04. Passwords

Blase Ur and Mainack Mondal

April 4th, 2018

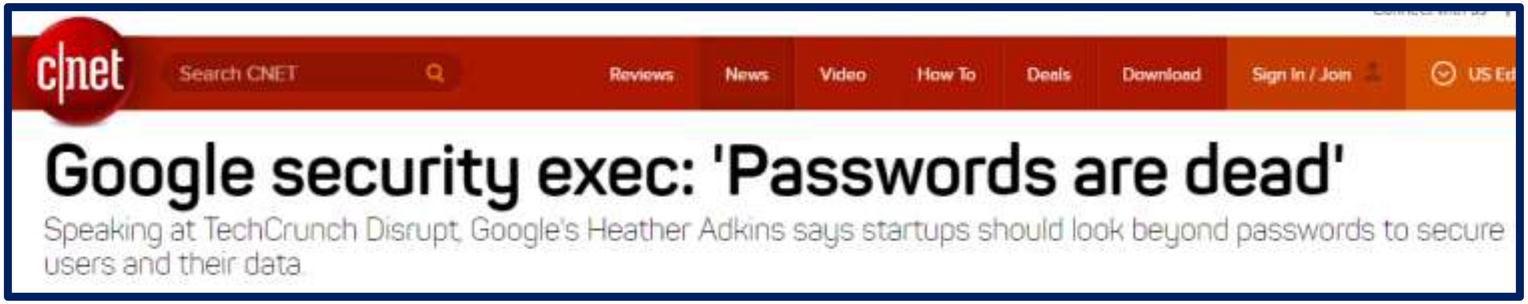
CMSC 23210 / 33210

THE UNIVERSITY OF CHICAGO

UCHICAGO SUPER GROUP

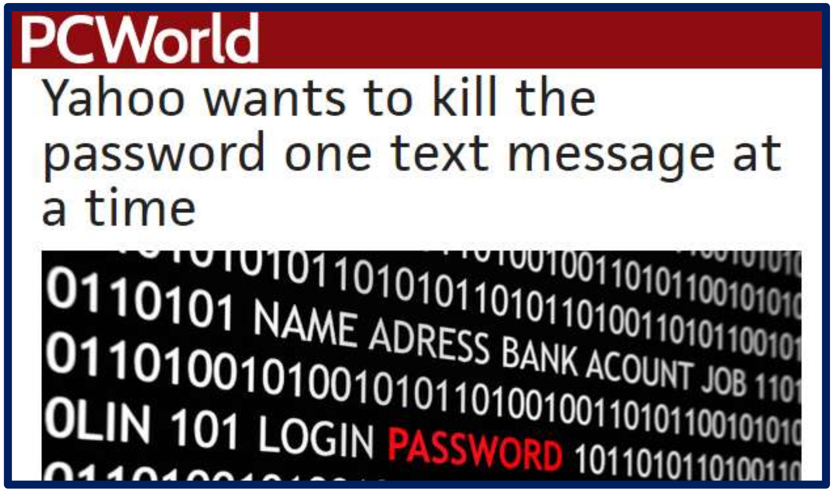
Security, Usability, & Privacy Education & Research

123
robert
killer
iloved
jennifer
forever
spongebob
chocolate
charlie
america
lovers
beautiful
blink182
rangers
monica
whatever
dragon
bubbles
hottie
cookie
12345
1234567
654321
rainbow
orange
steven
thomas
angel
carlos
babygirl
000000
hannah
michelle
samantha
monkey
jessica
eminem
computer
william
rockyou
flower
soccer
tigger
nicole
liverpool
summer
melissa
christian
password
shadow
purple
princess
princess1
sakura
michael
andrea
tinkerbell
junior
12345678
123456789
softball
matthew
ashley
password1
daniel
1234567890
anthony
jesus
mickey
lovely
friends
elizabeth
patrick
brandon
dancer
chelsea
pretty
barbie
secret
jordan
football
playboy
666666
jasmine
poohbear
angels
justin
andrew
qwerty
iloveyou
hello
basketball
abc123
butterfly
superman
sunshine
pokemon
heaven
miguel

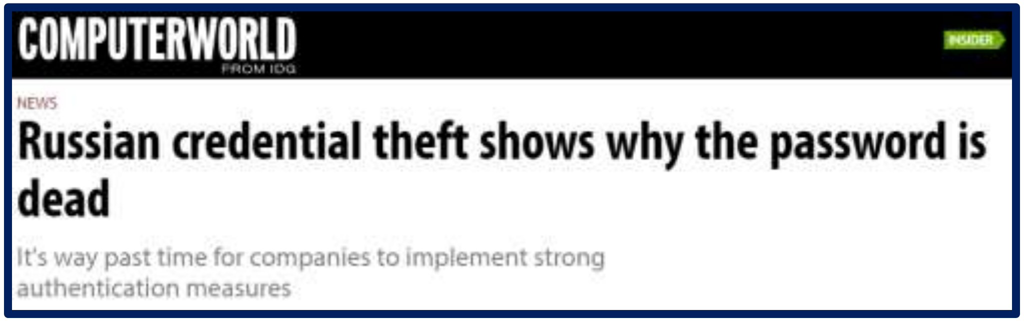


Google security exec: 'Passwords are dead'

Speaking at TechCrunch Disrupt, Google's Heather Adkins says startups should look beyond passwords to secure users and their data



Yahoo wants to kill the password one text message at a time

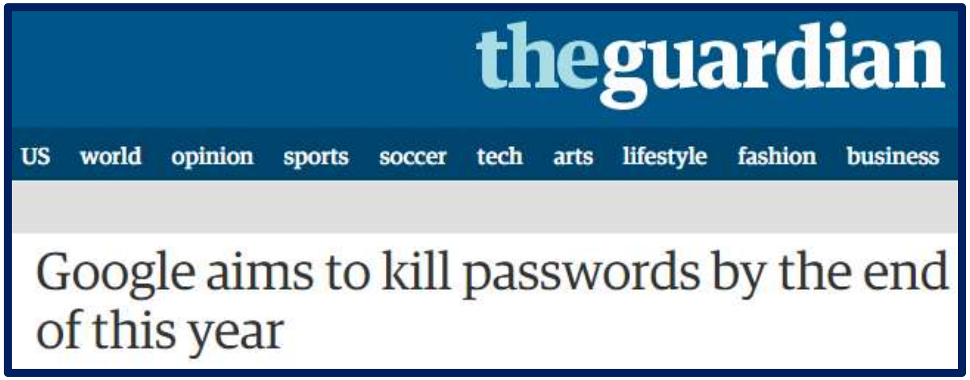


NEWS

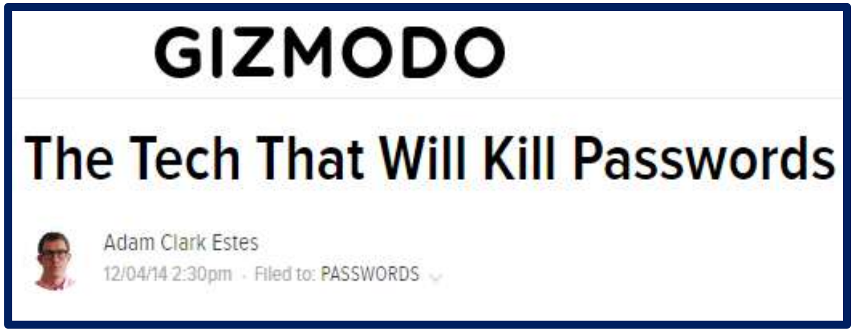
Russian credential theft shows why the password is dead

It's way past time for companies to implement strong authentication measures

WHY A FORMER OLYMPIC ATHLETE WANTS TO KILL YOUR PASSWORD



Google aims to kill passwords by the end of this year



The Tech That Will Kill Passwords

Adam Clark Estes

12/04/14 2:30pm · Filed to: PASSWORDS

Why Passwords?

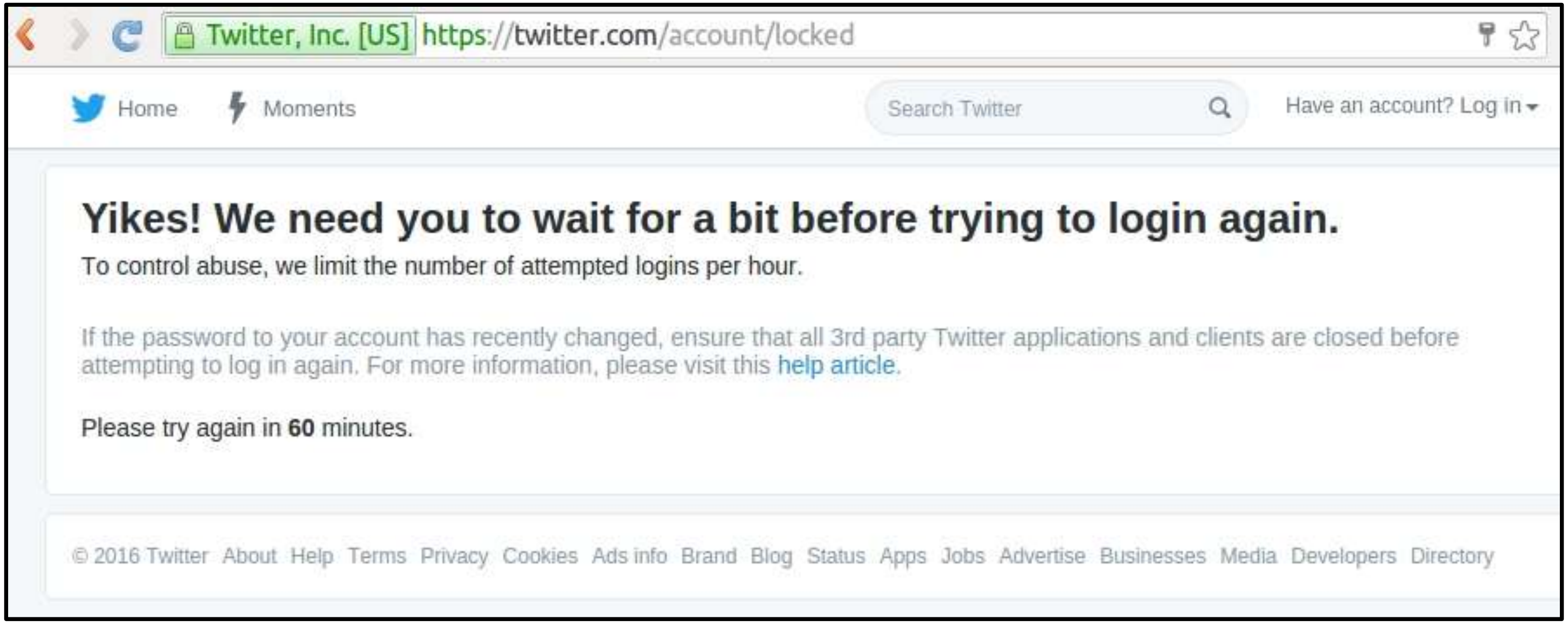
- Familiar to people
- Nothing to carry
- Difficult to coerce
- Easy to deploy, revoke, and replace

Threats to Password Security

- Online attack against live system

Threats to Password Security

- Online attack against live system
  - Rate-limiting



Yikes! We need you to wait for a bit before trying to login again.

