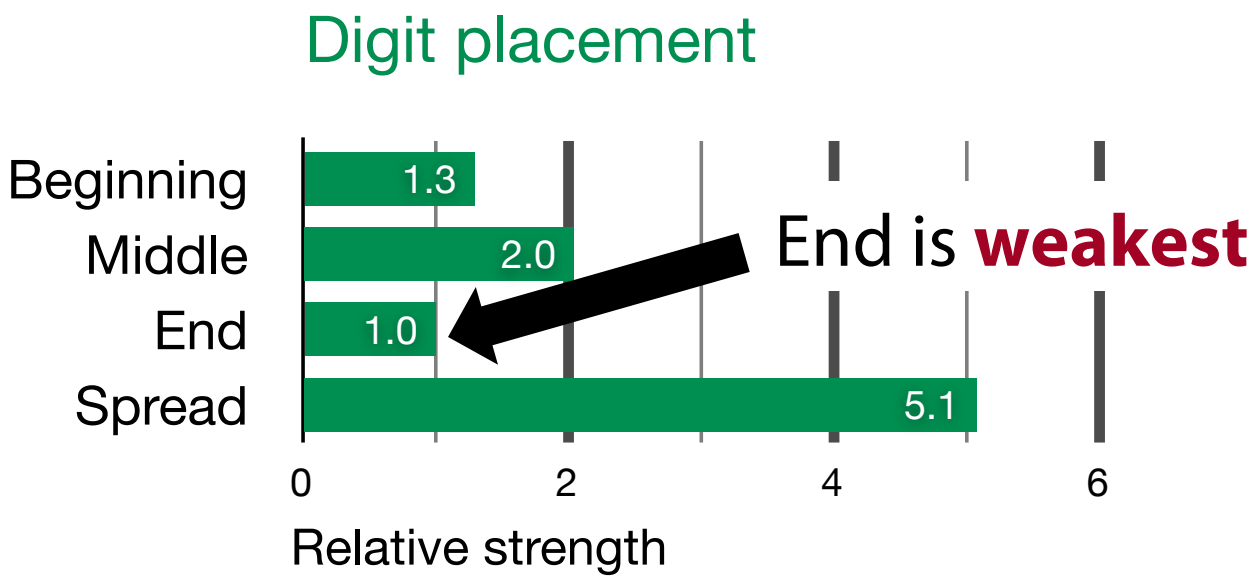


Other demographic results

- No effect for faculty/ student/staff or age
- Men **1.1x stronger** passwords than women

Password composition

- Each added character **1.4x stronger**
- Common locations for digits less helpful



- Similar results for symbols, uppercase

Survey results

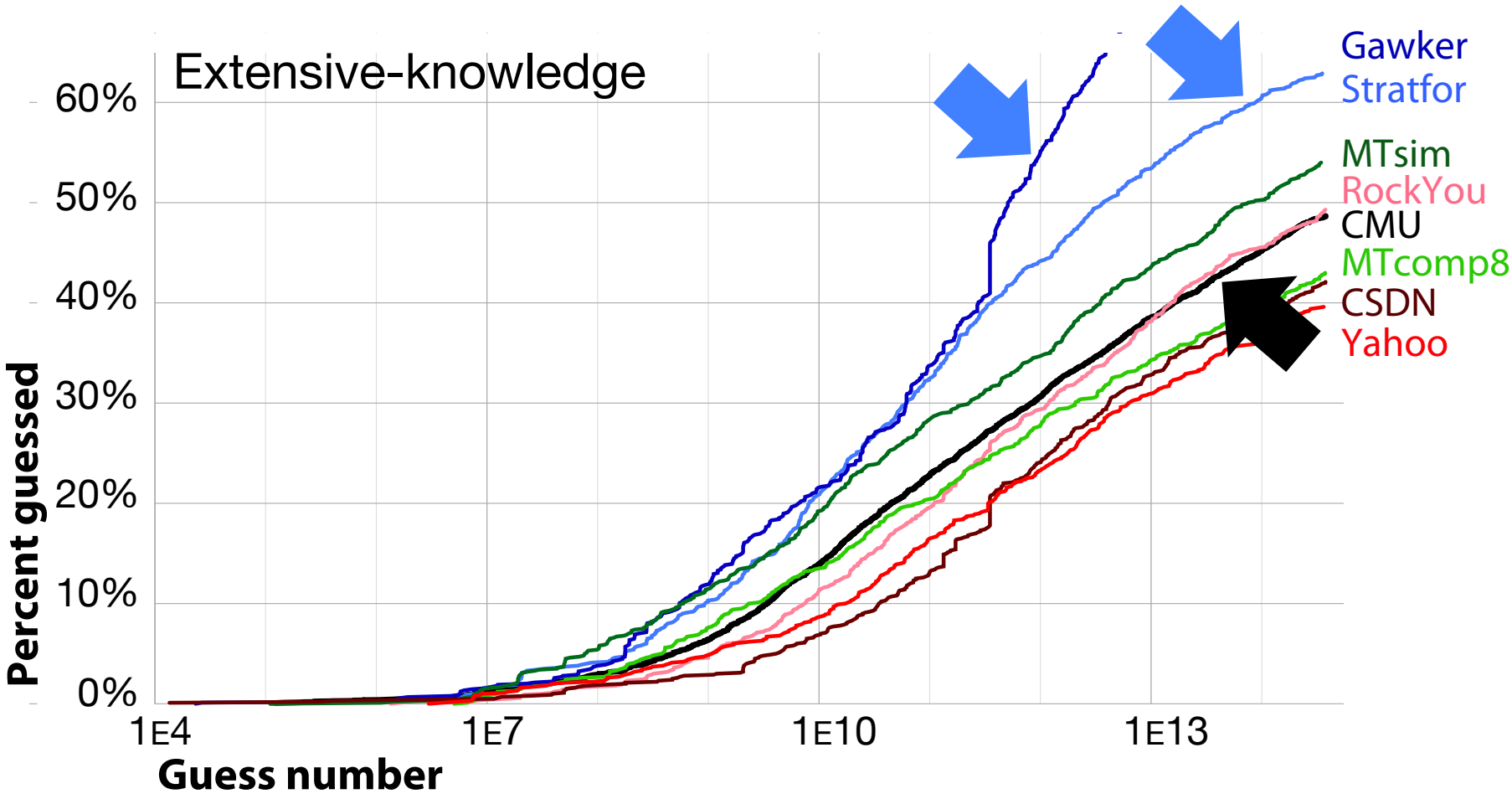
- Password creation was annoying: **1.5x weaker**

Comparing password sets

- Real CMU passwords
- Online studies
  - Similar to CMU password requirements
- Leaked: plaintext

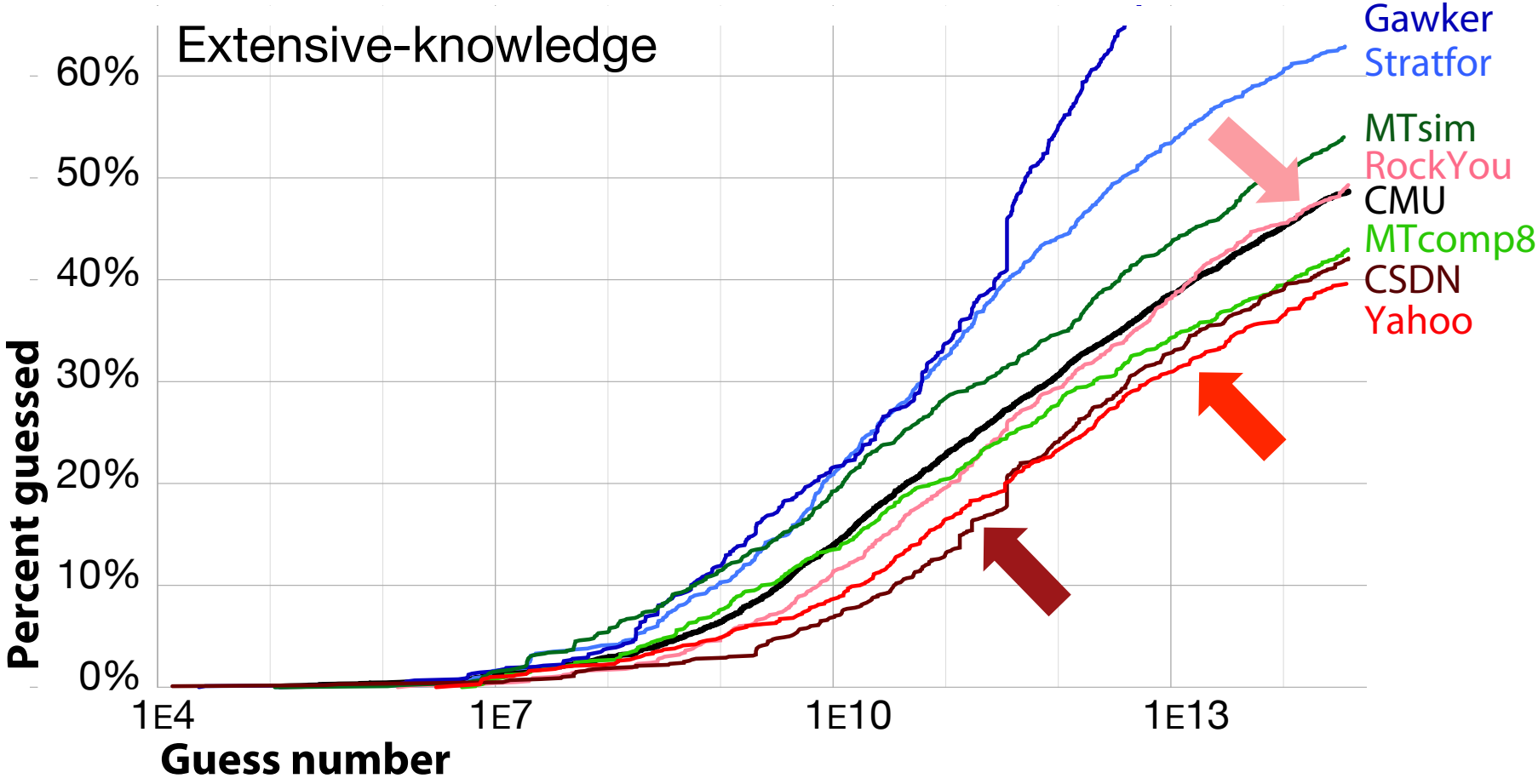
Used subset of leaked passwords **conforming** to CMU policy

Comparing sets – Guessability



Leaked hashed/cracked: Very easy to guess

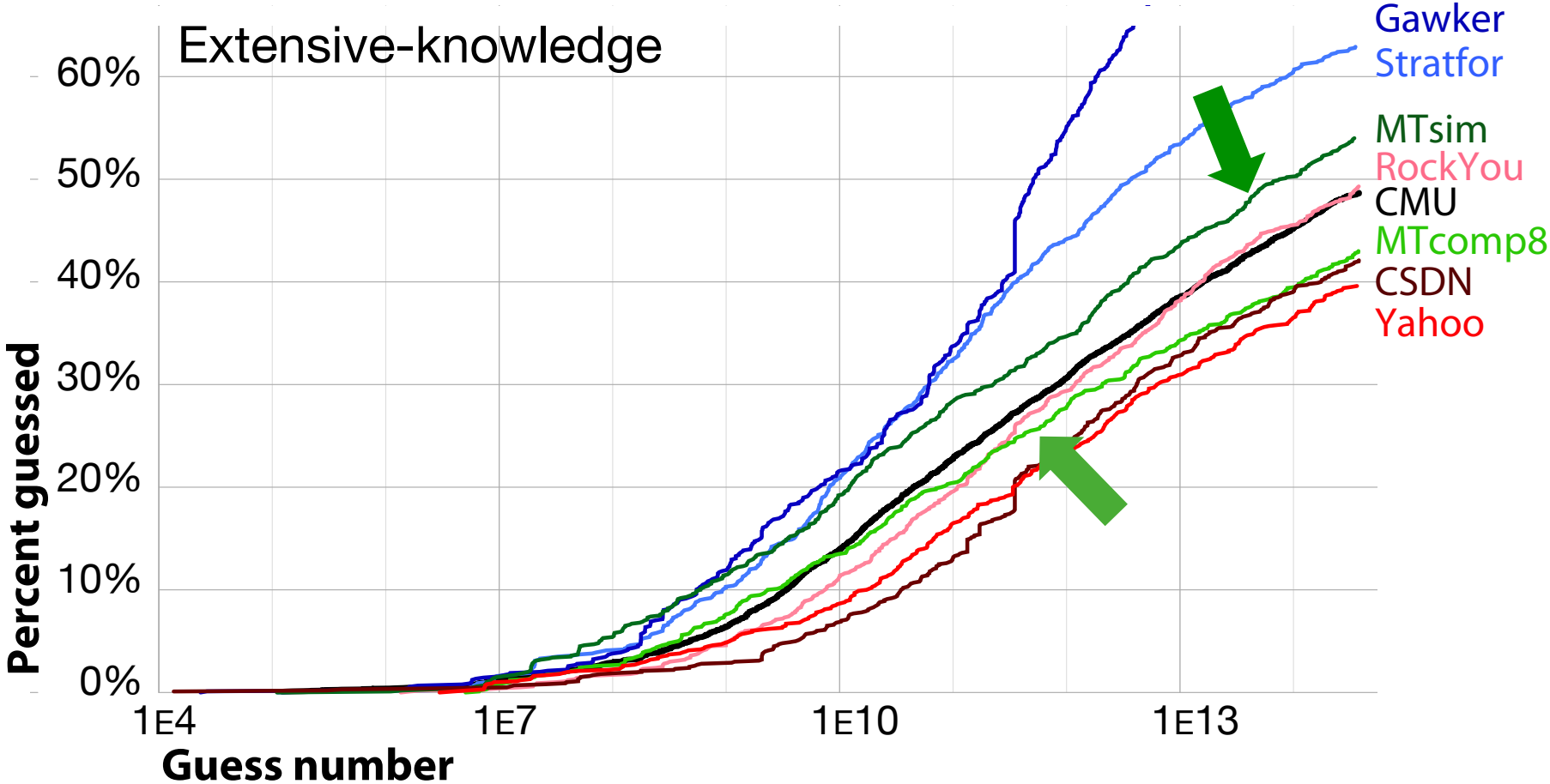
Comparing sets – Guessability



Leaked plaintext:

RockYou close to CMU, others much tougher

Comparing sets – Guessability



Online studies: Closest across all metrics

Online study passwords FTW!