To control abuse, we limit the number of attempted logins per hour.

If the password to your account has recently changed, ensure that all 3rd party Twitter applications and clients are closed before attempting to log in again. For more information, please visit this help article.

Please try again in **60** minutes.

© 2016 Twitter About Help Terms Privacy Cookies Ads info Brand Blog Status Apps Jobs Advertise Businesses Media Developers Directory

Threats to Password Security

- Online attack against live system
- Attack against password-protected file
- Offline attack against stolen database

LinkedIn
Ashley Madison
Life is Short. Have an Affair.
Adobe
SONY
GAWKER
Domino's Pizza
000webhost.com
better than paid hosting
YAHOO!
STRATFOR
GLOBAL INTELLIGENCE

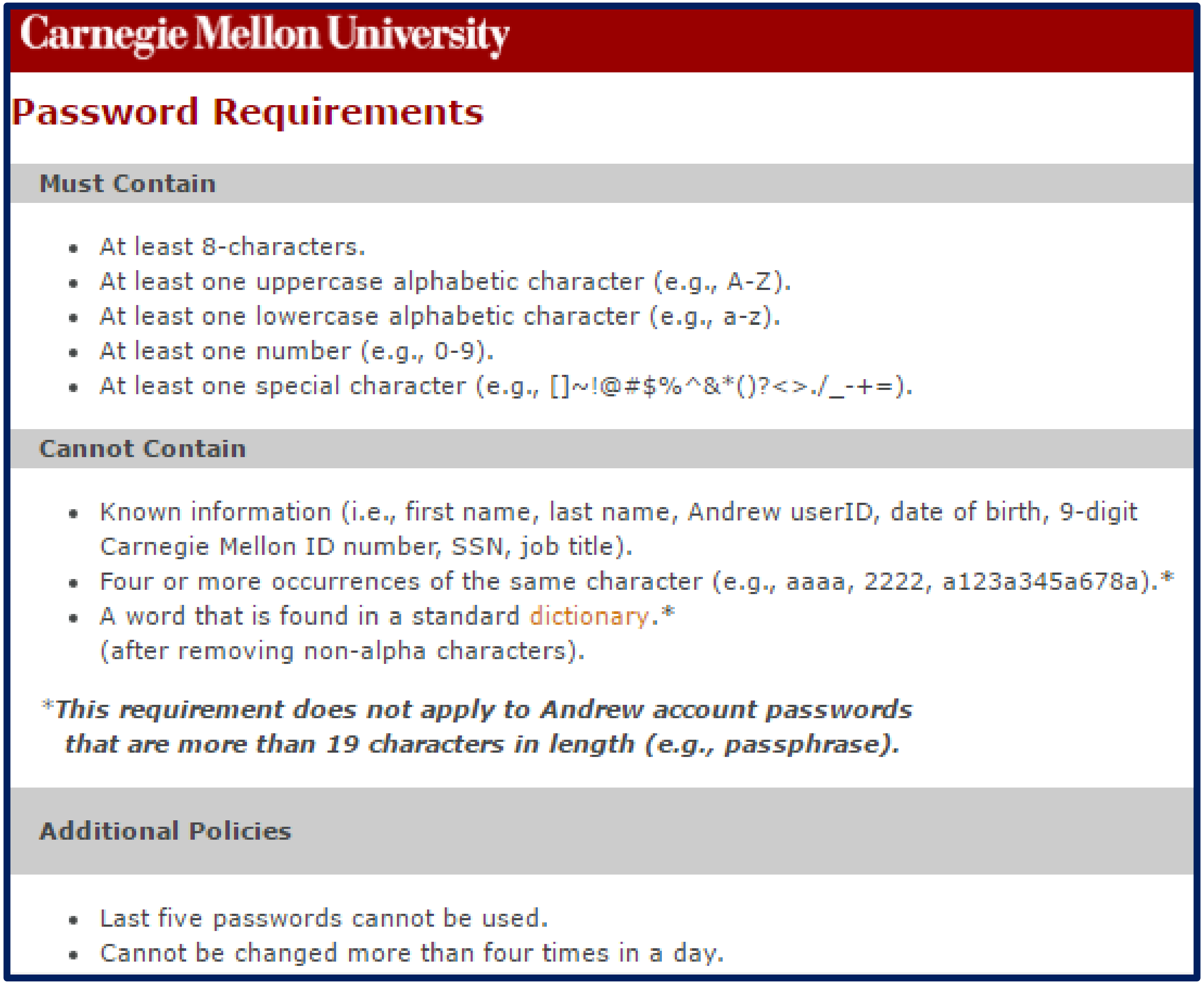
Anatomy of an Offline Attack

- Attacker compromises database
  - hash(“Blase”) =

$2a$04$iHdEgkI681VdDMc3f7edau9phRwORvhYjqWAIb7hb4B5uFJO1g4zi

- Attacker makes and hashes guesses
- Finds match → try on other sites

Problem 1: Absurd Advice



Carnegie Mellon University

Password Requirements

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.*
  (after removing non-alpha characters).

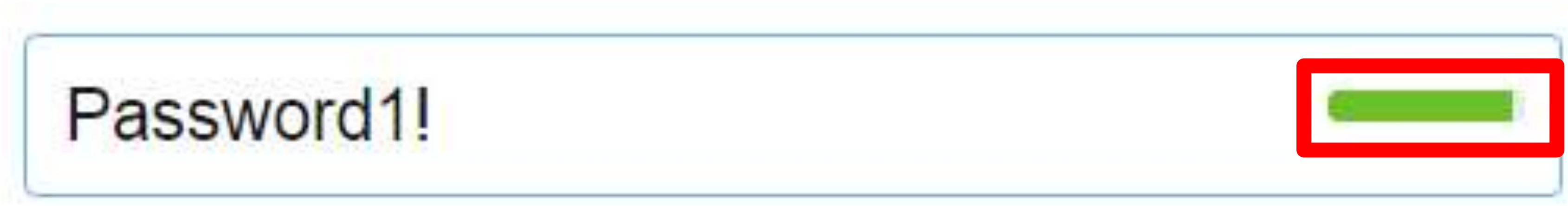
****This requirement does not apply to Andrew account passwords that are more than 19 characters in length (e.g., passphrase).***

Additional Policies

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

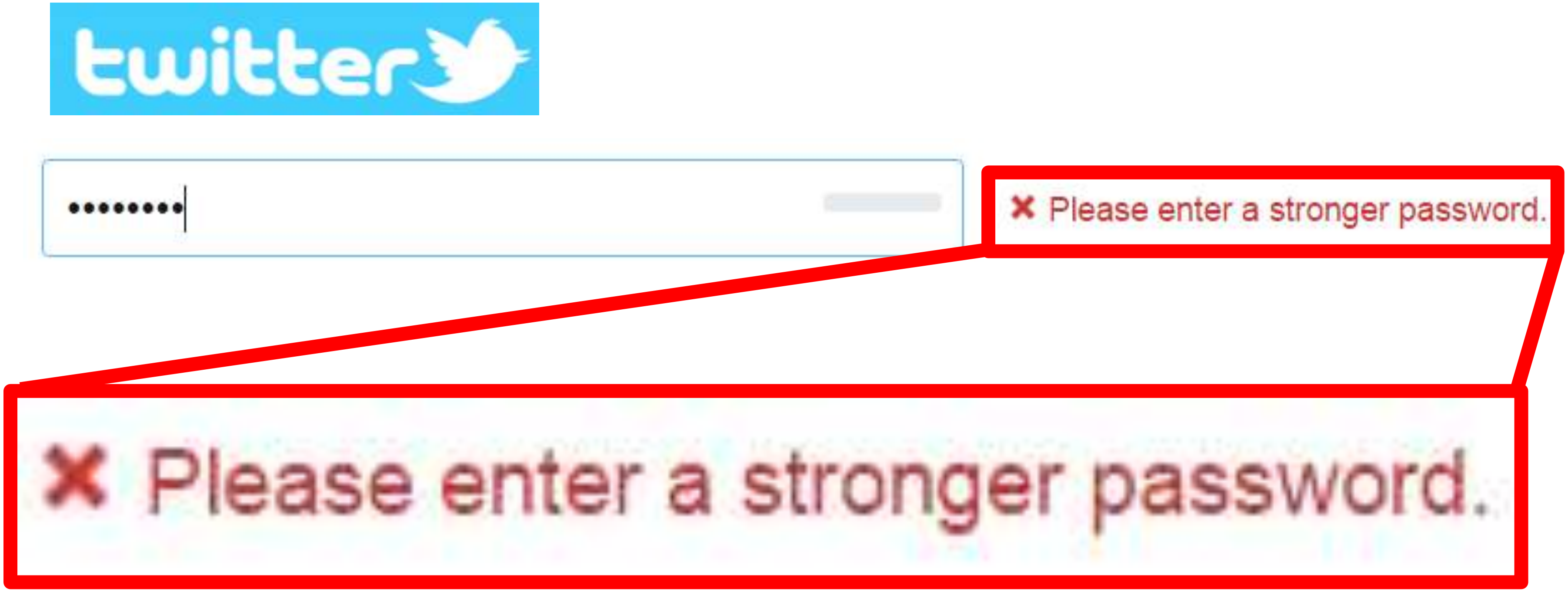
Problem 2: Inaccurate Feedback

twitter



Password1!

Problem 3: Unhelpful Feedback



•••••••••

✖ Please enter a stronger password.

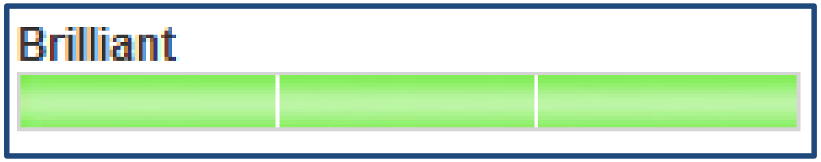
✖ Please enter a stronger password.

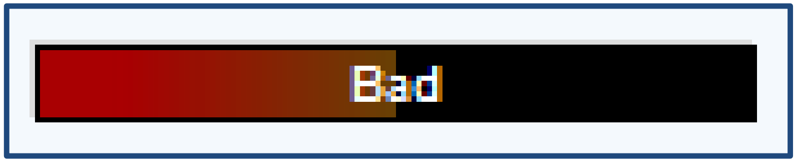
1. Impact of password meters
2. Modeling password cracking
3. Password perceptions
4. Neural-network-based guessing
5. Building a data-driven meter

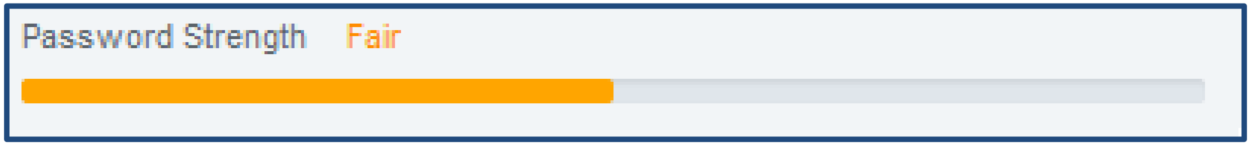
Meters' Security & Usability Impact

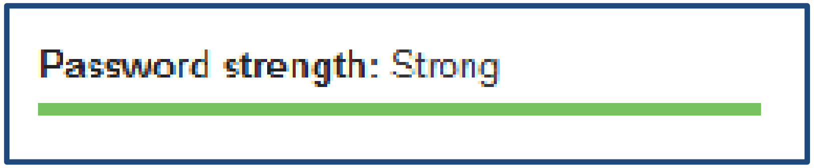
Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In *Proc. USENIX Security Symposium*, 2012.

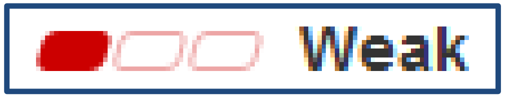
Meters Are Ubiquitous

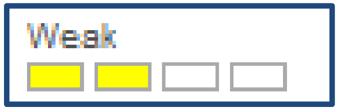

Brilliant

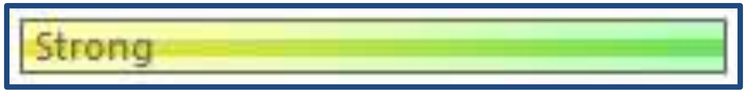

Bad

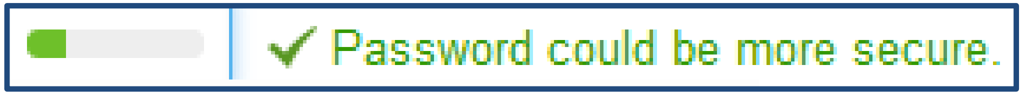

Password Strength Fair


Password strength: Strong


Weak


Weak

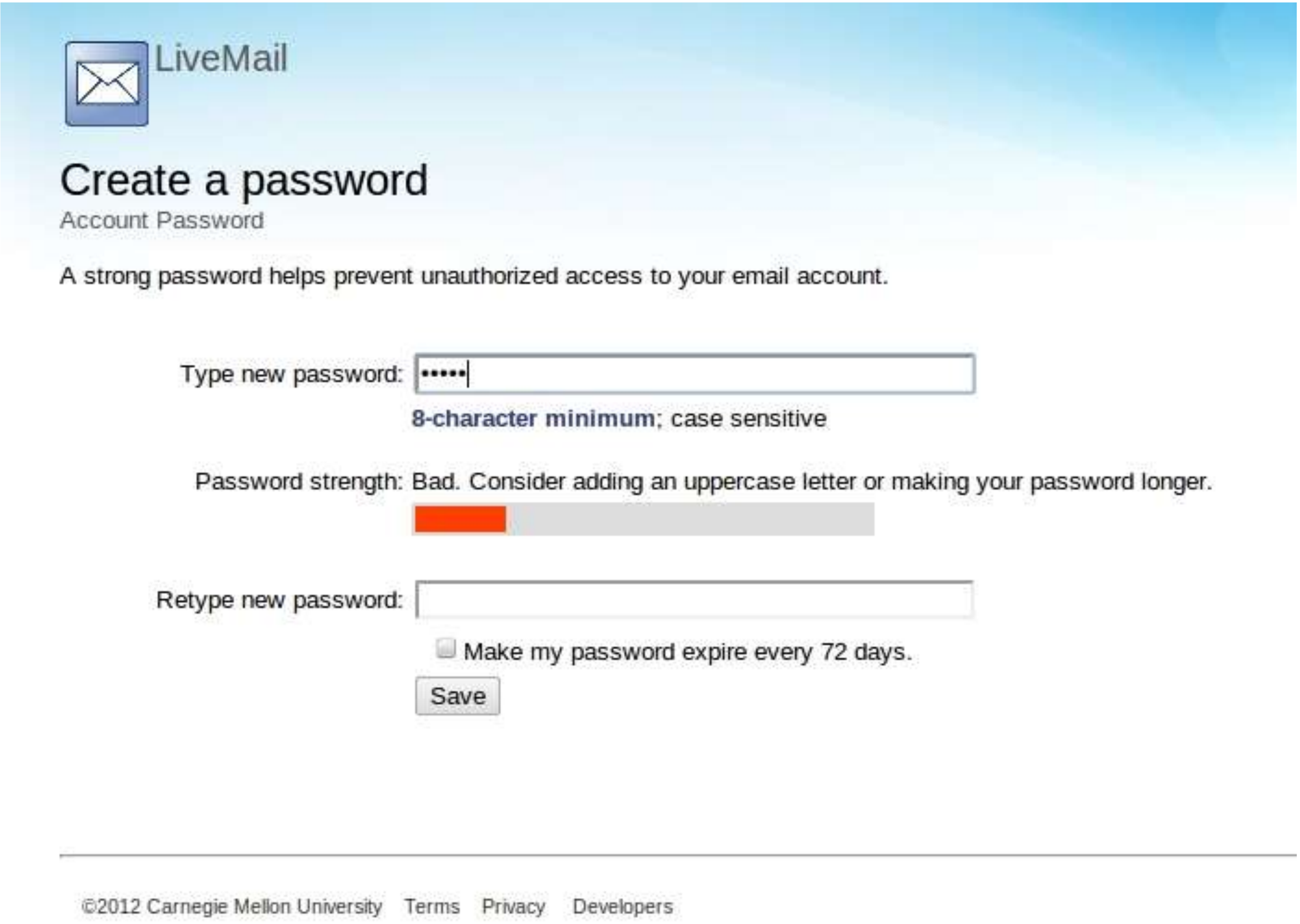

Strong


✓ Password could be more secure.

Test Meters' Impact

- How do meters impact password security?
- How do meters impact usability?
  - Memorability
  - User sentiment
  - Timing
- What meter features matter?
- 2,931-participant online study

Baseline Password Meter



LiveMail

Create a password

Account Password

A strong password helps prevent unauthorized access to your email account.

Type new password: •••••

8-character minimum; case sensitive

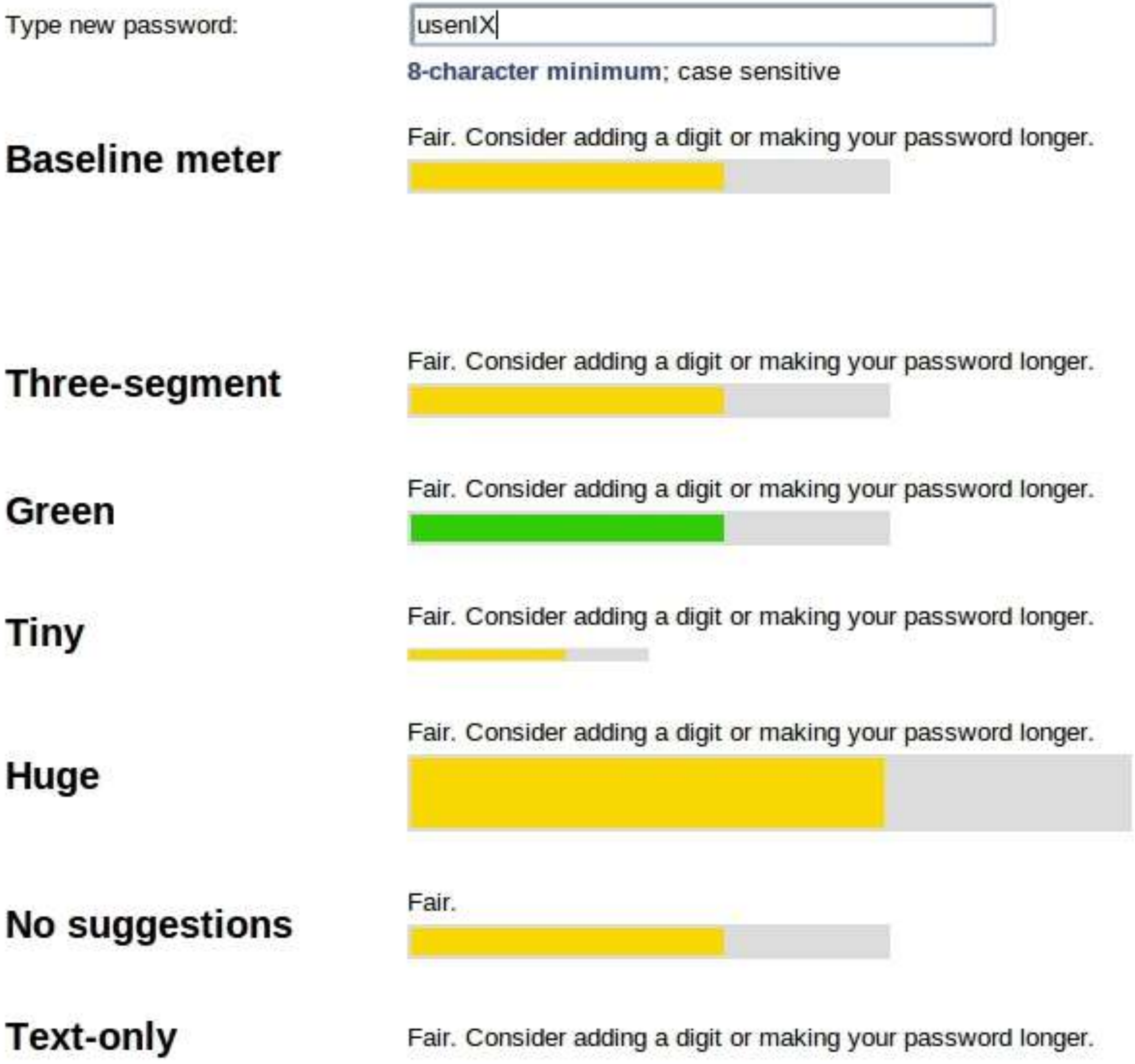
Password strength: Bad. Consider adding an uppercase letter or making your password longer.