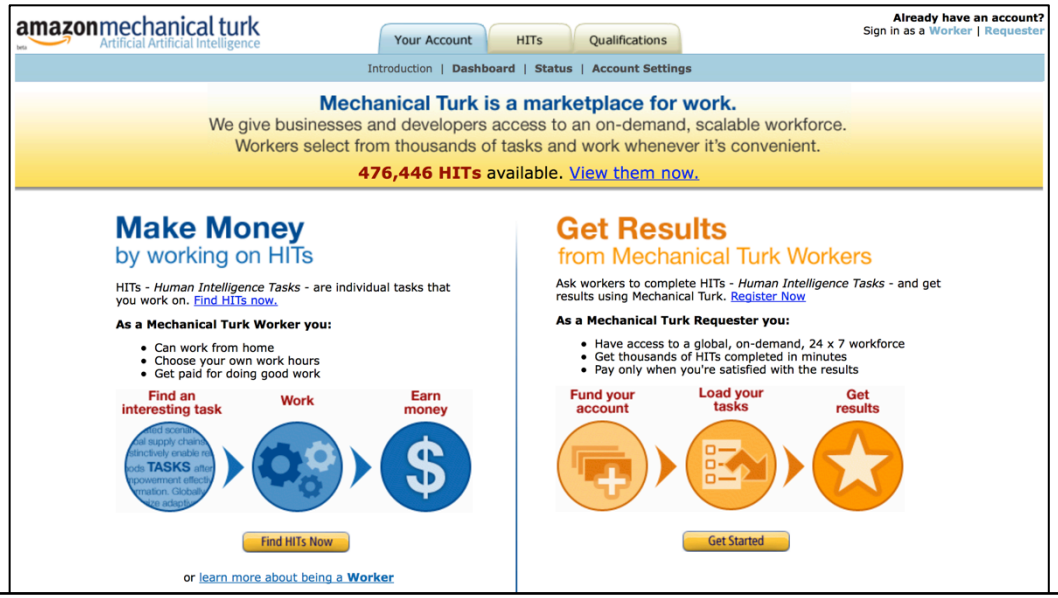
- Real passwords are ideal to study, but hard to obtain and handle securely
- Subsets from leaked datasets are hit and miss
- Passwords from online studies are consistently closer to real passwords

Outline

- Password study methods
- **Finding good password-composition policies** [CHI 2011, IEEE SP 2012, CHI 2014]
- Password meters, feedback, and guidance
- Passphrases
- Perceptions
- Expiry
- Conclusions

Online studies

- Mechanical Turk studies
- Evaluated many password policies for strength and usability



Condition: Basic8

password

Condition: Dictionary8

sapsword

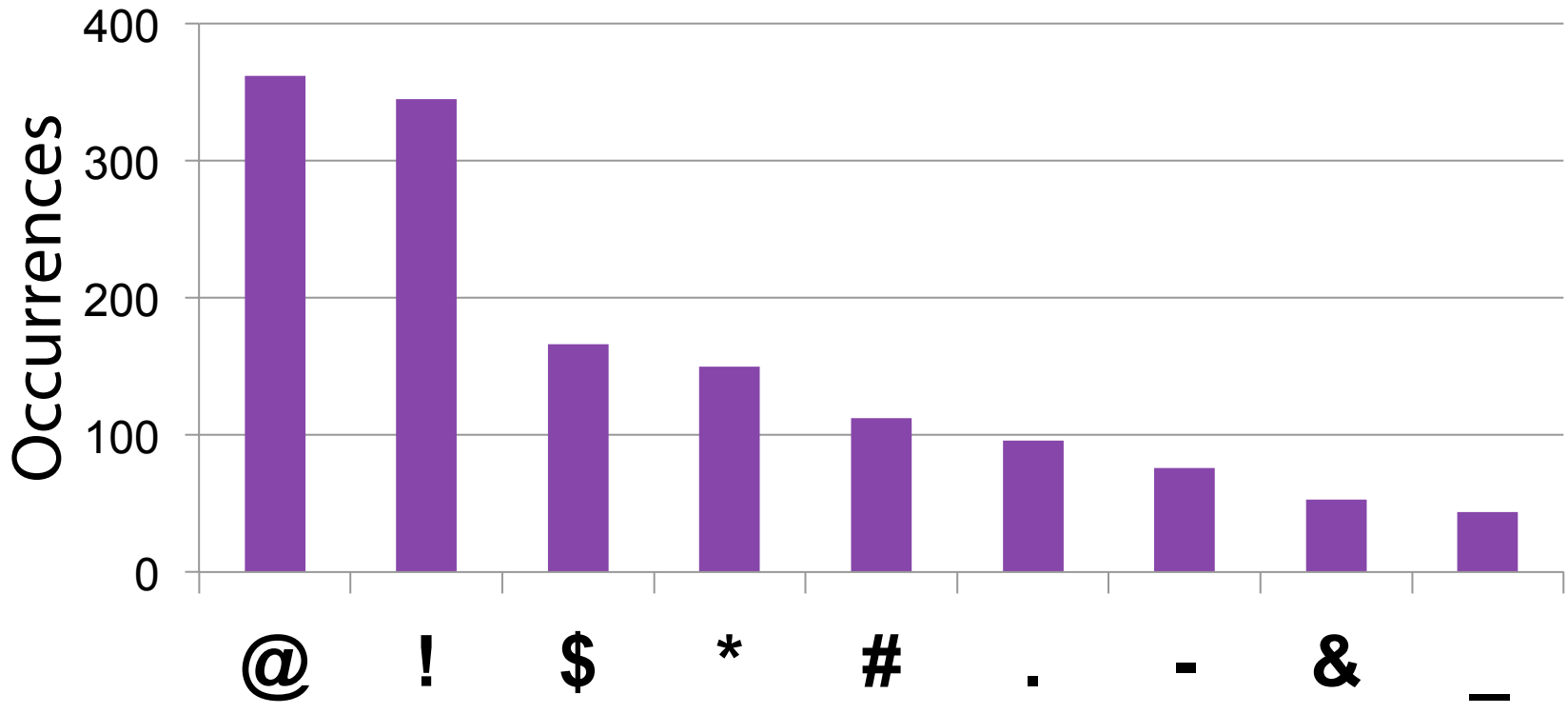
Condition: Comprehensive8

Sapsword1!

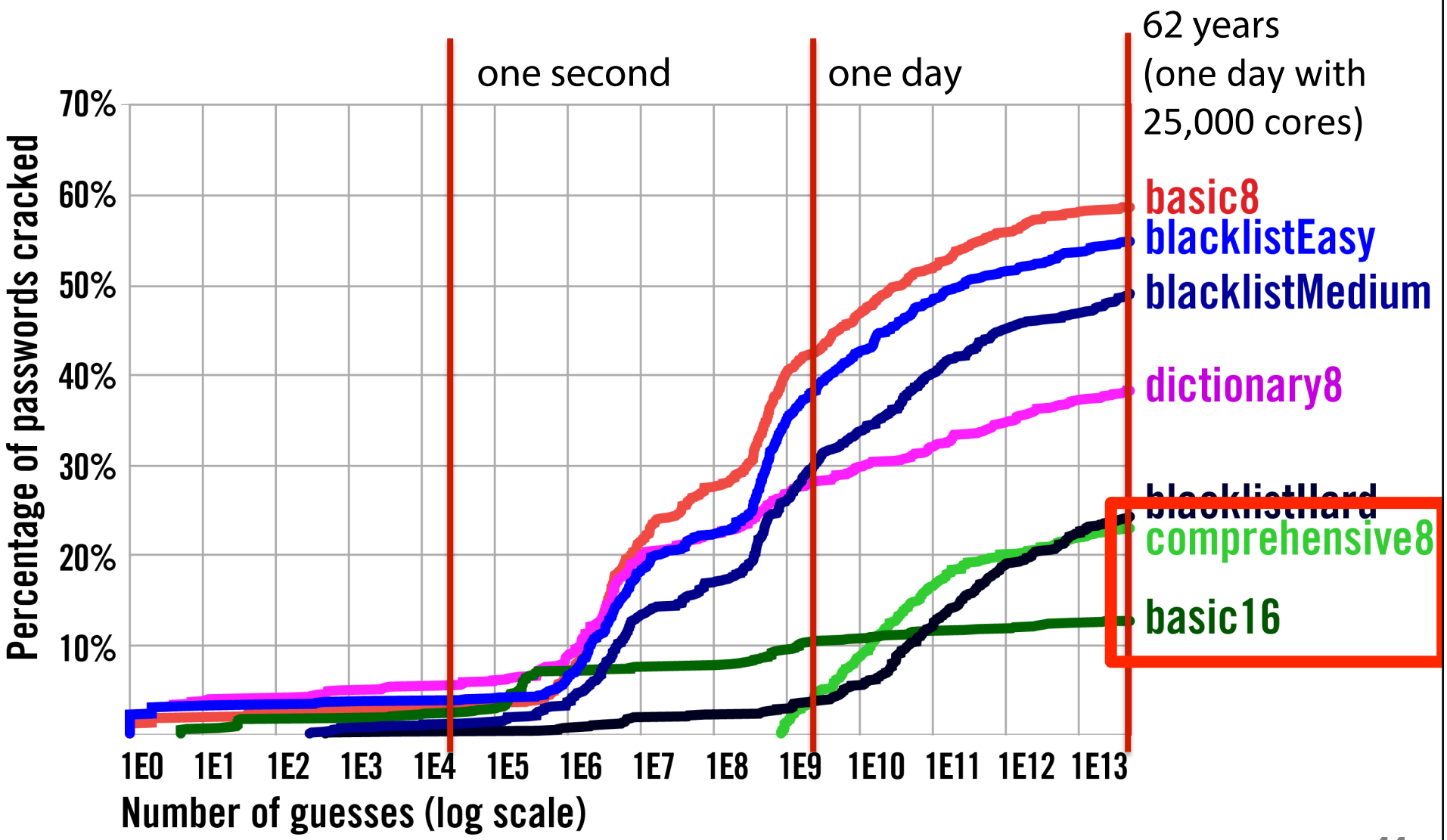
Condition: Basic16

passwordpassword

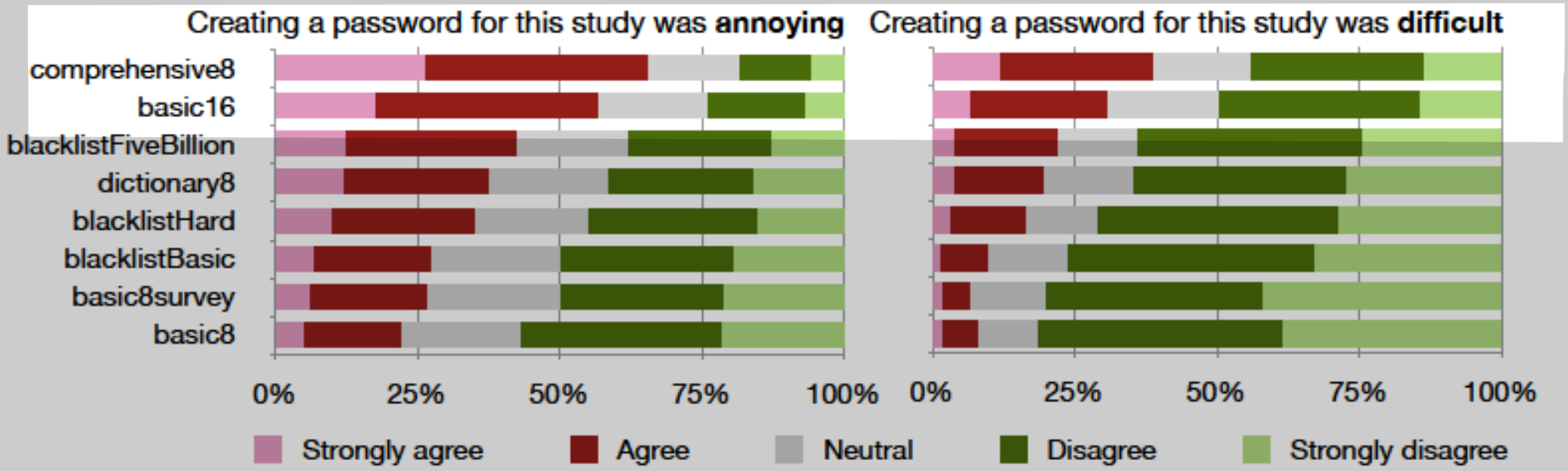
Symbols in passwords



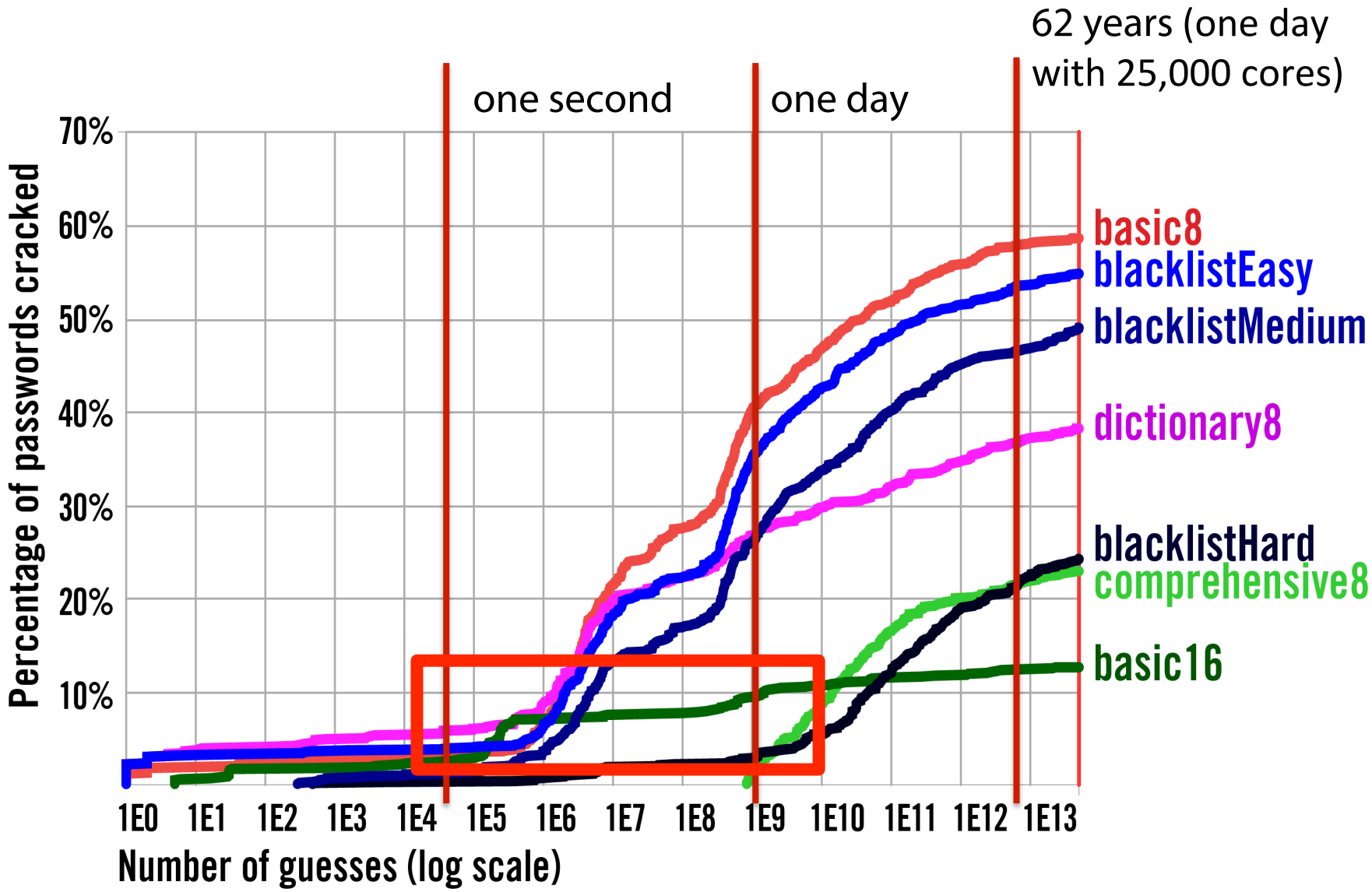
Password strength



Usability


Creating a password for this study was **annoying**
Creating a password for this study was **difficult**
comprehensive8
basic16
blacklistFiveBillion
dictionary8
blacklistHard
blacklistBasic
basic8survey
basic8
0%
25%
50%
75%
100%
Strongly agree
Agree
Neutral
Disagree
Strongly disagree

Basic16 not so good early on



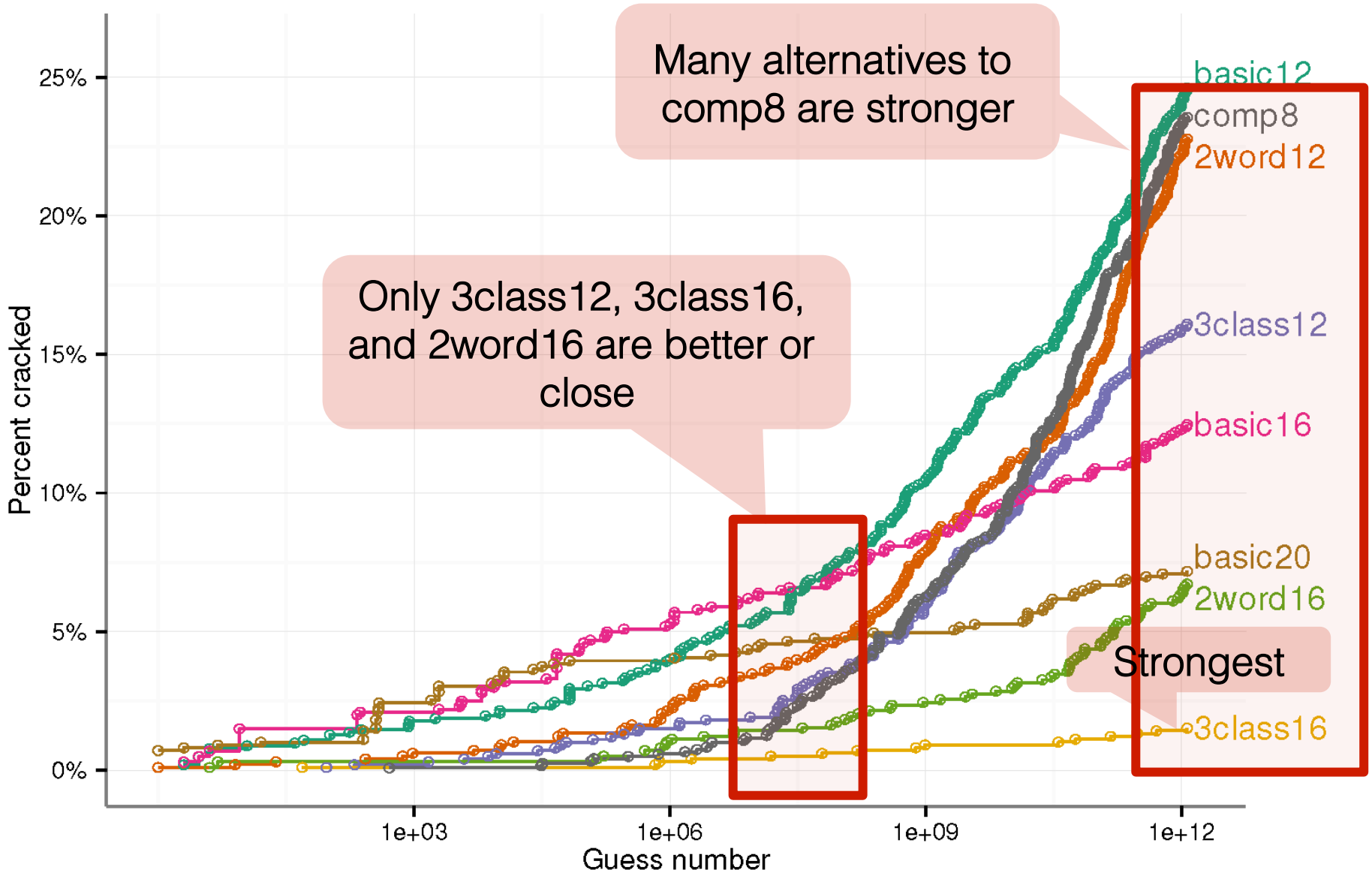
Easily guessed basic16

```
Baseballbaseball
1234567890987654
xxxxxxxxxxxxxxxx
```

Require length plus?