Retype new password:

□ Make my password expire every 72 days.

©2012 Carnegie Mellon University Terms Privacy Developers

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.

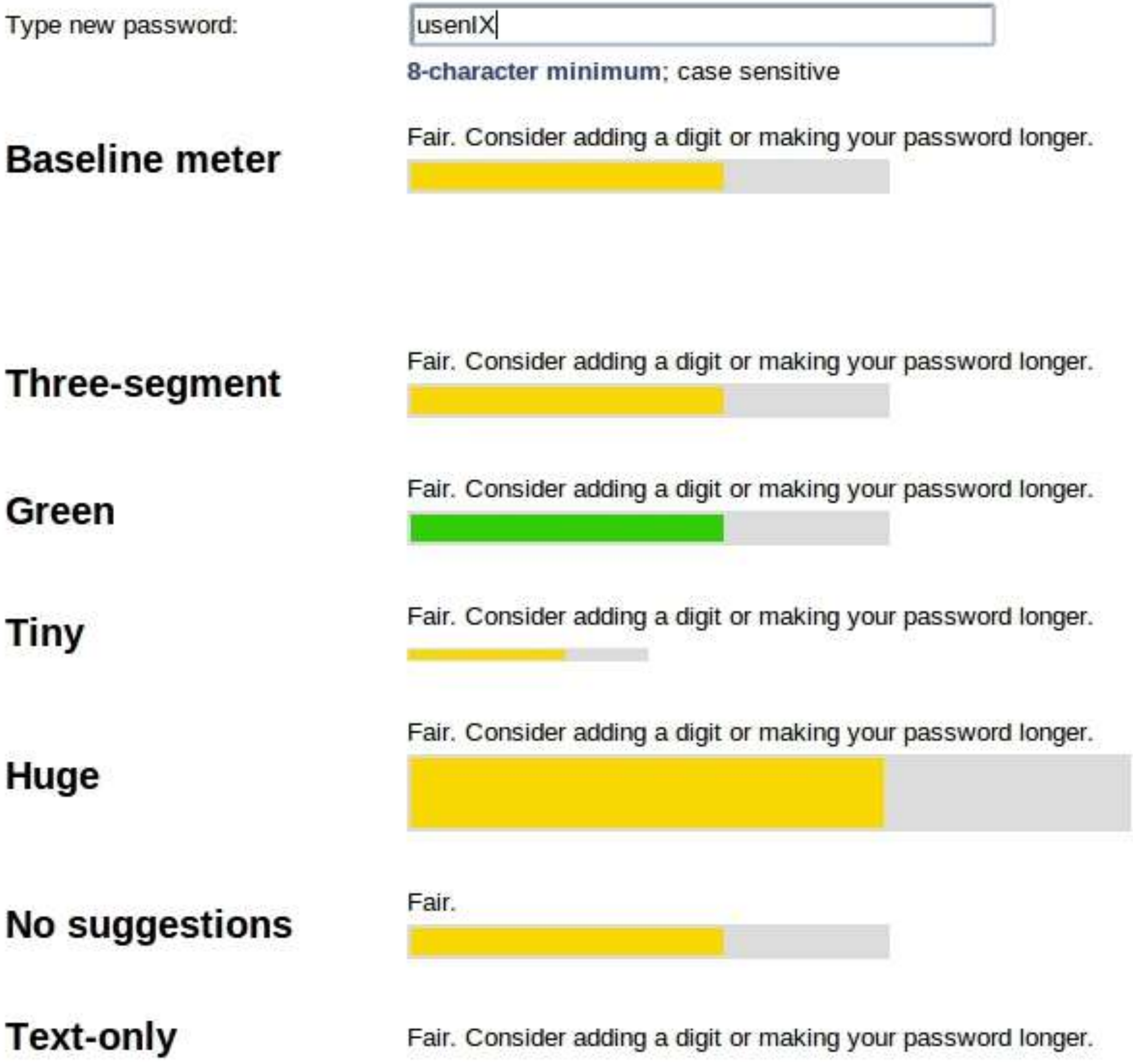
No suggestions

Fair.

Text-only

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

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.

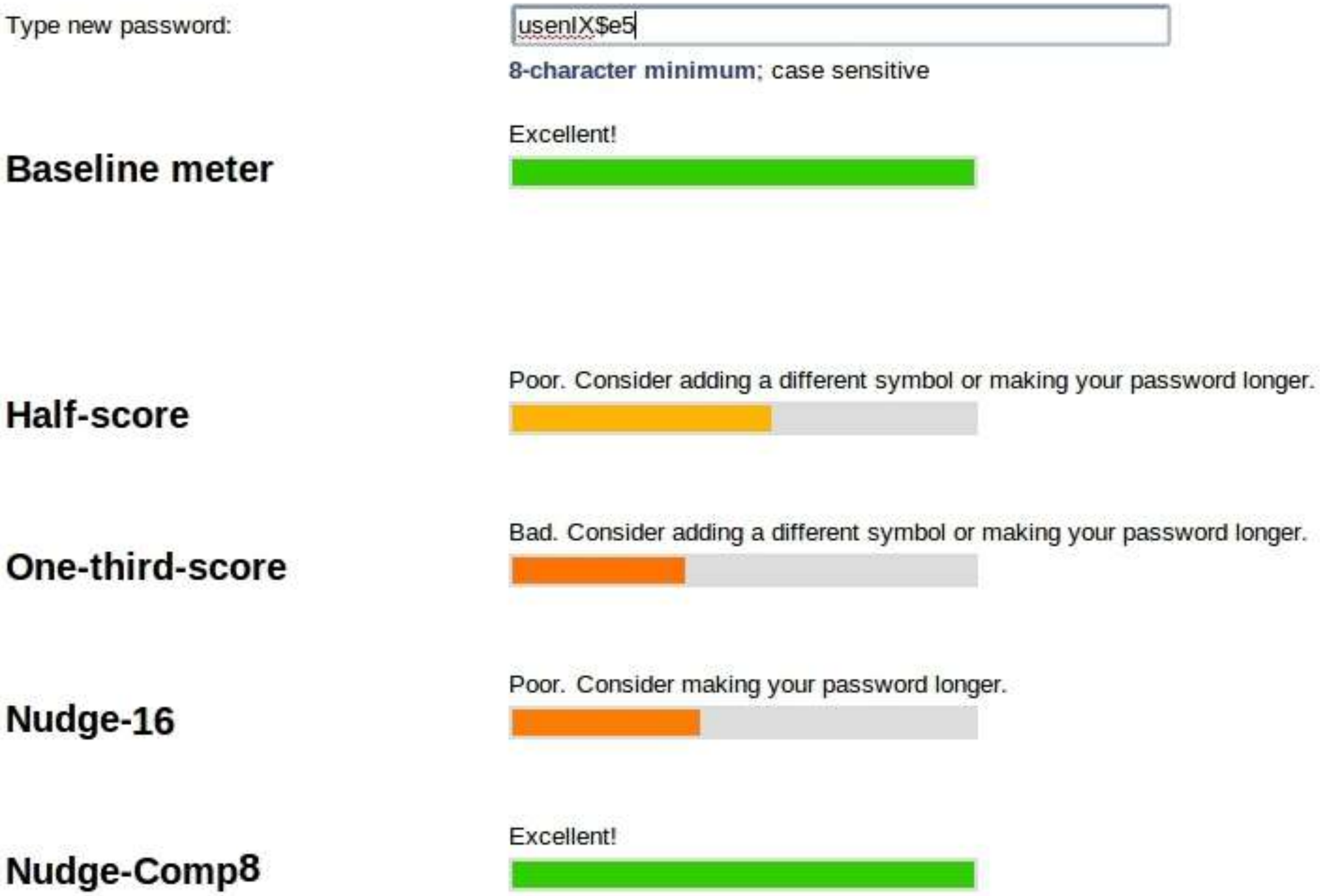
No suggestions

Fair.

Text-only

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

Scoring Differences



Type new password: usenIX$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-16

Poor. Consider making your password longer.

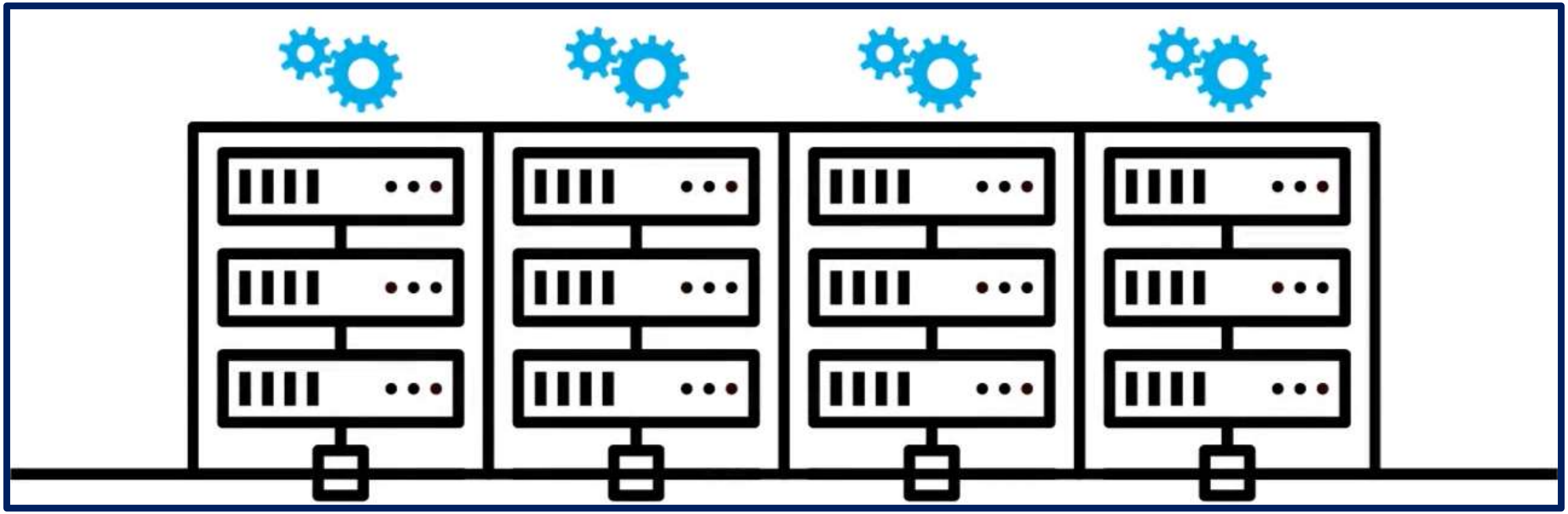
Nudge-Comp8

Excellent!

Key Results

- Stringent meters with visual bars increased resistance to guessing
- Visual differences did not significantly impact resistance to guessing
- No significant impact on memorability

Modeling Password Cracking



Blase Ur, Sean M. Segreti, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Saranga Komanduri, Darya Kurilova, Michelle L. Mazurek, William Melicher, Richard Shay. Measuring Real-World Accuracies and Biases in Modeling Password Guessability. In *Proc. USENIX Security Symposium*, 2015.

Password-Strength Metrics

- Statistical approaches
  - Traditionally: Shannon entropy
  - Recently: α-guesswork
- Disadvantages for researchers
  - Usually no per-password estimates
  - Huge sample required
  - Not real-world attacks

Parameterized Guessability

- How many guesses a particular cracking algorithm with particular training data would take to guess a password

```
j@mesb0nd007!
```

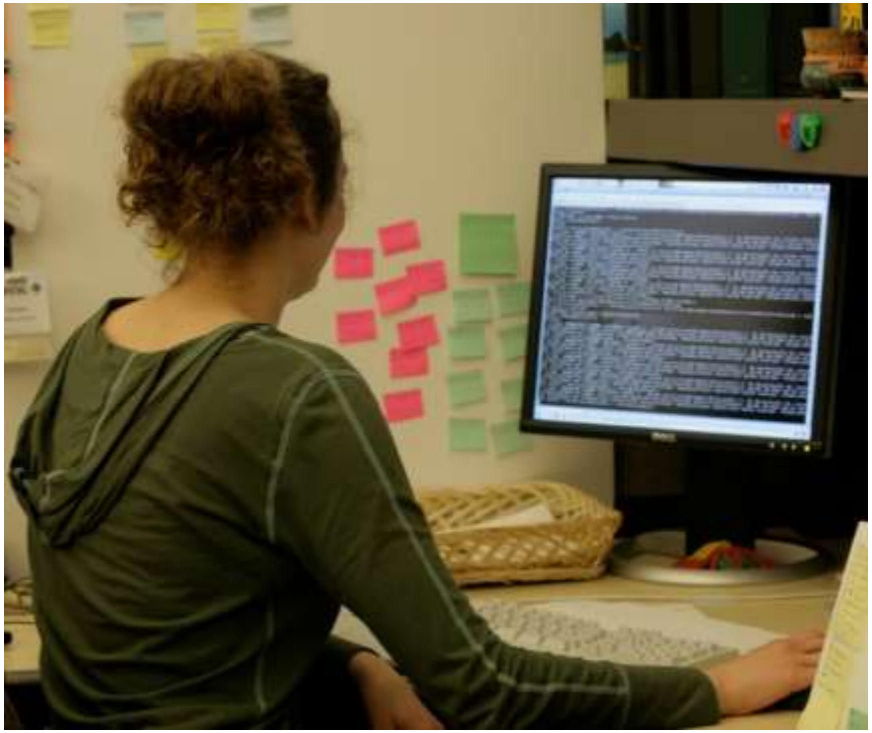
Guess # 366,163,847,194

```
n(c$JZX!zKc^bIAX^N
```

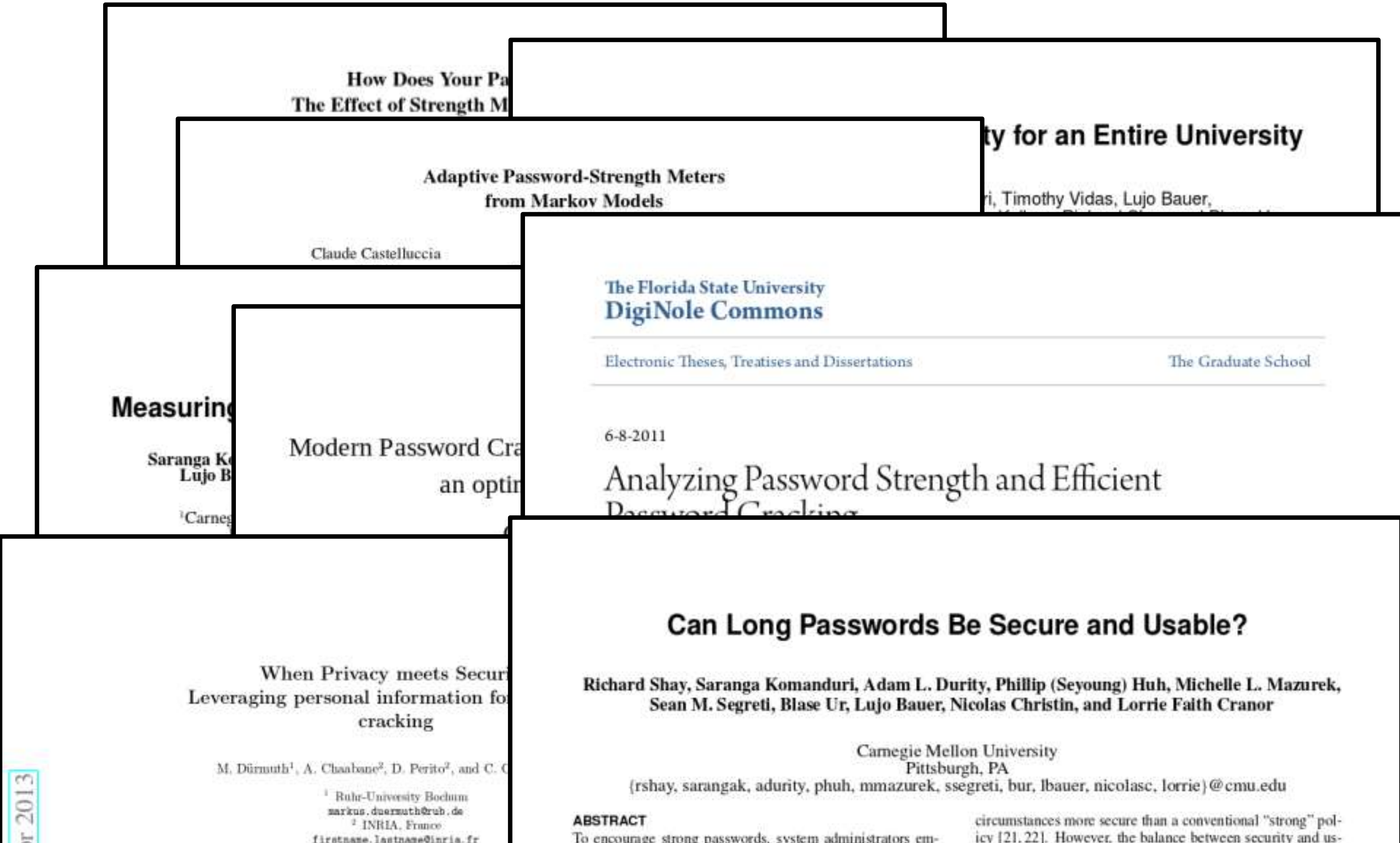
Guess # past cutoff

Guessability in Practice

Guessability in Practice



Single Cracking Approach



How Does Your Pa
The Effect of Strength M

ty for an Entire University

i, Timothy Vidas, Lujo Bauer,

Adaptive Password-Strength Meters
from Markov Models

Claude Castelluccia

The Florida State University
DigiNole Commons

Electronic Theses, Treatises and Dissertations

The Graduate School

6-8-2011

Analyzing Password Strength and Efficient
Password Cracking

Measurin

Saranga K
Lujo B

[1]Carneg

Modern Password Cra
an optir

When Privacy meets Secur
Leveraging personal information fo
cracking

M. Dürmuth[1], A. Chaabane[2], D. Perito[2], and C. C

[1] Ruhr-University Bochum
markus.duermuth@rub.de
[2] INRIA, France
firstname.lastname@inria.fr

r 2013

Can Long Passwords Be Secure and Usable?