- Goal: Good combination of security and usability
  - At least as secure as comp8 (CMU passwords)
  - As usable as possible
- Policies tested
  - Basic: at least 12, 16, 20 chars
  - 2-word: at least 12 or 16 chars + 2 words
  - 3-class: at least 12 or 16 chars + 3 char classes
  - comp8: reference policy

Guessability results



Usability

	Mean creation attempts	Password entry time (seconds)	% Participants who stored password
comp8	2.3	13.2	56.9
3class12	**1.6**	14.8	54.9
3class16	**1.8**	**16.2**	60.2
2word16	2.0	14.6	51.3

Significantly better than comp8

Significantly worse than comp8

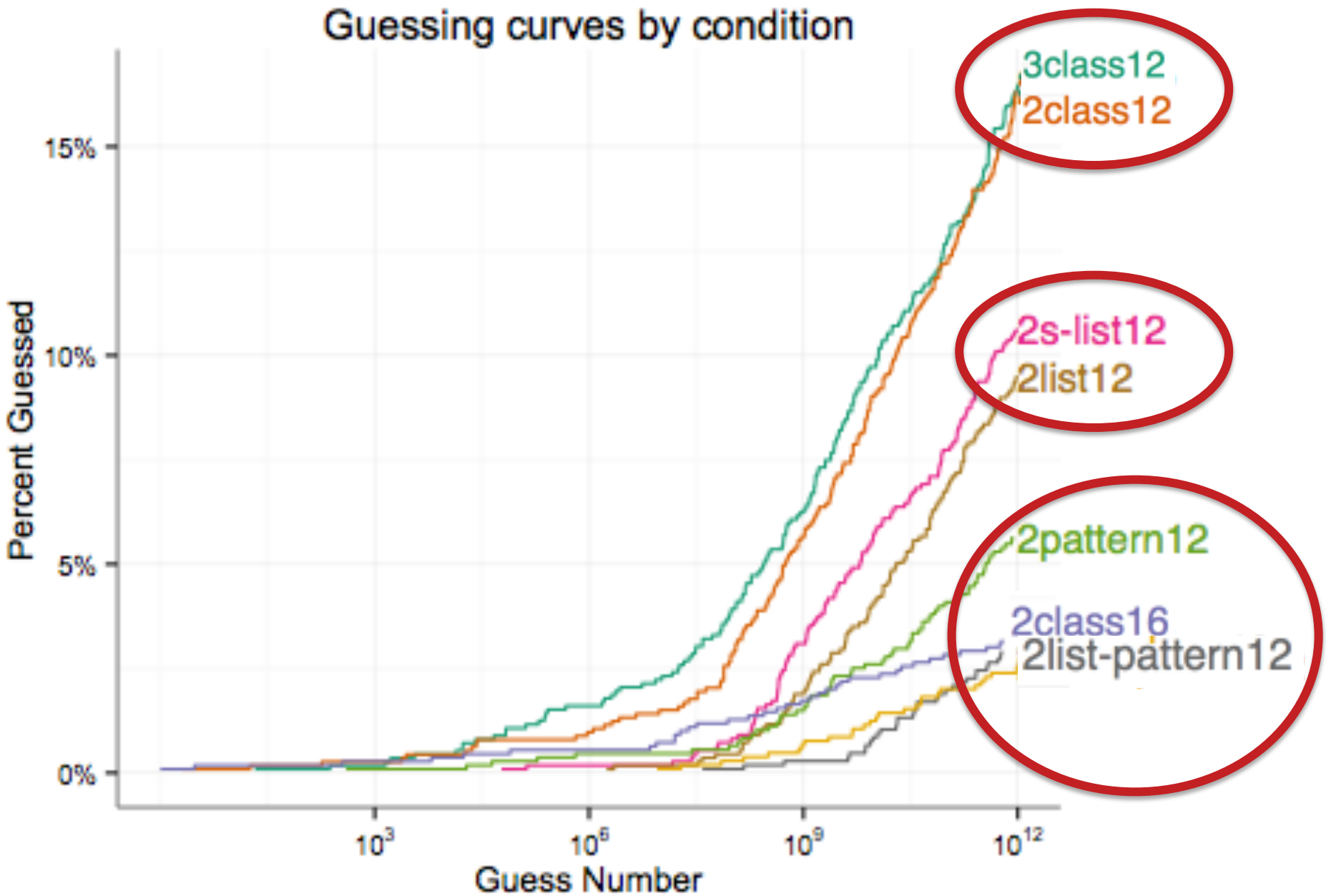
Follow-up study

- 3class12 was good… can we make it better?
- 2class12 might be more usable
- 2class16 might be stronger
- What if we require password to begin and end with lowercase?
- What if we add a blacklist requirement?
- What if we add both blacklist and pattern?

2list12

Do not include:

- *123!*, *amazon*, *character*, *monkey*, *number*, *survey*, *this*, *turk*
- Any year between *1950* and *2049*
- The same character four or more times in a row
- Any four consecutive characters from *password*
- Any four sequential digits (e.g., *5678*)
- Any four sequential letters in the alphabet (e.g., *wxyz*)
- Any four consecutive characters on the keyboard (e.g., *wsxc*)


Guessing curves by condition
3class12
2class12
2s-list12
2list12
2pattern12
2class16
2list-pattern12
15%
10%
5%
0%
Percent Guessed
10^3
10^6
10^9
10^{12}
Guess Number

53

	creation attempt	% creation difficult	% creation annoy	% recall difficult	% stored pass-word
3class12	**1.6**	**24.1**	**57.3**	**36.0**	**52.7**
2class12	1.6	25.1	54.0	35.4	50.8
2class16	1.8	40.1	70.0	38.5	56.7
2list12	1.8	32.8	61.4	35.7	59.6
2s-list12	1.9	27.4	57.9	32.6	56.5
2pattern12	2.4	46.8	74.7	47.4	61.7
2list-pattern12	2.4	50.0	77.3	49.1	64.0
2s-list-pattern12	2.6	50.2	76.0	49.0	67.5

Findings

- 3class12 and 2class12 almost identical
- Pattern requirement made passwords stronger, but also made creation and recall harder
- Blacklist requirement made passwords stronger, made creation but not recall harder

N-gram cracking

- Collect N-grams from various corpora
  - Google, books, IMDB, Twitter, lyrics, Wikipedia
- Provide N-gram information to cracking tools
- We can crack more passwords now

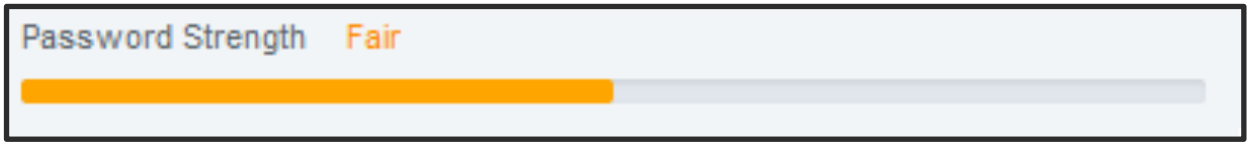
3class12 examples	**3class16 examples**
ineedca$hn0w Applesaucecake60	Mybonnieliesovertheocean. imsexyandiknowit#01

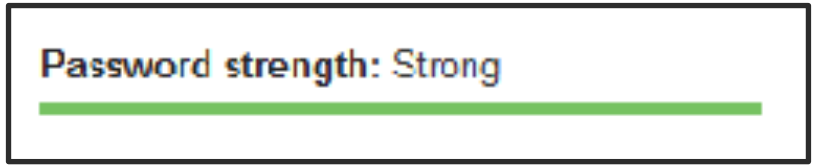
Outline

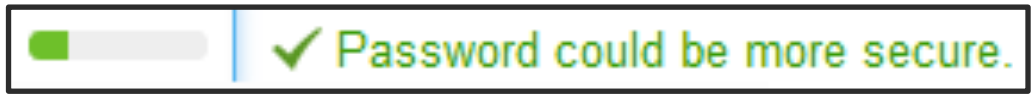
- Password study methods
- Finding good password-composition policies
- **Password meters, feedback, and guidance** [USENIX SEC '12] [CHI 2015]
- Passphrases
- Perceptions
- Expiry
- Conclusions

Password Meters …

… come in all shapes and sizes







Conditions with Visual Differences

Type new password: use

8-character minimum; case sensitive

Baseline meter

Bad. Consider adding a digit or making your password longer.

Three-segment

Bad. Consider adding a digit or making your password longer.

Green

Bad. Consider adding a digit or making your password longer.

Tiny

Bad. Consider adding a digit or making your password longer.

Huge

Bad. Consider adding a digit or making your password longer.

No suggestions

Bad.

Text-only

Bad. Consider adding a digit or making your password longer.

Conditions with Visual Differences

Type new password: usen

8-character minimum; case sensitive

Baseline meter

Bad. Consider adding a digit or making your password longer.

Three-segment

Bad. Consider adding a digit or making your password longer.

Green

Bad. Consider adding a digit or making your password longer.

Tiny

Bad. Consider adding a digit or making your password longer.

Huge

Bad. Consider adding a digit or making your password longer.

No suggestions

Bad.

Text-only

Bad. Consider adding a digit or making your password longer.

Conditions with Visual Differences

Type new password: usenIX

8-character minimum; case sensitive

Baseline meter

Fair. Consider adding a digit or making your password longer.

Three-segment

Fair. Consider adding a digit or making your password longer.

Green

Fair. Consider adding a digit or making your password longer.

Tiny

Fair. Consider adding a digit or making your password longer.

Huge

Fair. Consider adding a digit or making your password longer.

No suggestions

Fair.

Text-only

Fair. Consider adding a digit or making your password longer.

Conditions with Visual Differences

Type new password: usenIX$

8-character minimum; case sensitive

Baseline meter

Good. Consider adding a digit or making your password longer.

Three-segment

Good. Consider adding a digit or making your password longer.

Green

Good. Consider adding a digit or making your password longer.

Tiny

Good. Consider adding a digit or making your password longer.

Huge

Good. Consider adding a digit or making your password longer.

No suggestions

Good.

Text-only

Good. Consider adding a digit or making your password longer.

Conditions with Visual Differences

Type new password: usenIX$e5

8-character minimum; case sensitive

Baseline meter

Excellent!

Three-segment

Excellent!

Green

Excellent!

Tiny

Excellent!

Huge

Excellent!

No suggestions

Excellent!

Text-only

Excellent!

Conditions with Visual Differences

Type new password: usenIX$e5

8-character minimum; case sensitive

Baseline meter

Excellent!

Three-segment

Excellent!

Green

Excellent!

Tiny

Excellent!

Huge

Excellent!

No suggestions

Excellent!

Text-only

Excellent!

Bunny Condition

A strong password helps prevent unauthorized access to your email account.
The stronger your password, the faster Bugs Bunny dances!

Type new password:

8-character minimum; case sensitive

Password strength: Please enter a password in the box above.

Retype new password:

Make my password expire every 72 days.

Save

Conditions with Scoring Differences

Type new password: usenIX

8-character minimum; case sensitive

Baseline meter

Fair. Consider adding a digit or making your password longer.

Half-score

Bad. Consider adding a digit or making your password longer.

One-third-score

Bad. Consider adding a digit or making your password longer.

Nudge-B^{16}

Bad. Consider making your password longer.

Nudge-Comp^{8}

Fair. Consider adding a digit or making your password longer.

Conditions with Scoring Differences

Type new password: usenlX$e5

8-character minimum; case sensitive

Baseline meter

Excellent!

Half-score

Poor. Consider adding a different symbol or making your password longer.

One-third-score

Bad. Consider adding a different symbol or making your password longer.

Nudge-B^{16}

Poor. Consider making your password longer.

Nudge-Comp^{8}

Excellent!

Conditions with Scoring Differences

Type new password: usenIX$e5WHYis

8-character minimum; case sensitive

Baseline meter

Excellent!

Half-score

Fair. Consider adding a different symbol or making your password longer.

One-third-score

Poor. Consider adding a different symbol or making your password longer.

Nudge-B^{16}

Good. Consider making your password longer.

Nudge-Comp^{8}

Excellent!

Conditions with Scoring Differences

Type new password: usenIX$e5WHYismyP4$$

8-character minimum; case sensitive

Baseline meter

Excellent!

Half-score

Good. Consider adding a different symbol or making your password longer.

One-third-score

Poor. Consider adding a different symbol or making your password longer.

Nudge-B^{16}

Excellent.

Nudge-Comp^{8}

Excellent!

Conditions with Scoring Differences

Type new password: usenIX$e5WHYismyP4$$word99

8-character minimum; case sensitive

Baseline meter

Excellent!

Half-score

Excellent!

One-third-score

Fair. Consider adding a different symbol or making your password longer.

Nudge-B^{16}

Excellent.

Nudge-Comp^{8}

Excellent!

Conditions with Scoring Differences

Type new password: usenIX$e5WHYismyP4$$word99notGOOD

8-character minimum; case sensitive

Baseline meter

Excellent!

Half-score

Excellent!

One-third-score

Fair. Consider making your password longer.

Nudge-B^{16}

Excellent.

Nudge-Comp^{8}

Excellent!

Conditions with Scoring Differences

Type new password: usenIX$e5WHYismyP4$$word99notGOODenough?

8-character minimum; case sensitive

Baseline meter — Excellent!

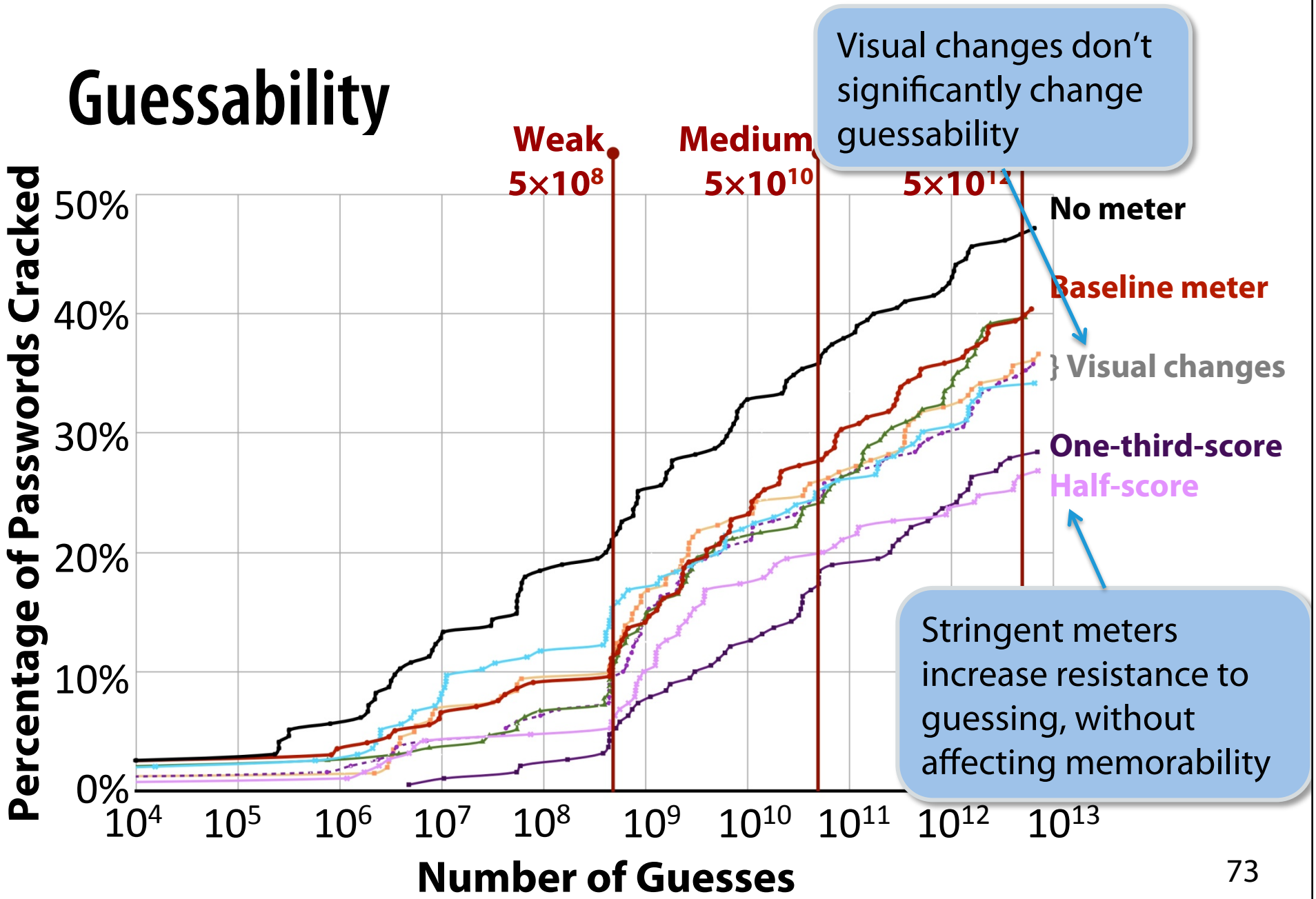
Half-score — Excellent!