Richard Shay, Saranga Komanduri, Adam L. Durity, Phillip (Seyoung) Huh, Michelle L. Mazurek, Sean M. Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor

Carnegie Mellon University
Pittsburgh, PA
{rshay, sarangak, adurity, phuh, mmazurek, ssegreti, bur, lbauer, nicolasc, lorrie}@cmu.edu

ABSTRACT

To encourage strong passwords, system administrators em-

circumstances more secure than a conventional "strong" policy [21, 22]. However, the balance between security and us-

Default Configuration

Of Password
Measuring the Effect of Pas

Saranga Komanduri[1], Richard Shay[1], Pa

On The Ecological Validi

Sascha Fahl, Marian Harbach, Y
Usable Security and P
...versity Ha
smith@

topic
pass-
study

Improving Text Passwords Through Persuasion

Alain Forget[1,2], Sonia Chiasson[1,2], P.C. van Oorschot[1], Robert Biddle[2]
[1]School of Computer Science & [2]Human Oriented Technology Lab
Carleton University, Ottawa, Canada
{aforget, chiasson, paulv}@scs.carleton.ca, robert_biddle@carleton.ca

A Study of User Password Strategy for Multiple Accounts

S M Taiabul Haque
Department of C
University of Texas at
Arlington,TX USA 7
eresh03@gmail

Matthew Wright

Shannon Scielzo

ABSTRACT

Despite advances in biometrics
words remain the most common
tion in computer systems. User
levels for different passwords.
the degree of similarity among
rity levels of a user. We conduc
with 80 students from a public
United States. We asked the su

The Tangled Web of Passw

Anupam Das*, Joseph Bonneau†, Matthew Caesar*, Nikita Boris
*University of Illinois at Urbana-Champaign
{das17, caesar, nikita}@illinois.edu

From *Very Weak* to *Very Strong*:
Analyzing Password-Strength Meters

Xavier de Carné de Carnavalet and Mohammad Mannan
Concordia Institute for Information Systems Engineering
Concordia University, Montreal, Canada

International Journal of Innovative Computing, Information and Control
Volume **9**, Number **2**, February **2013**

ICIC International ©2013 ISSN 1349-4198
pp. 821–836

PASSWORD CRACKING BASED ON LEARNED PATTERNS
FROM DISCLOSED PASSWORDS

Hsien-Cheng Chou[1], Hung-Chang Lee[2], Hwan-Jeu Yu[1], Fei-Pei Lai[1,3]
Kuo-Hsuan Huang[1] and Chih-Wen Hsueh[1]

[1]Department of Computer Science and Information Engineering
[3]Graduate Institute of Biomedical Electronics and Bioinformatics
National Taiwan University
No. 1, Section 4, Roosevelt Road, Taipei 10617, Taiwan
{ d96922034; flai }@csie.ntu.edu.tw; ecpro@seed.net.tw

[2]Department of Information Management
Tamkang University
No. 151, Yingzhuan Road, Tamsui District, New Taipei City 25137, Taiwan
hclee@mail.im.tku.edu.tw

The Florida State University
DigiNole Commons

Electronic Theses, Treatises and Dissertations

The Graduate School

6-8-2011

Analyzing Password Strength and Efficient
Password Cracking

Shiva Houshmand Yazdi
Florida State University

Questions About Guessability

1) How does guessability used in research compare to an attack by professionals?
2) Would substituting another cracking approach impact research results?

Approach

4 password sets ✖ 5 approaches

password
iloveyou
teamo123
…

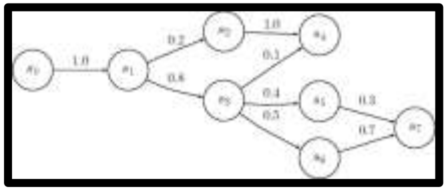
passwordpassword
1234567812345678
!1@2#3$4%5^6&7*8
…

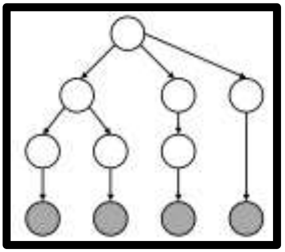
Pa$$w0rd
iLov3you!
1QaZ2W@x
…

pa$$word1234
12345678asDF
!q1q!q1q!q1q
…

John the Ripper

hashcat
advanced
password
recovery





KoreLogic
SECURITY

Key Results

- Configuration is critical
- Considering single approach insufficient
  - Multiple approaches proxy for pros
- Analyses of password sets robust
  - More granular analyses not robust

Per-Password Highly Impacted

`P@ssw0rd!`

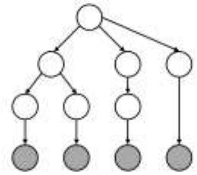
Per-Password Highly Impacted

- JTR guess # 801

P@ssw0rd!

Per-Password Highly Impacted

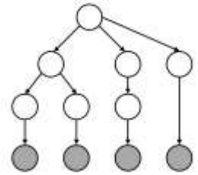
- JTR guess # 801
- Not guessed in 10^{14} PCFG guesses



P@ssw0rd!

Per-Password Highly Impacted

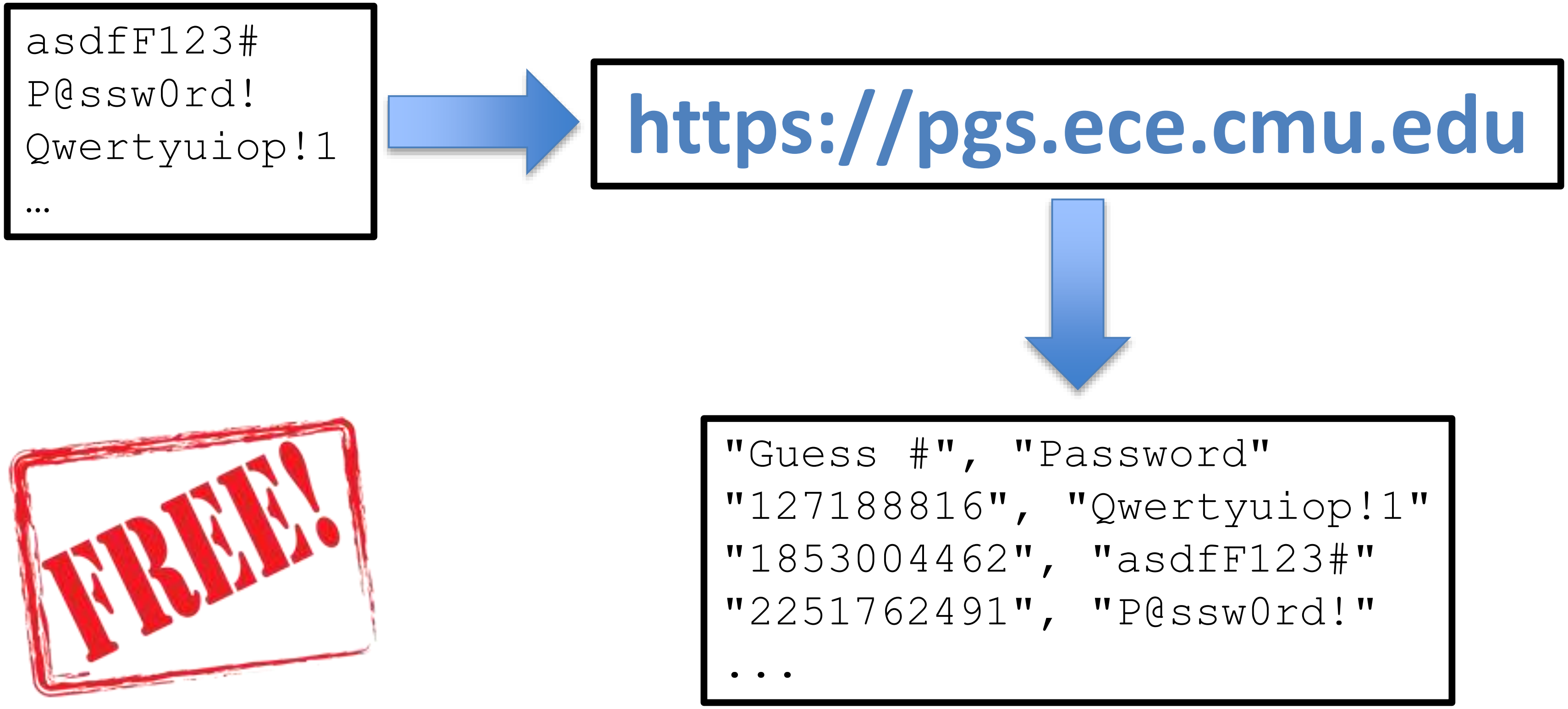
- JTR guess # 801
- Not guessed in 10^{14} PCFG guesses



P@ssw0rd!

Password Guessability Service

- Guessability of plaintext passwords



```
asdfF123#
P@ssw0rd!
Qwertyuiop!1
…
```