One-third-score — Excellent!

Nudge-B^{16} — Excellent.

Nudge-Comp^{8} — Excellent!

Guessability



Visual changes don't significantly change guessability

Stringent meters increase resistance to guessing, without affecting memorability

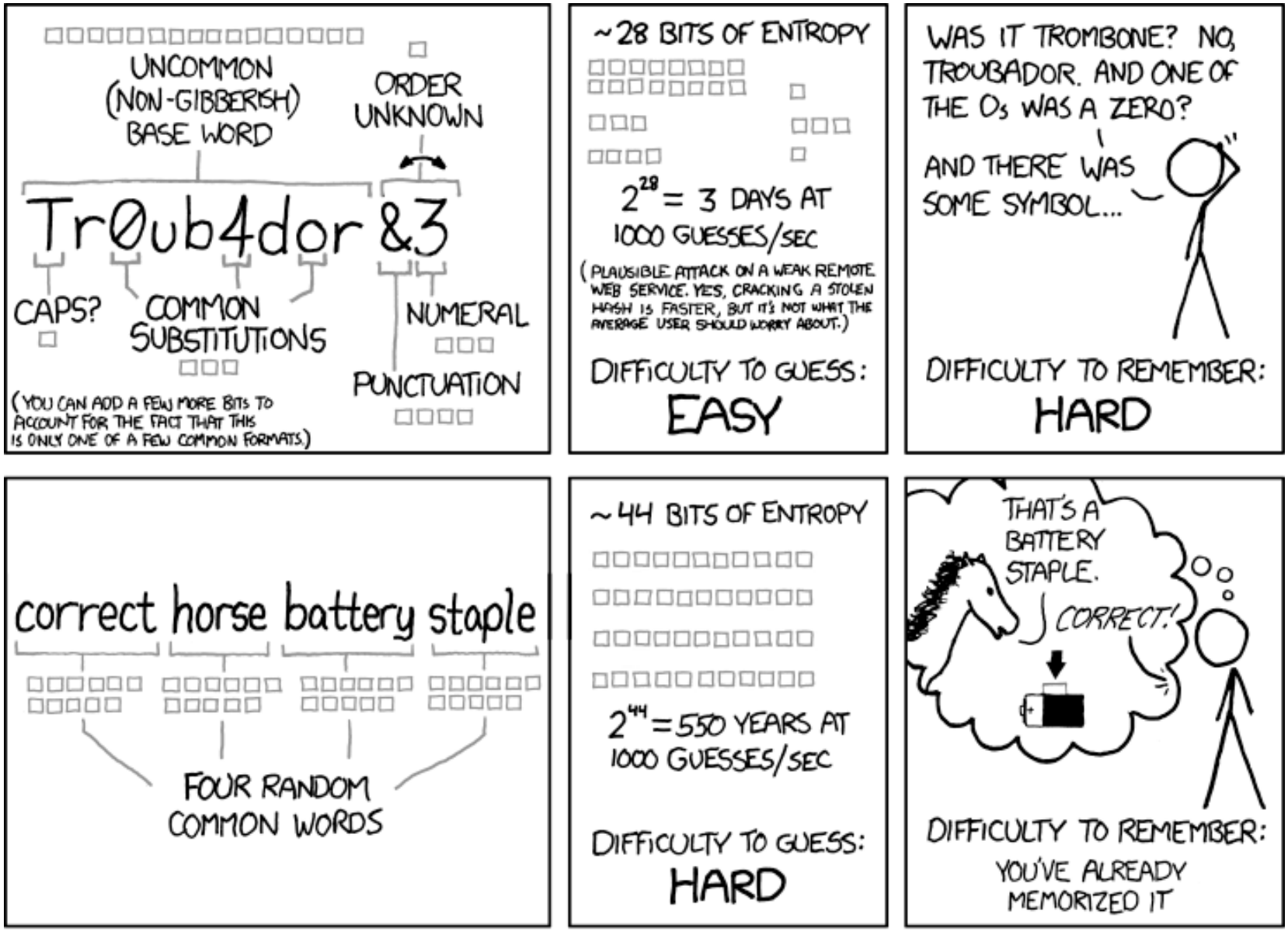
73

Open-source password meter

- In development at CMU based on empirical research
- Will provide specific suggestions for strengthening the password

Outline

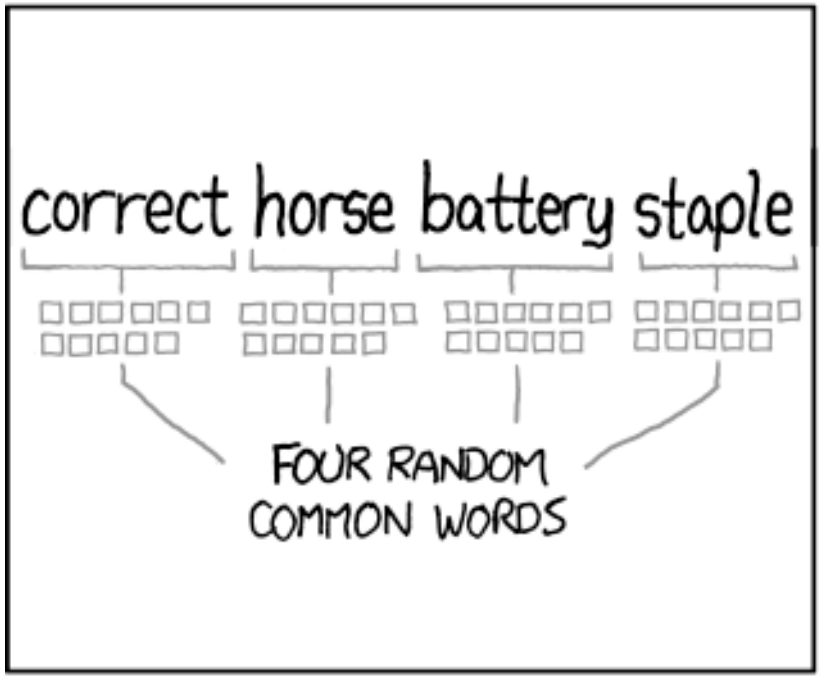
- Password study methods
- Finding good password-composition policies
- Password meters, feedback, and guidance
- **Passphrases**
  [SOUPS 2012]
- Perceptions
- Expiry
- Conclusions



http://xkcd.com/936/

Passphrase study

- Usability comparison
- System-assigned passphrases vs. passwords
- System-assigned assures random selection



Methodology

- 1,476-participant Mturk study
- Users are assigned their password or passphrase
- 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

Results

- 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
- Passphrases might have advantages for higher levels of security

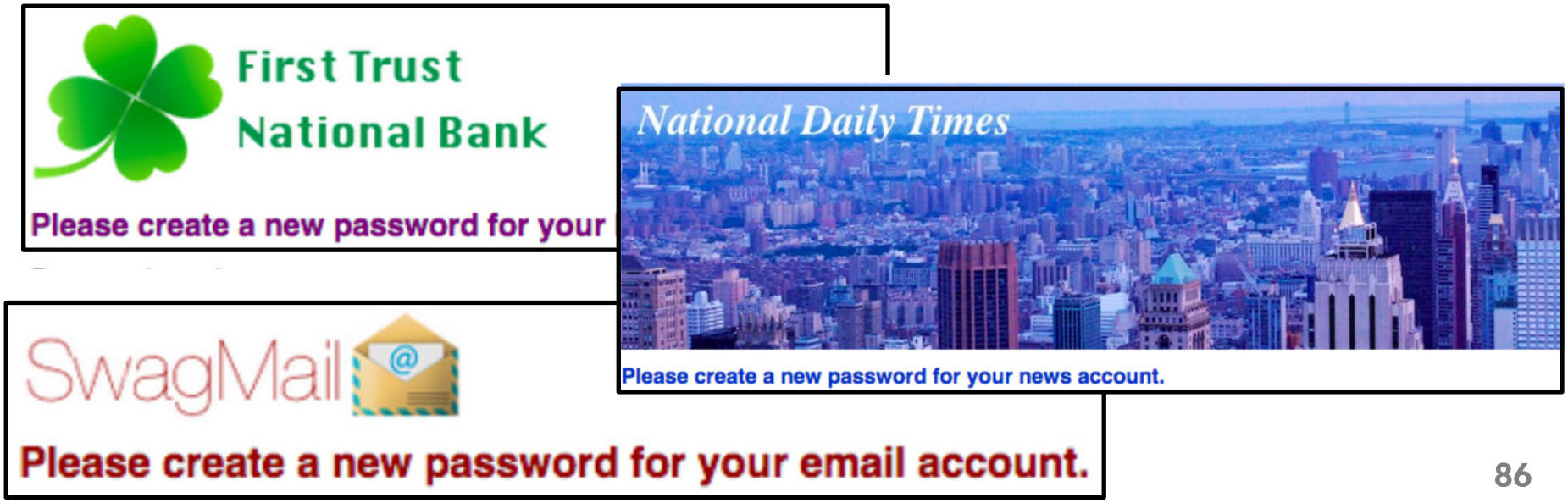
Outline

- Password study methods
- Finding good password-composition policies
- Password meters, feedback, and guidance
- Passphrases
- **Perceptions**
  [SOUPS 2015]
- Expiry
- Conclusions

Perception vs. Reality

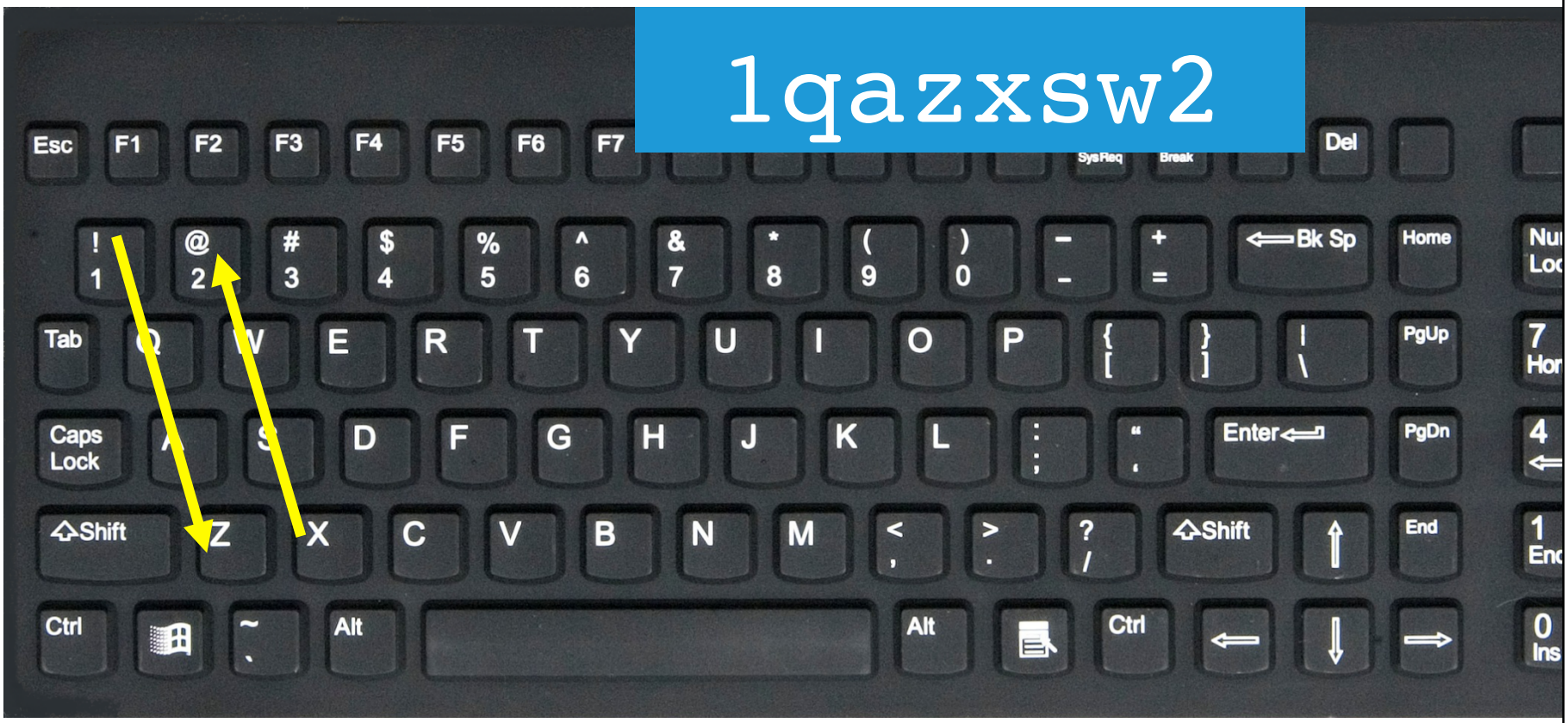
How do people make passwords?

- 49-participant think-aloud lab study
- How do they assign value to accounts?
- What makes a password secure (or not)?



MISCONCEPTION

Keyboard patterns are secure



Ur et al. "I Added '!' At The End To Make It Secure": Observing Password Creation in the Lab. SOUPS 2015

MISCONCEPTION

Adding ! to the end makes it secure

Password!

iloveyou!

monkey!

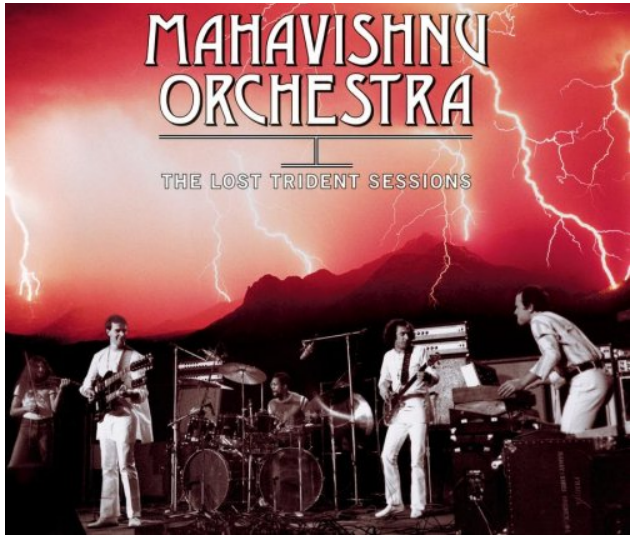
MISCONCEPTION

Dictionary words are never secure

junglesalmon711

Misunderstanding attackers

- Mahavishnu Orchestra is secure because "this band name is hard to spell."



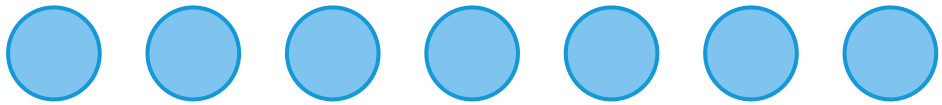
Goldie: "hackers cannot guess [it] because I have no pictures of him on my Facebook account."

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`

MISCONCEPTION

Reality

`iloveyou88`

`ieatkale88`

4,000,000,000 × more secure!

Which is more secure?

`brooklyn16`

`brooklynqy`

Study participants' perceptions

`brooklyn16`

`brooklynqy`

MISCONCEPTION

Study participants' perceptions

`brooklyn16`

`brooklynqy`

300,000 ×
more secure!

Participants were not all wrong

- Knew to avoid common words + names
  - But didn't recognize common phrases

~~**password**~~
~~**michael**~~
iloveyou

- Knew digits + symbols added strength
  - But over estimated

password!
michael2015

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

10^{60} guesses?

2 guesses?