https://pgs.ece.cmu.edu

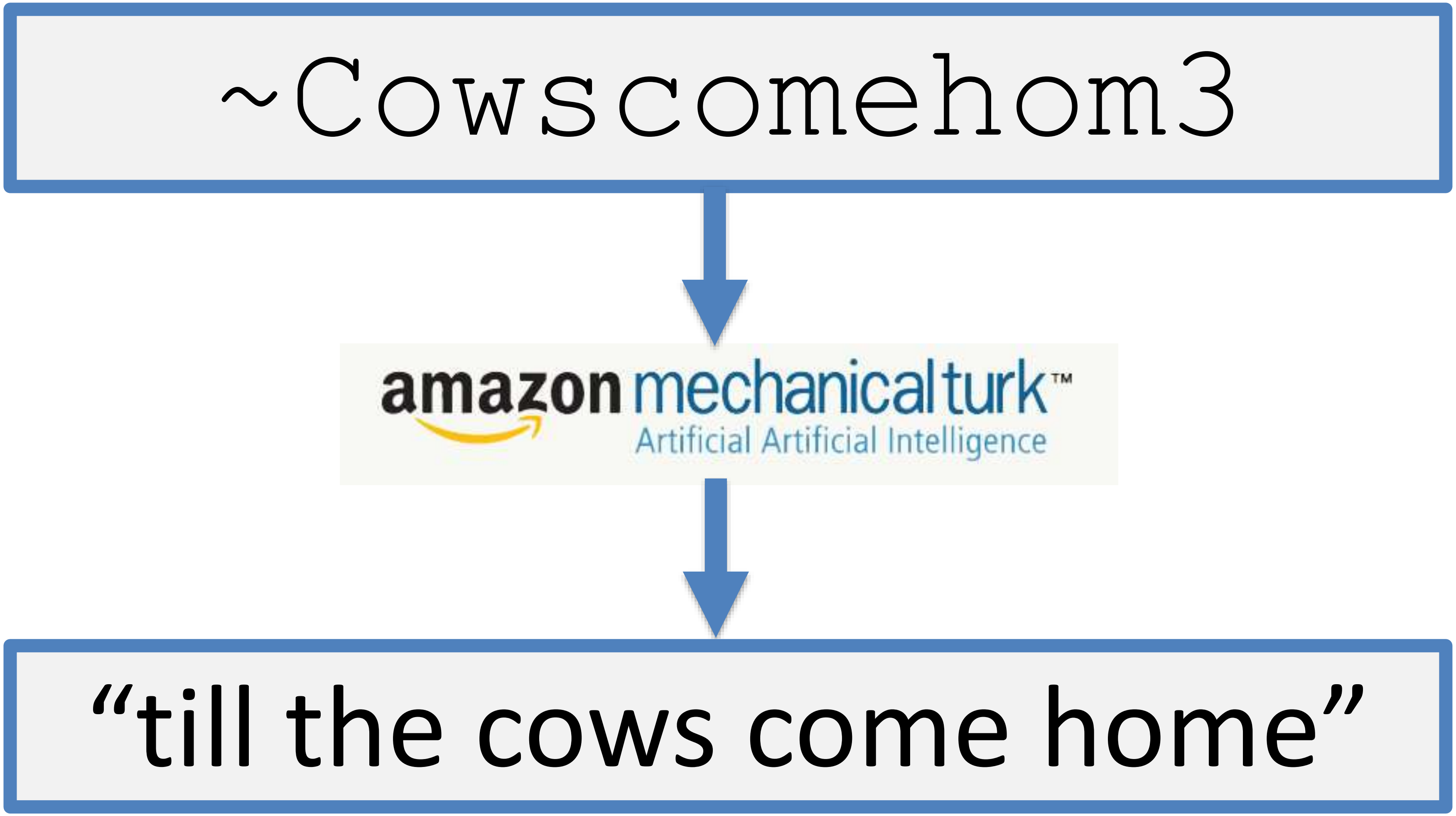
```
"Guess #", "Password"
"127188816", "Qwertyuiop!1"
"1853004462", "asdfF123#"
"2251762491", "P@ssw0rd!"
...
```

FREE!

The Art of Password Creation

Blase Ur, Saranga Komanduri, Lujo Bauer, Lorrie Faith Cranor, Nicolas Christin, Adam L. Durity, Phillip (Seyoung) Huh, Stephanos Matsumoto, Michelle L. Mazurek, Sean M. Segreti, Richard Shay, Timothy Vidas. The Art of Password Creation: Semantics, Strategies, and Strategies. Image Creative Commons by Lasya J on Flickr.

Reverse-Engineering Passwords



~Cowscomehom3

"till the cows come home"

Key Results

- Character substitutions both infrequent and predictable
- Words and phrases frequently used
  - Wikipedia excellent source of training data
- Composition policy detrimental for some

Understanding Password Creation

Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor. “I Added ‘!’ at the End to Make It Secure”: Observing Password Creation in the Lab. In *Proc. SOUPS*, 2015.

Understand Origin of Passwords

LEFTbrown8!

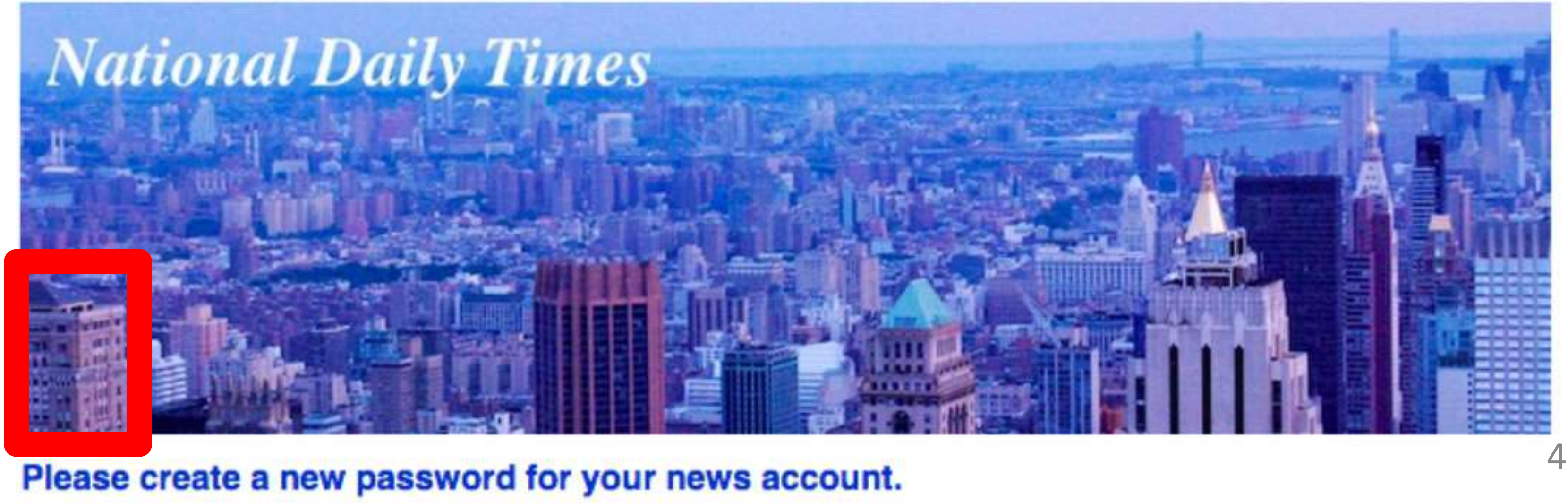
Understand Origin of Passwords

LEFTbrown8!

Please create a new password for your news account.

Understand Origin of Passwords

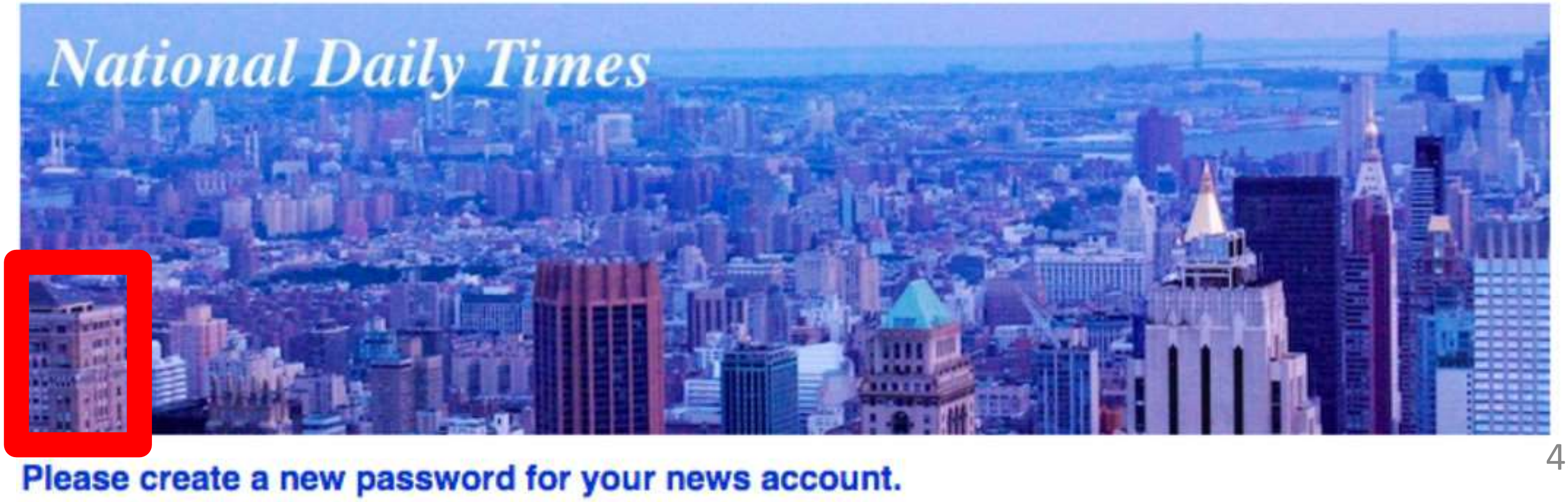
LEFTbrown8!



Please create a new password for your news account.

Understand Origin of Passwords

`LEFTbrown8!`



Please create a new password for your news account.

Key Results

- Important misconceptions
  - Digits and symbols
  - Keyboard patterns
  - Dictionary words
- Misallocation of effort in password creation

Perceptions of Password Security

Blase Ur, Jonathan Bees, Sean M. Segreti, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor. Do users' perceptions of password security match reality? In *Proc. CHI*, 2016.

Perception vs. Reality

Compare actual strength of passwords to users' perceptions

Measuring Perceptions

- Online study
  - Compensated $5 for ~30 minutes
- 165 participants from Mechanical Turk
  - Age 18+, live in United States
  - Median age 33
  - 49% female, 51% male
  - 16% CS or related degree or job
  - 4% student/professional in computer security