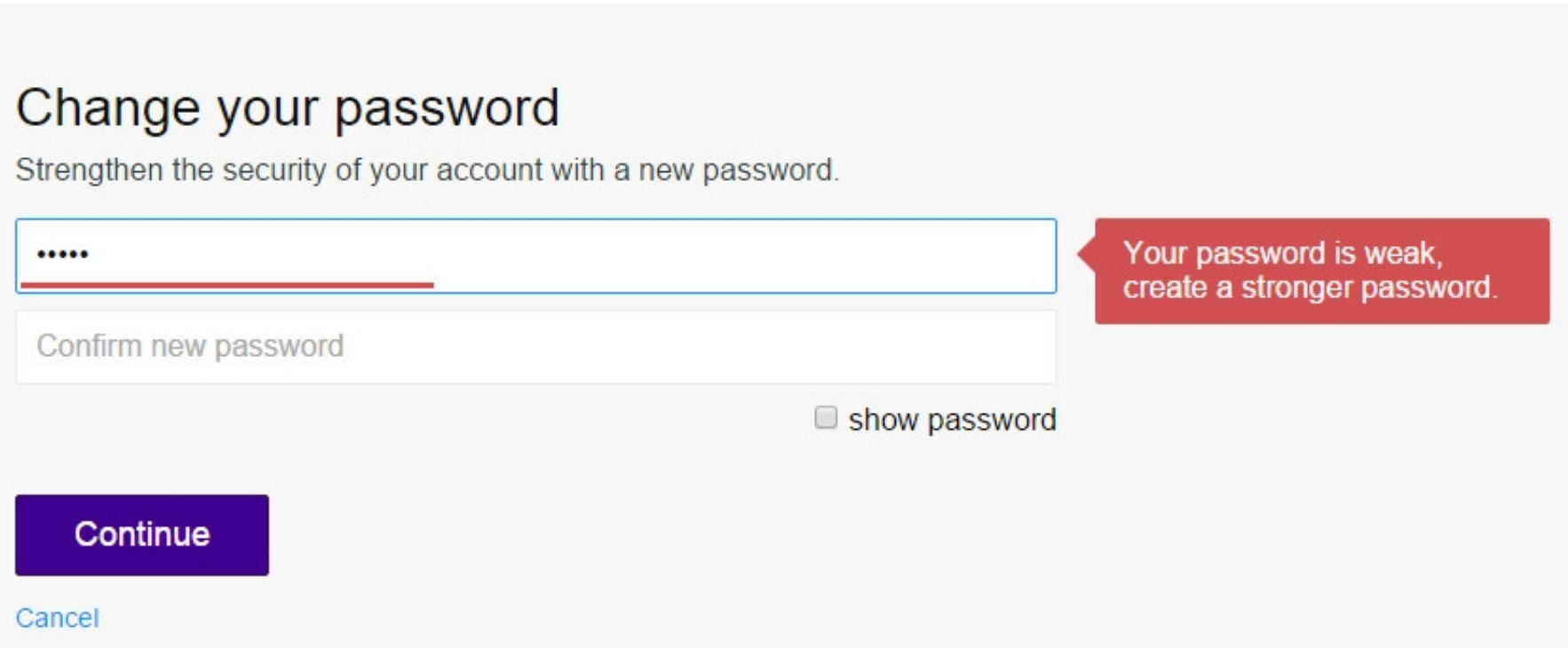
Reality: Small-Scale Guessing

- Targeted guessing by someone you know
- Automated attack by a stranger
- 1 – 1,000,000 guesses

Reality: Large-Scale Guessing

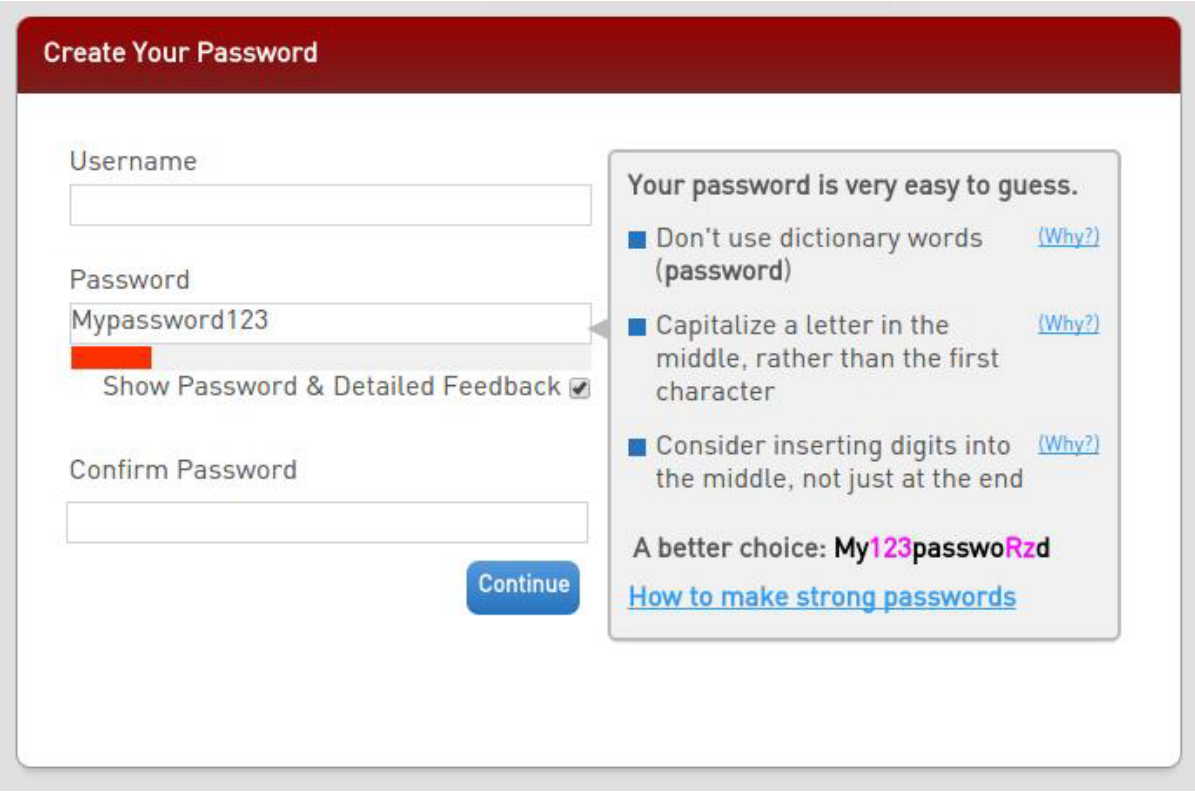
- Against stolen database of passwords
- Against password-protected file
- 1,000,000 guesses (best practices)
- 10^{14} or more (common reality)

Current feedback insufficient



Data-driven password meter

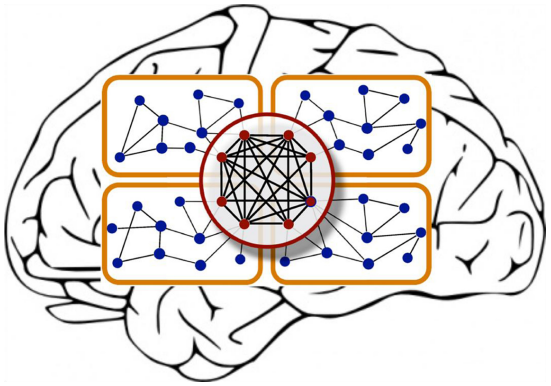
- More accurate
- Actionable feedback
- Tested in small lab study and large online study



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

Scoring guessability accurately

- Neural network rates guessability of passwords quickly on client side



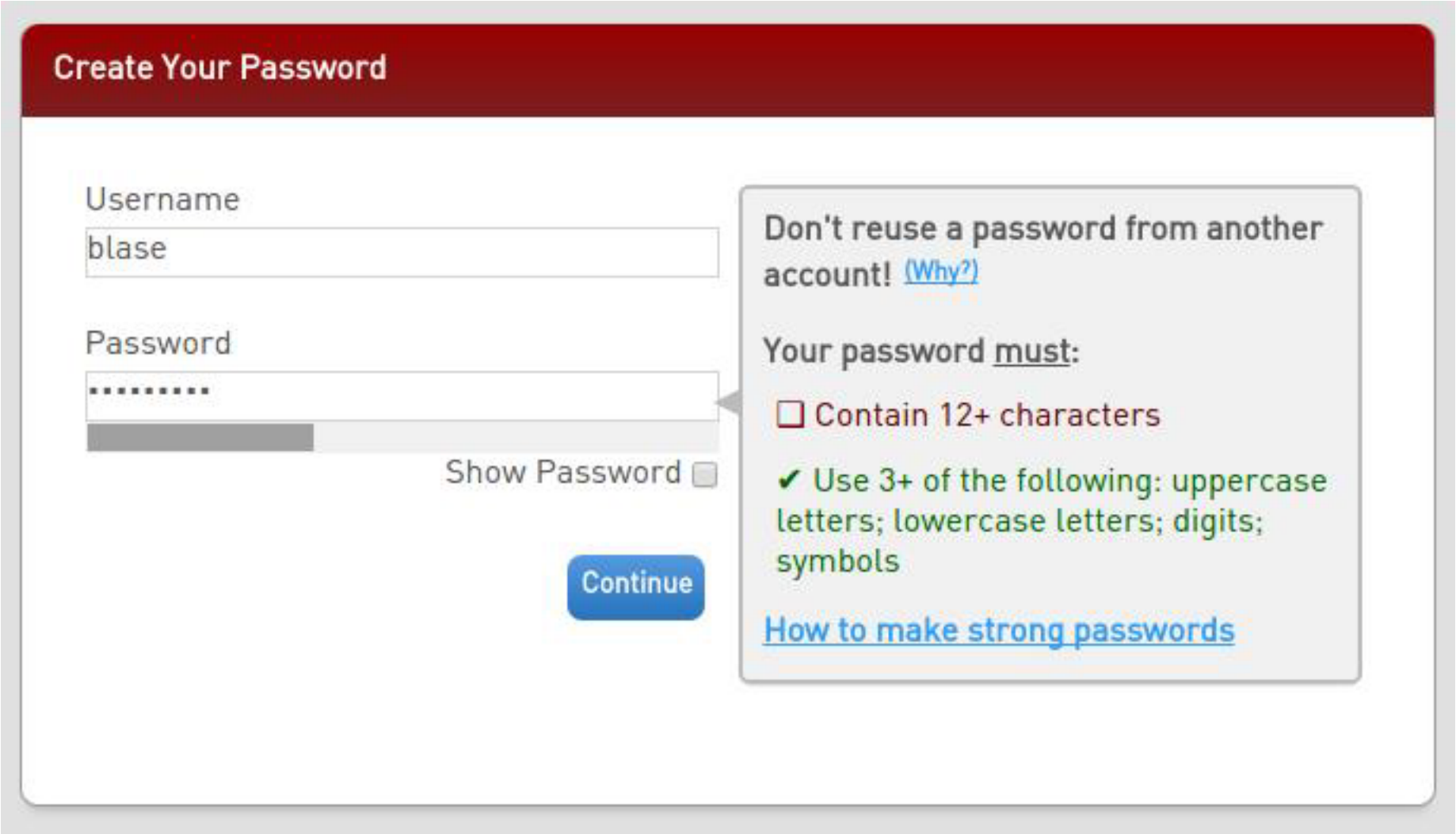
- Heuristics identify 21 characteristics that lead to weak passwords
  - Dictionary words and phrases
  - Keyboard patterns, dates
  - Location of uppercase, digits, symbols

Image credit: doi:10.3389/fninf.2010.00112

Actionable feedback

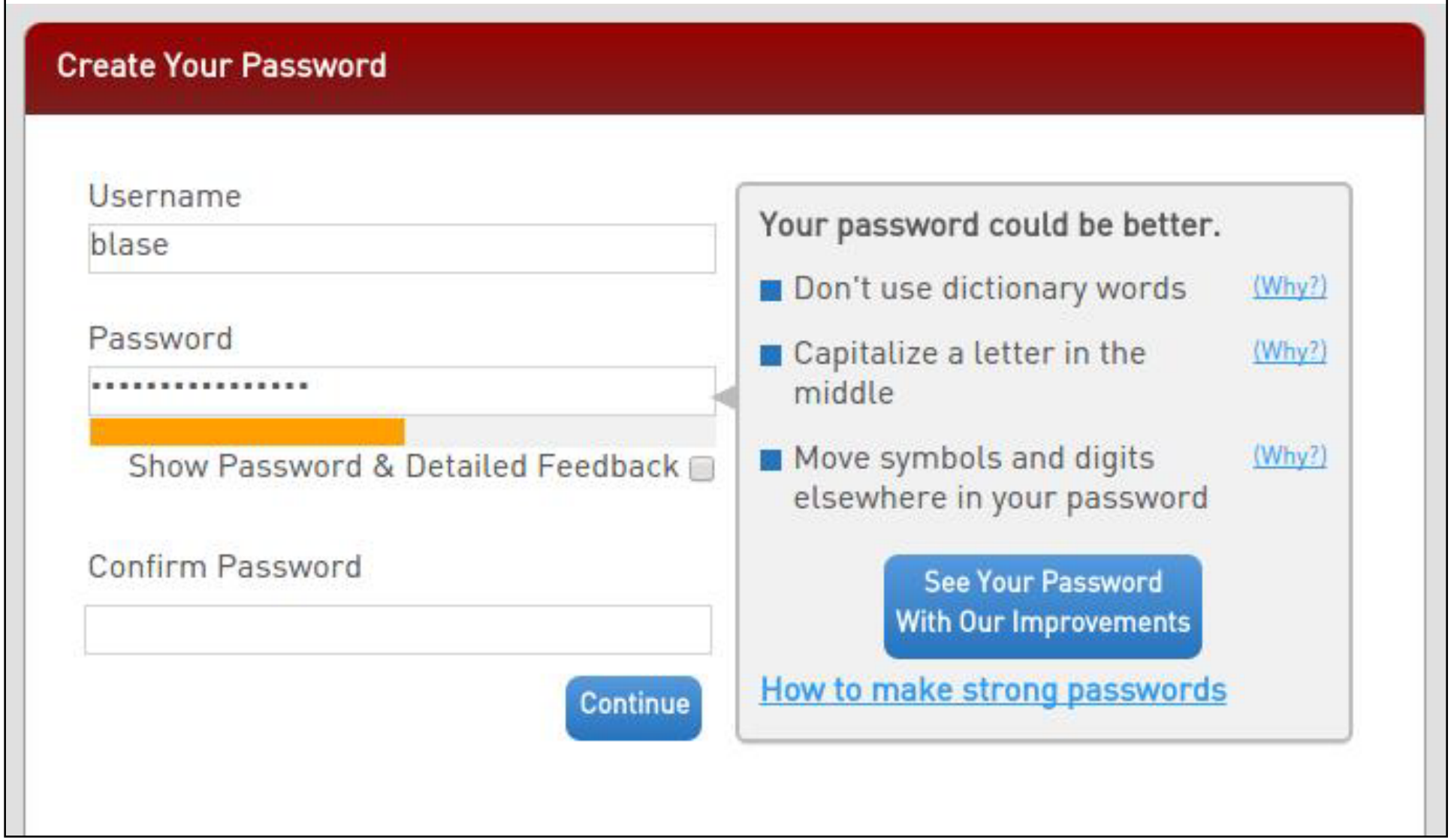
- Meeting minimum requirements
- Generic advice
- Feedback on up to 3 most important ways to improve password
- Detailed feedback specific to password if user shows password
- Suggested improved password

Meeting minimum requirements

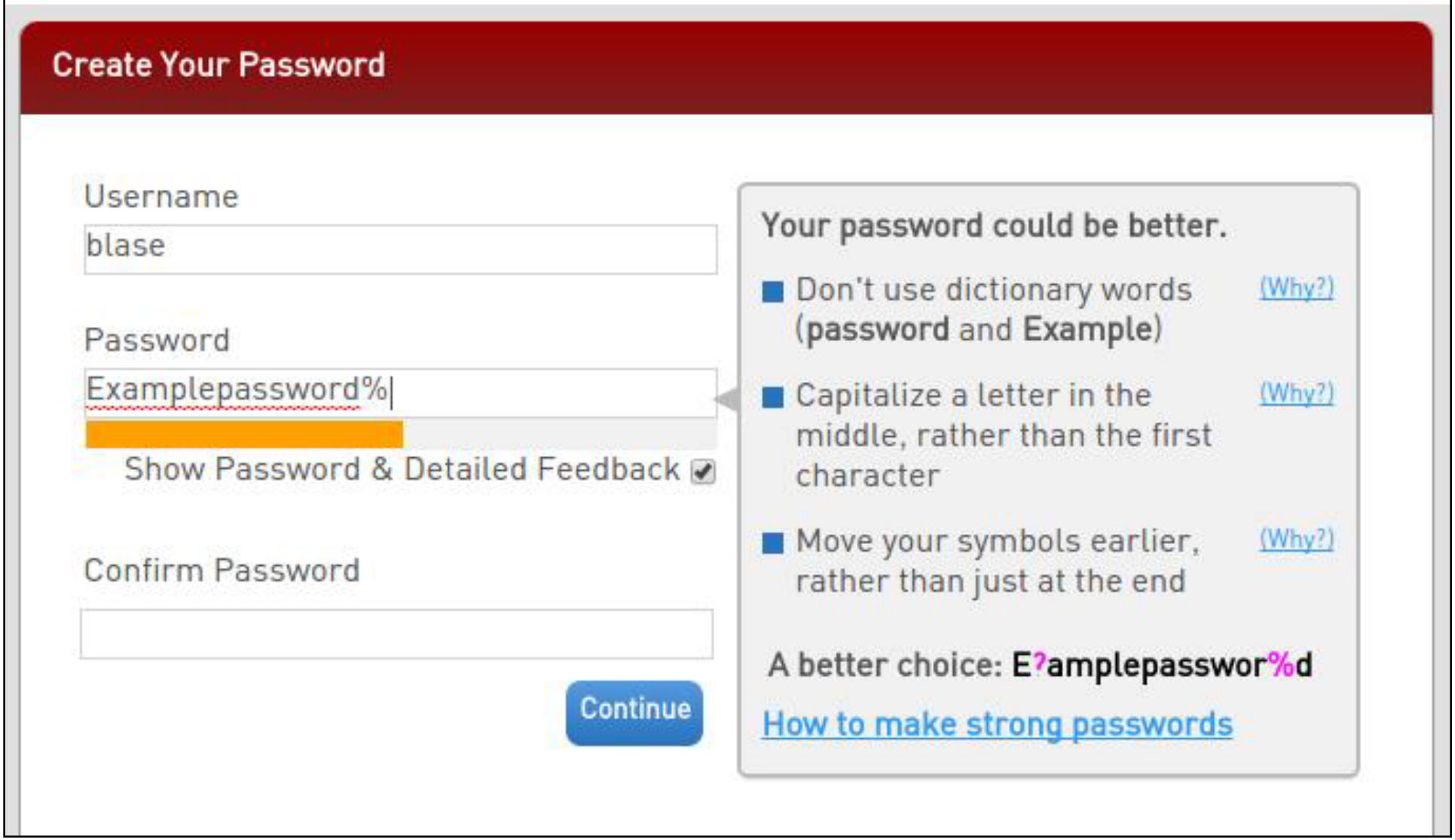


Generic advice modal

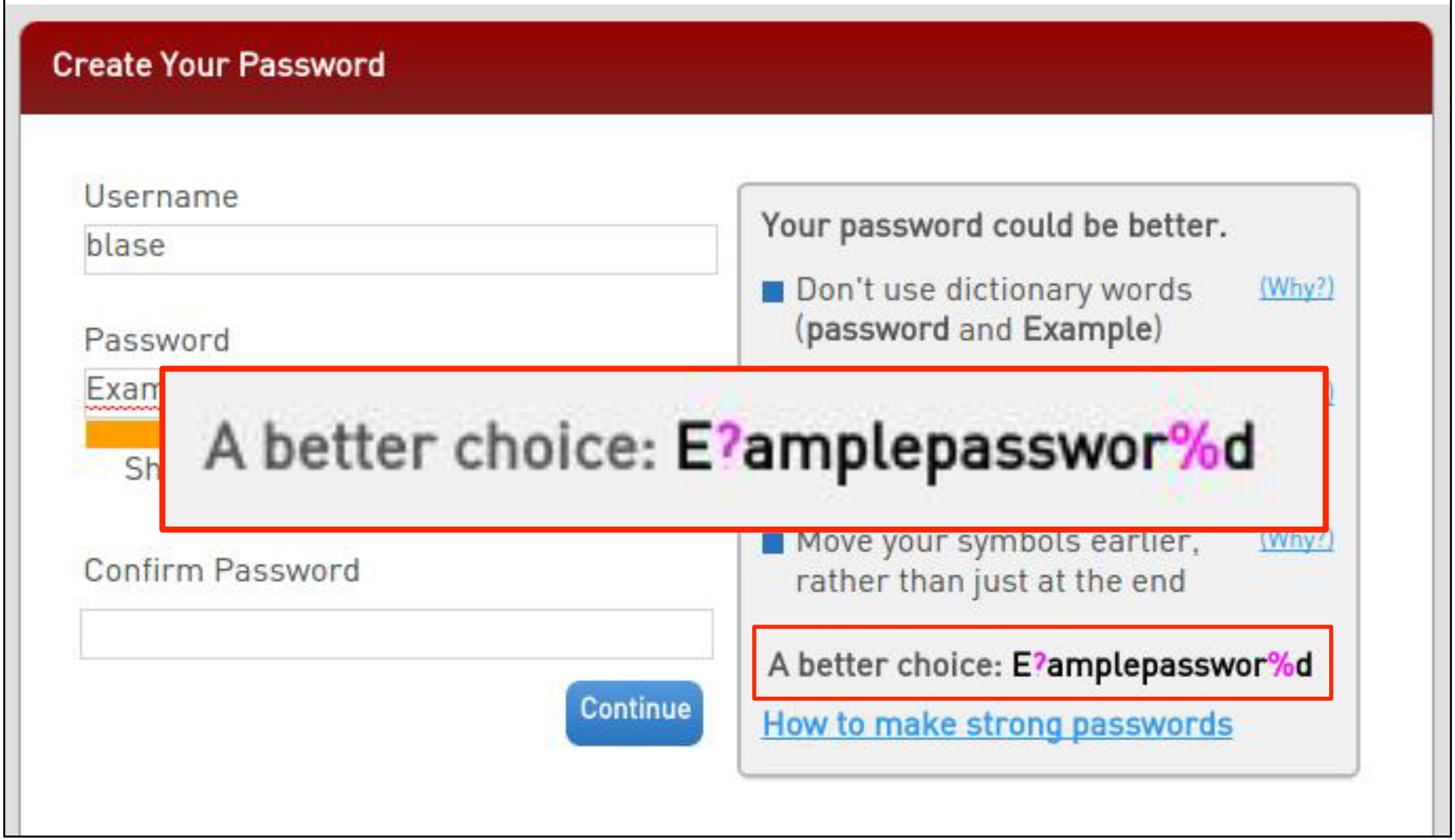
Up to 3 suggested improvements



Detailed feedback when password displayed on screen



Suggested improved password



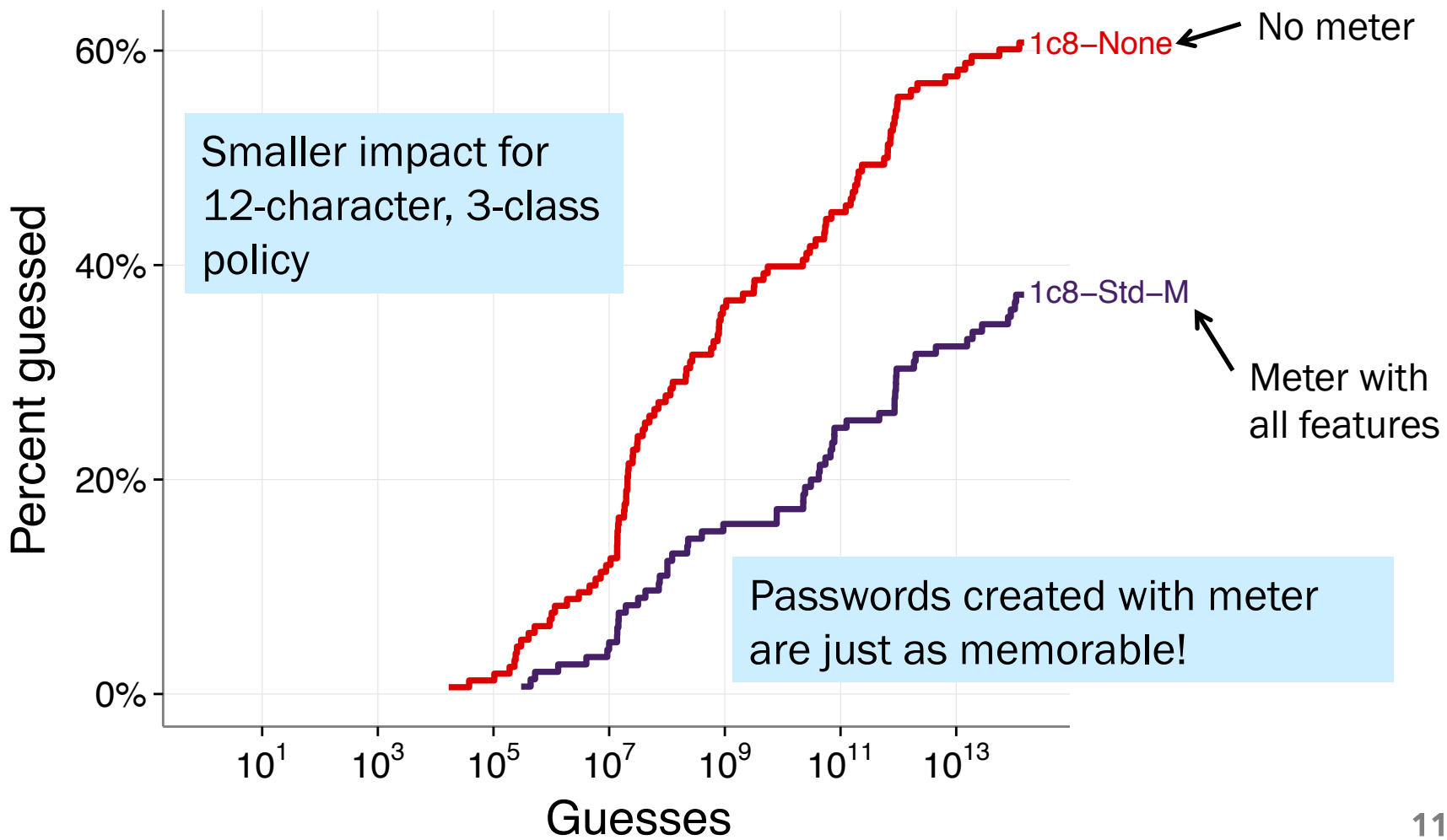
Online user study

- 4,509 participants
- 2 parts
  - Create password, complete survey, recall password
  - Return 2+ days later to recall password, complete survey
- Experimental treatments tested
  - 2 password policies
  - 3 scoring stringencies
  - 6 types of feedback

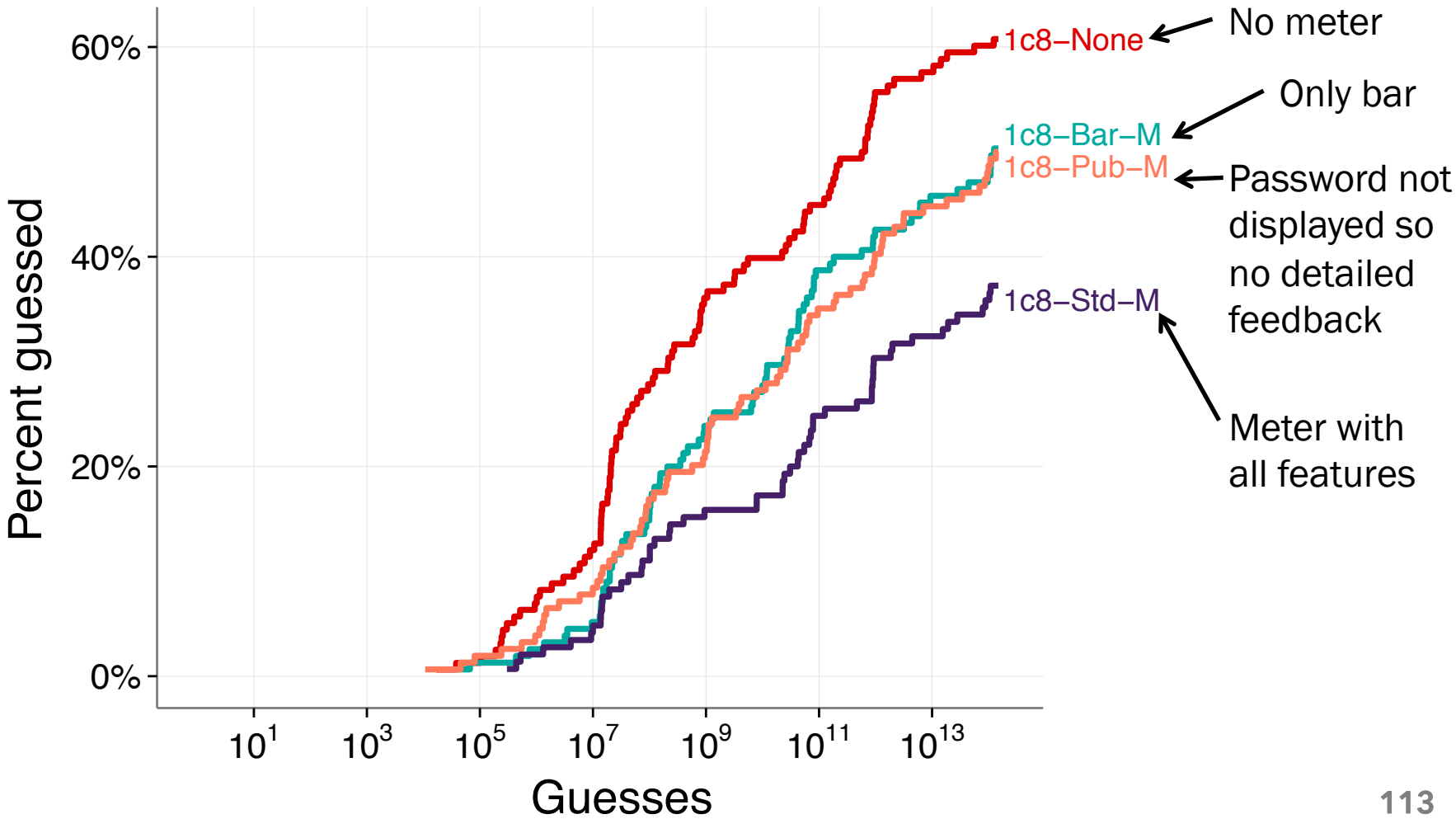
Users reported meter was useful

- 32% learned something new about passwords from text feedback
- 62% agreed text feedback made their password stronger
- 77% found feedback informative

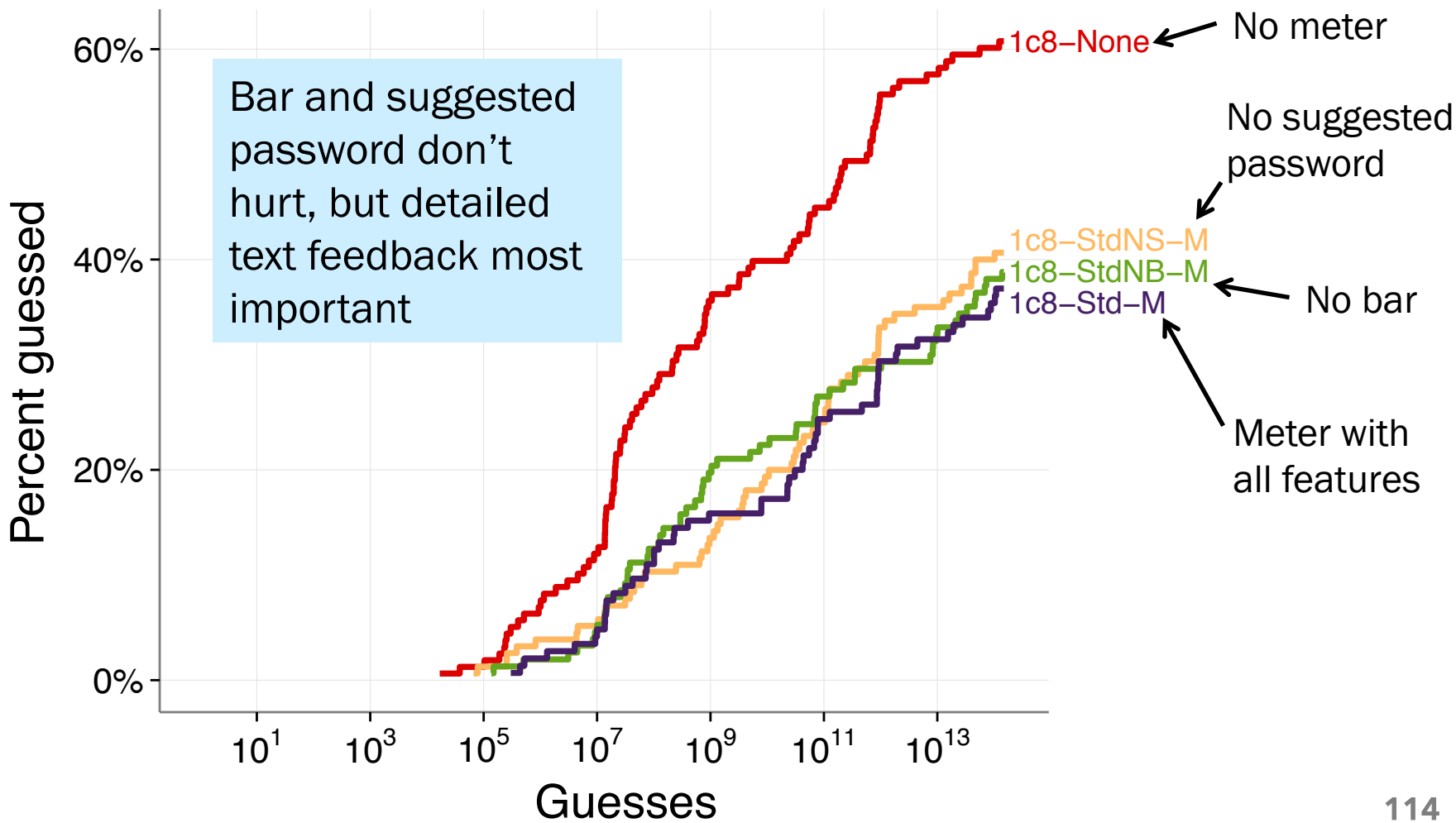
Meter improves strength for common 8-character policy



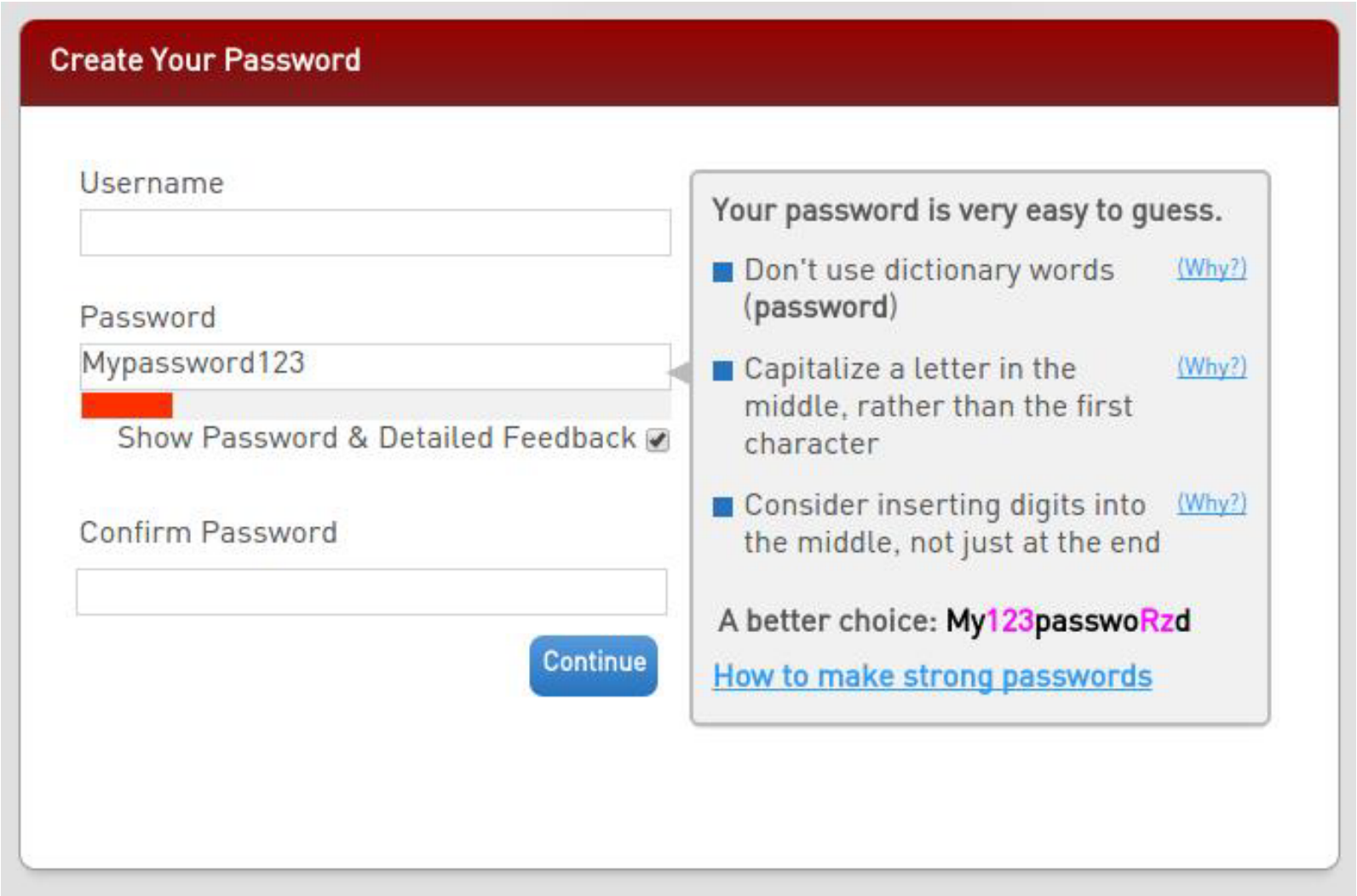
Meter less effective without detailed feedback



Bar and suggested password have little impact on strength



Open source release coming soon



Outline

- Password study methods
- Finding good password-composition policies
- Password meters, feedback, and guidance
- Passphrases
- Perceptions
- **Expiry**
  [Tech@FTC]
- Conclusions

FTC
@FTC

Following

Encourage your loved ones to change passwords often, making them long, strong, and unique. More tips: go.usa.gov/cEqkH. #ChatSTC

RETWEETS 10 LIKES 4

3:51 PM - 27 Jan 2016

Reply to @FTC

PacificEast Research @PacificEast · Jan 27

PASSWORDS ARE LIKE UNDERPANTS

Change them often, keep them private and never share them with anyone.

ftc.gov

Contact | Stay Connected | Privacy Policy | FTC en español

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Search

ABOUT THE FTC | NEWS & EVENTS | ENFORCEMENT | POLICY | TIPS & ADVICE | I WOULD LIKE TO...

News & Events » Blogs » Tech@FTC » Time to rethink mandatory password changes

Time to rethink mandatory password changes

By: Lorrie Cranor, Chief Technologist | Mar 2, 2016 10:55AM

TAGS: Authentication | Human-computer interaction | Passwords | Research

Data security is a process that evolves over time as new threats emerge and new countermeasures are developed. The FTC's longstanding advice to companies has been to conduct risk assessments, taking into account factors such as the sensitivity of information they collect and the availability of low-cost measures to mitigate risks. The FTC has also advised companies to keep abreast of security research and advice affecting their sector, as that advice may change. What was reasonable in 2006 may not be reasonable in 2016. This blog post provides a case study of why keeping up with security advice is important. It explores some age-old security advice that research suggests may not be

Categories

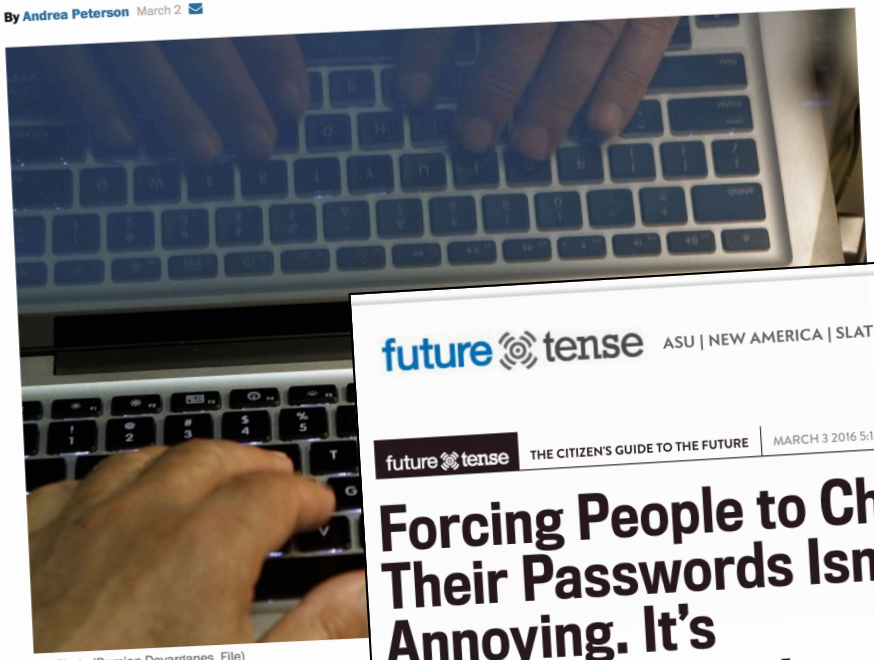
- Data security (7)
- Privacy (12)
- Passwords (2)
- Authentication (2)
- MAC address tracking (2)
- Mobile location analytics (2)
- Wi-Fi tracking (1)
- Mobile device settings (3)
- In-app purchases (1)
- Human-computer interaction (4)
- Accountability (4)
- Personal harms (3)
- Data sharing risks (2)
- Research (6)
- Fellowships (2)
- Training (1)
- Design (3)

The Washington Post

Sections

Why changing your password regularly may do more harm than good

By Andrea Peterson March 2



(AP Photo/Damian Dovarganes, File)

Most office drones have had to deal with a
clockwork, maybe every six months or so.
flushing out old passwords will cut off acce

WIRED

Want Safer Passwords? Don't Change Them So Often

SHARE

SHARE 63

TWEET

PIN

BRIAN BARRETT SECURITY 03.10.16 7:00 AM

WANT SAFER PASSWORDS? DON'T CHANGE THEM SO OFTEN

ONE/WIRED

AY, ALL OF you IT managers, it's time we had a talk.

now you mean well. I know you think you're helping. But
en you demand that your co-workers' passwords change

Slate

future tense ASU | NEW AMERICA | SLATE

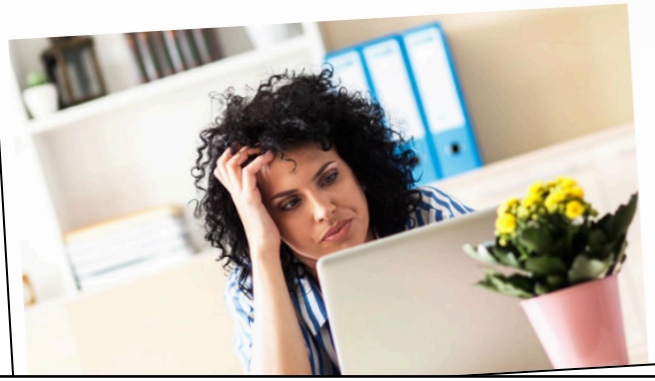
Learn more about Future Tense »

future tense THE CITIZEN'S GUIDE TO THE FUTURE | MARCH 3 2016 5:10 PM

Forcing People to Change Their Passwords Isn't Just Annoying. It's Counterproductive.

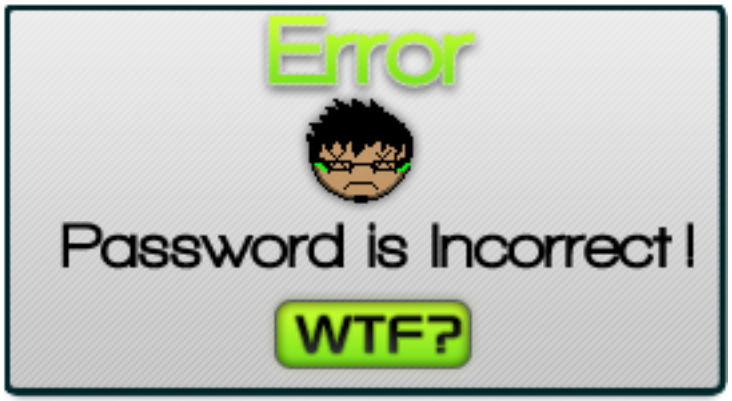
By Lily Hay Newman

749 159 93



Why require password changes?

Lock out attackers who have learned users' passwords



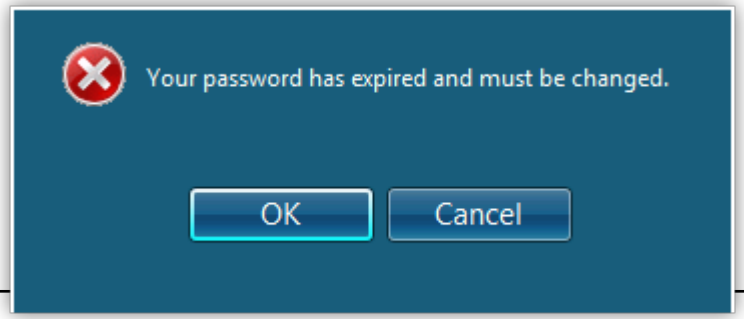
Password transformations

Password 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`

10,000+ defunct UNC accounts

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



Zhang, Monrose, and Reiter, *CCS 2010*

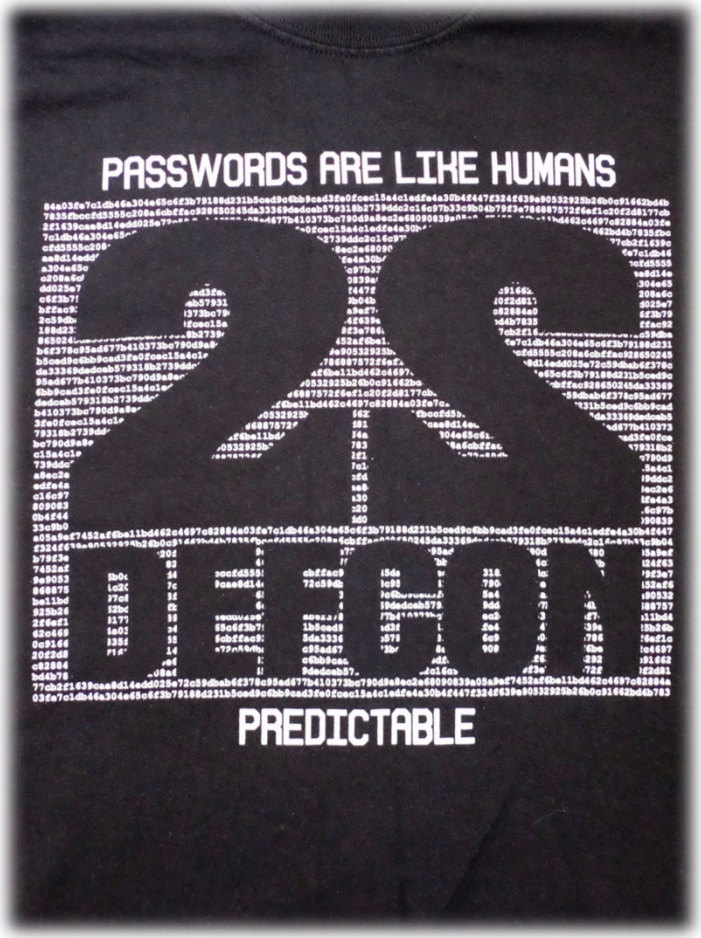
Evaluation

- Pick a known plaintext, non-last password (OLD)
- Pick any later password (NEW)
- Attempt to crack NEW using transform rules applied to OLD

Zhang, Monrose, and Reiter, *CCS 2010*

Results

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



Zhang, Monrose, and Reiter, *CCS 2010*

Benefits of expiry are limited

- Brute force attacks only slowed a little bit by password change
  - Slow hash functions slow them down more
- Attacker who gains access may install key logger and observe password change

Quantifying the Security Advantage of Password Expiration Policies. Chiasson & van Oorshot 2015.

Survey evidence

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

The problems with forcing regular password expiry

Version: 1
Created: 11 April 2016
Updated: 15 April 2016
Topics: Passwords, Best Practice

Why CESG decided to advise against this long-established security guideline.

Regular password expiry is a common requirement in many security policies. However, in CESG's Password Guidance published in 2015, we explicitly advised against it. This article explains why we made this (for many) unexpected recommendation, and why we think it's the right way forward.

Let's consider how we might limit the harm that comes from an attacker who knows a user's password. The obvious answer is to make the compromised password useless by forcing the legitimate user to replace it with a new one that the attacker doesn't know.

Related Content

Password Guidance: Simplifying Your Approach

Revealed: the most frequently used passwords of 2015

Certified Cyber Consultancy

Cyber Essentials

CESG advocates new approach to

pages.nist.gov

NIST National Institute of Standards and Technology U.S. Department of Commerce

NIST Website | About NIST | usnistgov on Github

Digital Authentication Guideline: Public Preview

SP 800-63-3
Digital Authentication Guideline

SP 800-63A
Identity Proofing & Enrollment

SP 800-63B
Authentication & Lifecycle Management

SP 800-63C
Federation & Assertions

Welcome to the NIST SP 800-63-3 Public Preview! We're excited to share the major transformation that this document has undergone, as well as collaboratively enhance and evolve the guidance as we head to a public draft later this summer.

A few formalities

Public preview vs public draft

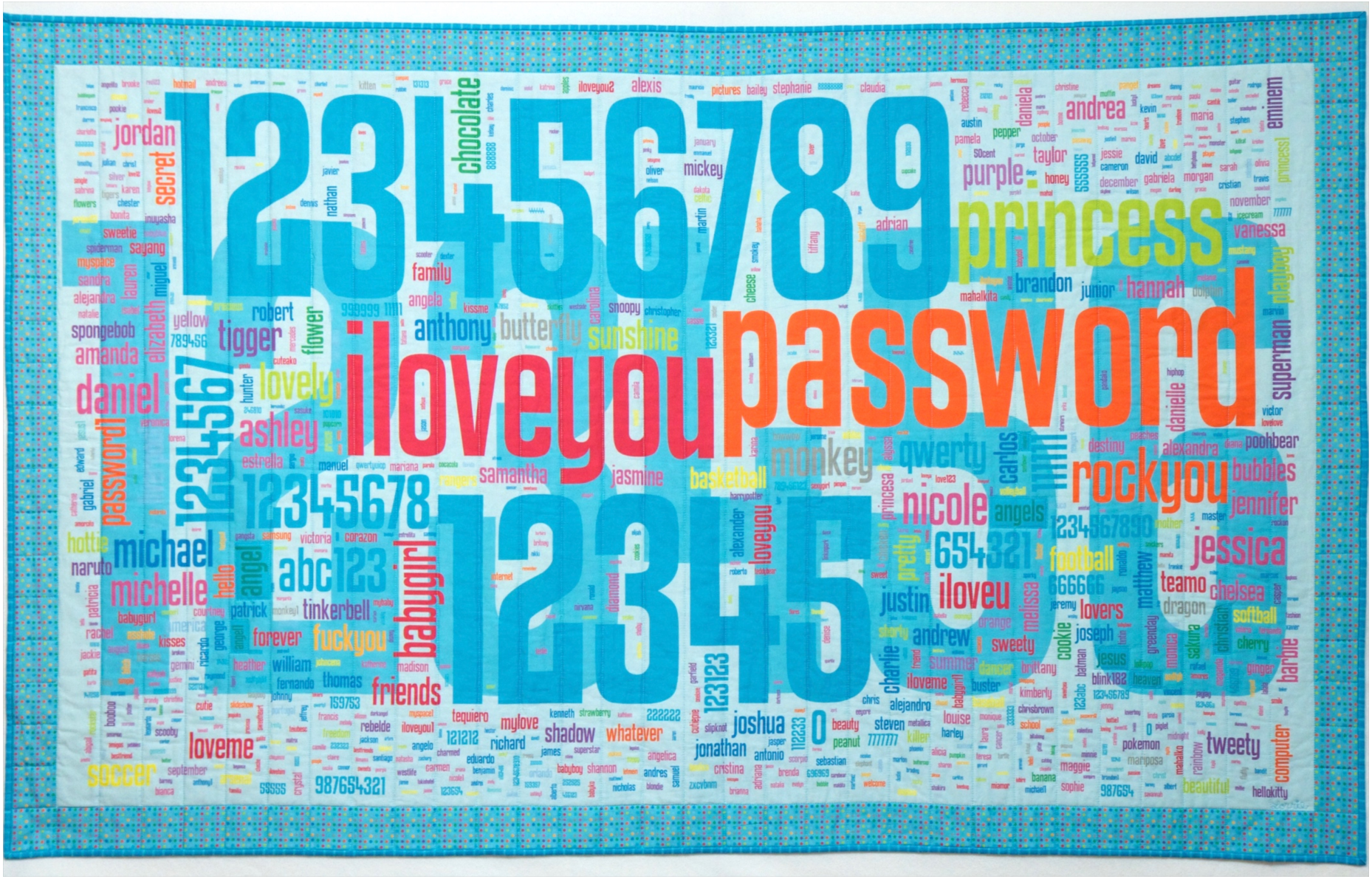
If you've made it to this page, you can see we're approaching this a little differently by putting our work up on GitHub, rather than the "traditional" comment period for a NIST Special Publication (SP). We're calling it a public preview because some of our agency partners (and NIST itself) have formal processes for public drafts. Calling it a public preview is our way of letting everyone know those processes aren't in play. This lets us do things differently…

A different cadence

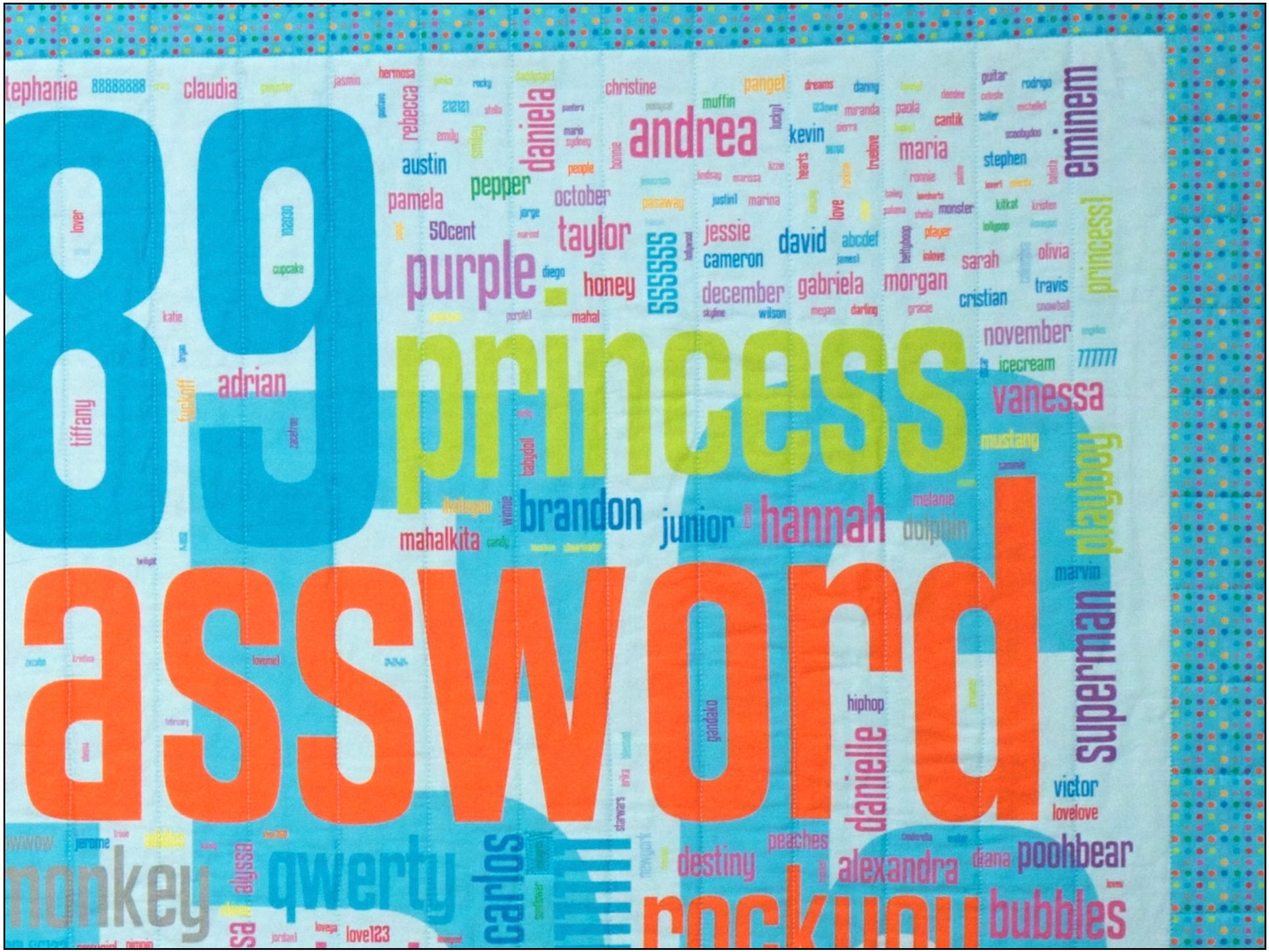
This public preview is focused on gaining input through successive open comment periods and editing iterations of the SP draft. This phase will include multiple iterations of comments of approximately 2 weeks in length, followed by a 2-3 week period for the editors to adjudicate comments and make appropriate updates to

Outline

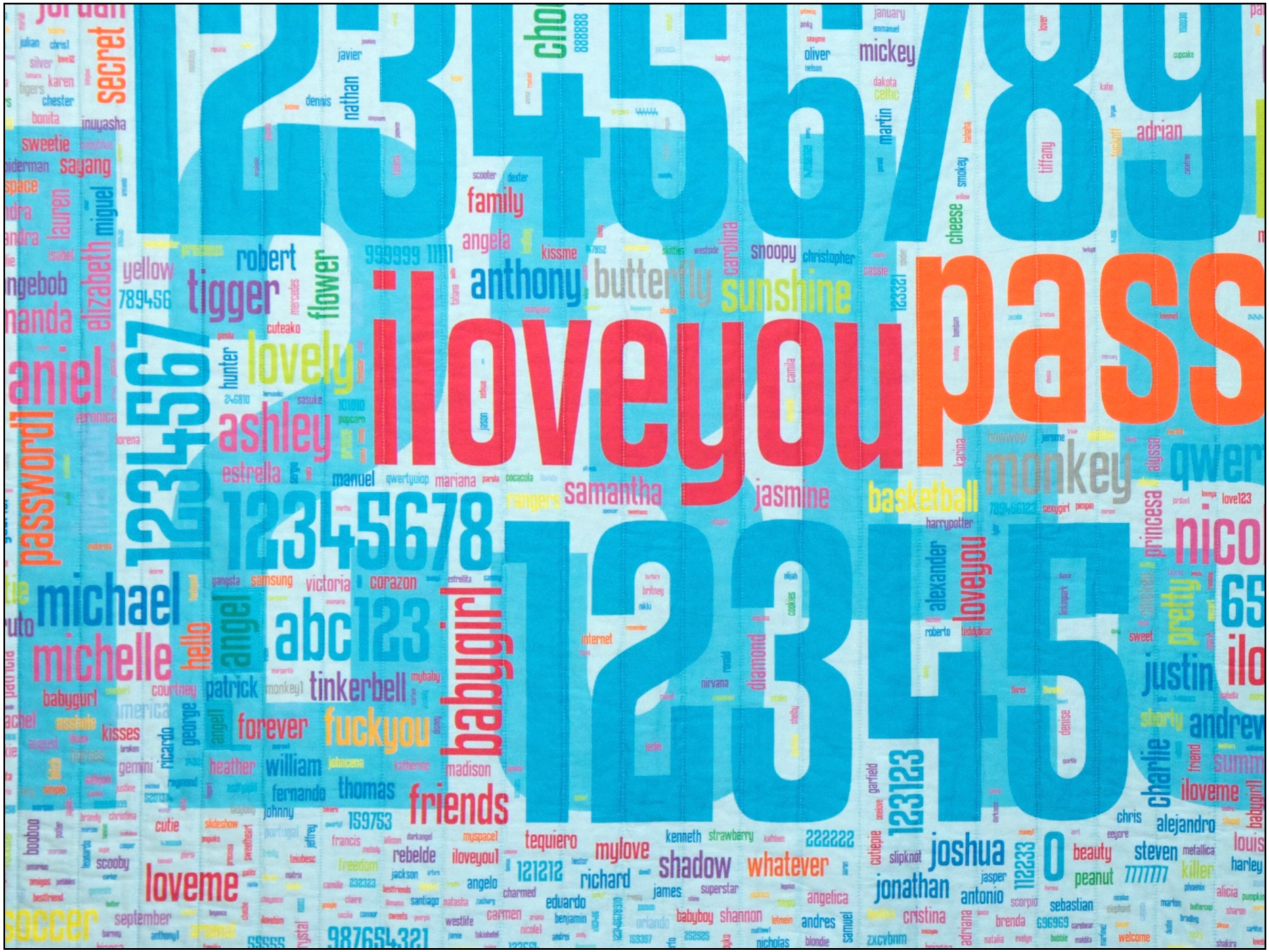
- Password study methods
- Finding good password-composition policies
- Password meters
- Passphrases
- Perceptions
- Expiry
- **Conclusions**


123456789
princess
password
iloveyou
12345
rockyou
12345678
1234567
monkey
jessica
nicole
babygirl
abc123
michael
michelle
daniel
ashley
lovely
tigger
friends
fuckyou
tinkerbell
loveme
soccer
jordan
secret
chocolate
anthony
butterfly
sunshine
samantha
jasmine
basketball
qwerty
654321
iloveu
justin
andrew
joshua
jonathan
shadow
whatever
tweety
computer
beautiful
hellokitty
superman
pooh bear
bubbles
jennifer
teamo
chelsea
softball
barbie
cherry
ginger
dragon
lovers
football
andrea
purple
taylor
hannah
brandon
vanessa
eminem
princess
spongebob
amanda
elizabeth
flower
family
mickey
sweetie
sayang
hottie
naruto
patrick
forever
kisses
tequiero
mylove
richard
987654321
987654


monkey
qwerty
basketball
nicole
654321
iloveu
justin
andrew
loveyou
alexander
princesa
pretty
angels
carlos
footba
666666
melissa
jeremy
love
orange
sweetly
cookie
josep
batman
brittany
dancer
summer
charlie
iloveme
buster
babygirl1
kimberly
chrisbrown
baseball
123abc
123123
joshua
0
beauty
steven
metallica
louise
monique
school
harley
killer
peanut
alejandro
chris
eeyore
cutiepie
slipknot
jasper
jonathan
harrypotter
roberto
teddybear
sweet
shorty
denise
friend
garfield
bowwow
jerome
karina
alyssa
sexygirl
pimpin
love123
volleyball
linkinpark
chicken
laura
cancer
valentina
bitch!
billabong
apple
phoenix



89
princess
assword
rockyou
monkey
qwerty
andrea
purple
brandon
hannah
superman
playboy
poohbear
bubbles
alexandra
danielle
carlos
eminem
princess1
vanessa
november
junior
taylor
maria
david
jessie
morgan
gabriela
december
honey
pamela
pepper
october
austin
daniela
rebecca
claudia
stephanie
88888888
christine
muffin
panget
kevin
stephen
sarah
olivia
travis
cristian
cameron
555555
50cent
adrian
tiffany
lover
cupcake
katie
mahalkita
dolphin
melanie
icecream
mustang
marvin
victor
lovelove
diana
destiny
peaches
hiphop
alyssa
jerome
love123
jordan1
gandako
starwars
newyork


123456789
iloveyou
pass
12345
12345678
1234567
password1
abc123
babygirl
monkey
qwert
michael
michelle
ashley
nicol
anthony
butterfly
sunshine
tigger
robert
lovely
angel
fuckyou
friends
loveme
soccer
tinkerbell
samantha
jasmine
basketball
princesa
pretty
justin
andrew
joshua
jonathan
shadow
whatever
mylove
family
angela
kissme
snoopy
christopher
chocolate
mickey
oliver
javier
nathan
dennis
julian
chris1
silver
karen
tigers
chester
bonita
secret
inuyasha
sweetie
sayang
space
lauren
miguel
elizabeth
yellow
789456
hunter
flower
cuteako
estrella
manuel
qwertyuiop
mariana
cocacola
rangers
999999
11111
carolina
123321
martin
adrian
tiffany
smokey
cheese
alyssa
love123
alexander
iloveyou
princess
pretty
charlie
iloveme
babygirl1
alejandro
steven
chris
beauty
peanut
777777
killer
louis
harley
antonio
sebastian
scorpio
cristina
brenda
adriana
samuel
andres
shannon
babyboy
angelica
superstar
james
richard
eduardo
benjamin
121212
angelo
rebelde
iloveyou1
myspace1
jackson
freedom
francis
159753
987654321
september
scooby
booboo
cutie
slideshow
sweetheart
portugal
johnny
jeffrey
fernando
thomas
william
heather
gemini
ricardo
george
kisses
horses
america
babygurl
courtney
patrick
monkey1
hello
victoria
corazon
samsung
gangsta
madison
katherine
johncena
kenneth
strawberry
222222
123123
garfield
cutiepie
slipknot
112233
jasper
diamond
nirvana
internet
babyboy
blondie
nicholas
zxcvbnm
natalia
metallica
alicia
phoenix
spiderman
daniel
amanda
sandra
hannah
spongebob
sasuke
popcorn
101010
jason
camila
samantha
linkinpark
sweet
friend
starly
summer
655
tuckoff
cupcake
january
emmanuel
dakota
celtic
nelson
scooter
dexter
westside
skittles
cassie
harrypotter
sexygirl
pimpin
lovers
mybaby
roberto
teddybear
cookies
britney
nikki
elijah
denise
jordan
naruto
patricia
rachel
august
isabel
veronica
lorena
miranda
carmen
nicole
orlando
eyeore
arsenal
888888
superman
mercedes
lovelove
anthony1
marlon
sharon
rangers
myspace

http://cups.cs.cmu.edu/passwords.html

Carnegie Mellon University
Master of Science in Information Technology
privacy ENGINEERING

Carnegie Mellon University
CyLab

isr institute for SOFTWARE RESEARCH

Engineering & Public Policy