Study Tasks

1. Evaluating password pairs

Study Tasks

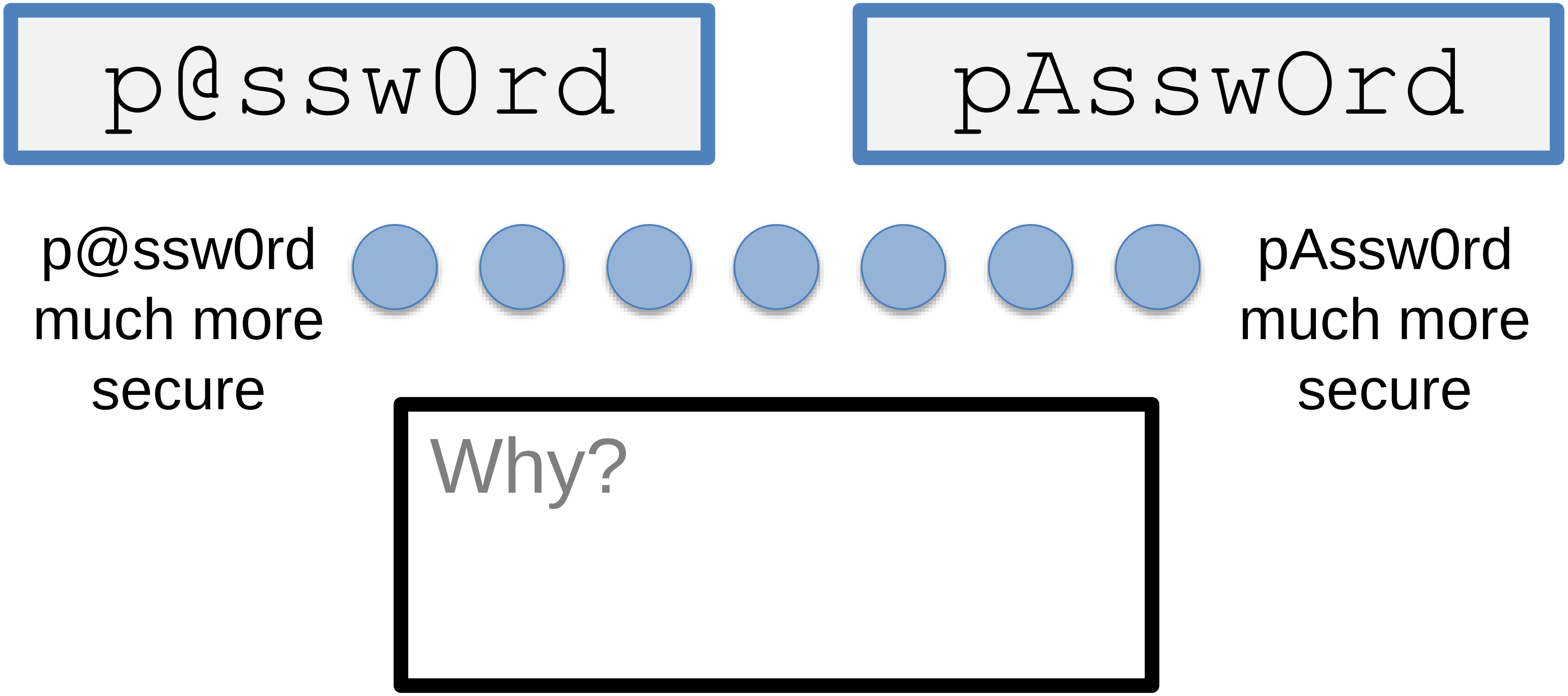
1. Evaluating password pairs

`p@ssw0rd` `pAssw0rd`

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

Study Tasks

1. Evaluating password pairs



p@ssw0rd

pAssw0rd

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

Why?

Task 1 Hypotheses

- 25 common characteristics, e.g.,
    - Capitalization
    - Letters vs. digits vs. symbols
    - Choice of words and phrases

Task 1 Hypotheses

- 25 common characteristics, e.g.,
  - Capitalization
  - Letters vs. digits vs. symbols
  - Choice of words and phrases
- Created 3 pairs per hypothesis
  - Randomly chose 1 pair per participant

Task 1 Hypotheses

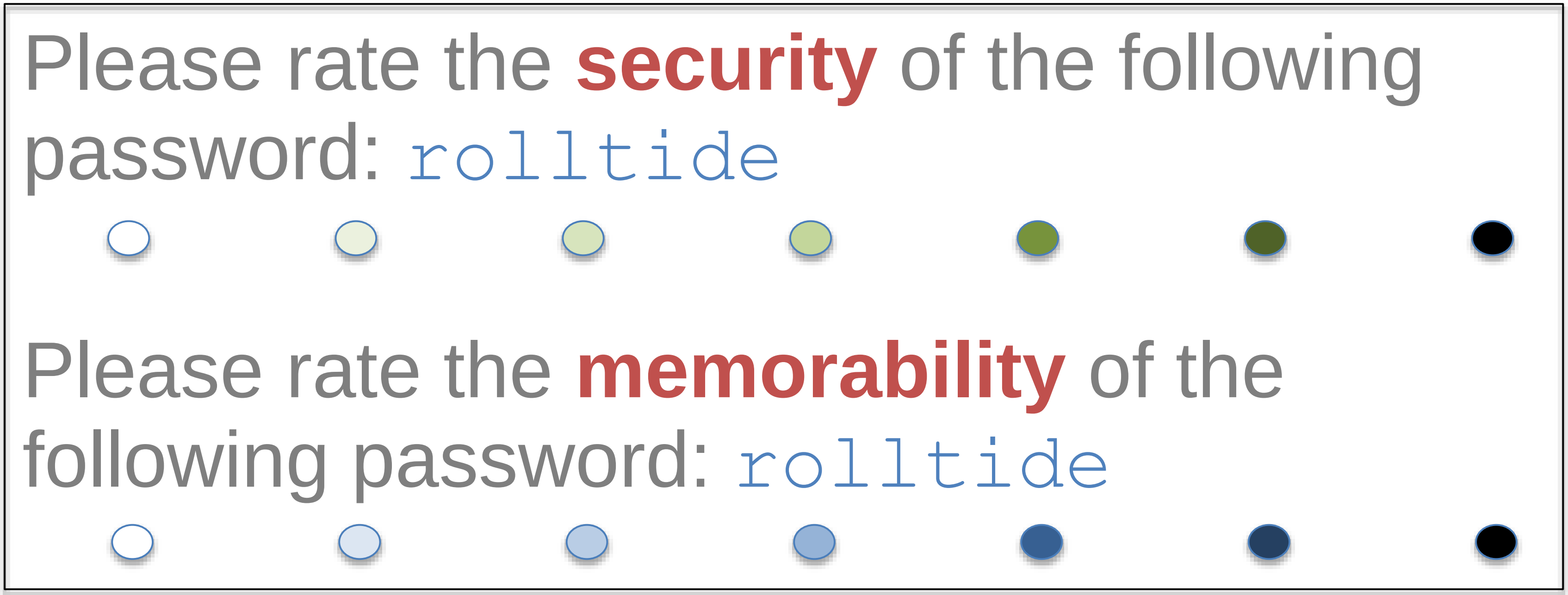
- 25 common characteristics, e.g.,
  - Capitalization
  - Letters vs. digits vs. symbols
  - Choice of words and phrases
- Created 3 pairs per hypothesis
  - Randomly chose 1 pair per participant
  - At least one password per pair from rockyou

Study Tasks

1. Evaluating password pairs
2. Rating selected passwords

Study Tasks

1. Evaluating password pairs
2. Rating selected passwords



Please rate the **security** of the following password: `rolltide`

○ ○ ○ ○ ○ ○ ○

Please rate the **memorability** of the following password: `rolltide`

○ ○ ○ ○ ○ ○ ○

Study Tasks

1. Evaluating password pairs
2. Rating selected passwords
3. Rating creation strategies

Study Tasks

1. Evaluating password pairs
2. Rating selected passwords
3. Rating creation strategies
4. Describing attackers
   - Who, why, how

Results

1. Evaluating password pairs
2. Rating selected passwords
3. Rating creation strategies
4. Describing attackers

Evaluating Password Pairs

`iloveyou88`

`ieatkale88`

Evaluating Password Pairs

`iloveyou88`

`ieatkale88`

Image Creative Commons by Jinx! (span112) on Flickr

Evaluating Password Pairs

`iloveyou88`

`ieatkale88`

Image Creative Commons by Jinx! (span112) on Flickr

Evaluating Password Pairs

`iloveyou88`

`ieatkale88`

4,000,000,000 × more secure!

Evaluating Password Pairs

`brooklyn16`

`brooklynqy`

Evaluating Password Pairs

brooklyn16

brooklynqy

Image Creative Commons by Jinx! (span112) on Flickr

Evaluating Password Pairs

brooklyn16

brooklynqy

Image Creative Commons by Jinx! (span112) on Flickr

Evaluating Password Pairs

`brooklyn16`

`brooklynqy`

300,000 × more secure!

Ways People Were Wrong

- Overstated security benefits of:
  - Digits
  - Character substitutions (e.g., a→@)
  - Keyboard patterns (e.g., 1qaz2wsx3edc)
- Did not recognize common words/phrases

Many Ways People Were Right

- Capitalize letters other than the first
- Put digits and symbols in middle, not end
- Use symbols rather than digits
- Avoid:
  - Common first names
  - Words related to account
  - Years and sequences

If perceptions of many individual characteristics are correct, then why do people make bad passwords?

Perceptions of Attackers

Images Creative Commons by Stephen C. Webster, Jinx! (span112), and Adam Thomas on Flickr, and on Wikimedia

Perception: How Many Guesses?

Perception: How Many Guesses?

- 2 guesses (Min)

Perception: How Many Guesses?

- 2 guesses (Min)
- 100,000,000,000,000,000,000,000,000,
000,000,000,000,000,000,000,000,000,
000,000 guesses (Max)

Perception: How Many Guesses?

- 2 guesses (Min)
- 100,000,000,000,000,000,000,000,000, 000,000,000,000,000,000,000,000,000, 000,000 guesses (Max)
- 34% ≤ 50 guesses (manual attack)

Perception: How Many Guesses?

- 2 guesses (Min)
- 100,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000 guesses (Max)
- 34% ≤ 50 guesses (manual attack)
- 67% ≤ 50,000 guesses (small-scale)

Perception: How Many Guesses?

- 2 guesses (Min)
- 100,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000 guesses (Max)
- 34% ≤ 50 guesses (manual attack)
- 67% ≤ 50,000 guesses (small-scale)
- 7% ≥ 10^{14} guesses (large-scale)

Reality: How Many Guesses?

Reality: Small-Scale Guessing

Reality: Small-Scale Guessing

- Targeted guessing by someone you know

Reality: Small-Scale Guessing

- Targeted guessing by someone you know
- Automated attack by a stranger

Reality: Small-Scale Guessing

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

Reality: Large-Scale Guessing

Reality: Large-Scale Guessing

- Against stolen database of passwords

Reality: Large-Scale Guessing

- Against stolen database of passwords
- Against password-protected file

Reality: Large-Scale Guessing

- Against stolen database of passwords
- Against password-protected file
- 1,000,000 guesses (best practices)

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)

Perception

Small-scale

67% ≤ 50,000

Reality

Small-scale…

…and large-scale

≥ 10^{14} guesses

Conclusions

Conclusions

- Perceptions of individual characteristics
  - Often consistent with current attacks
  - Some crucial differences

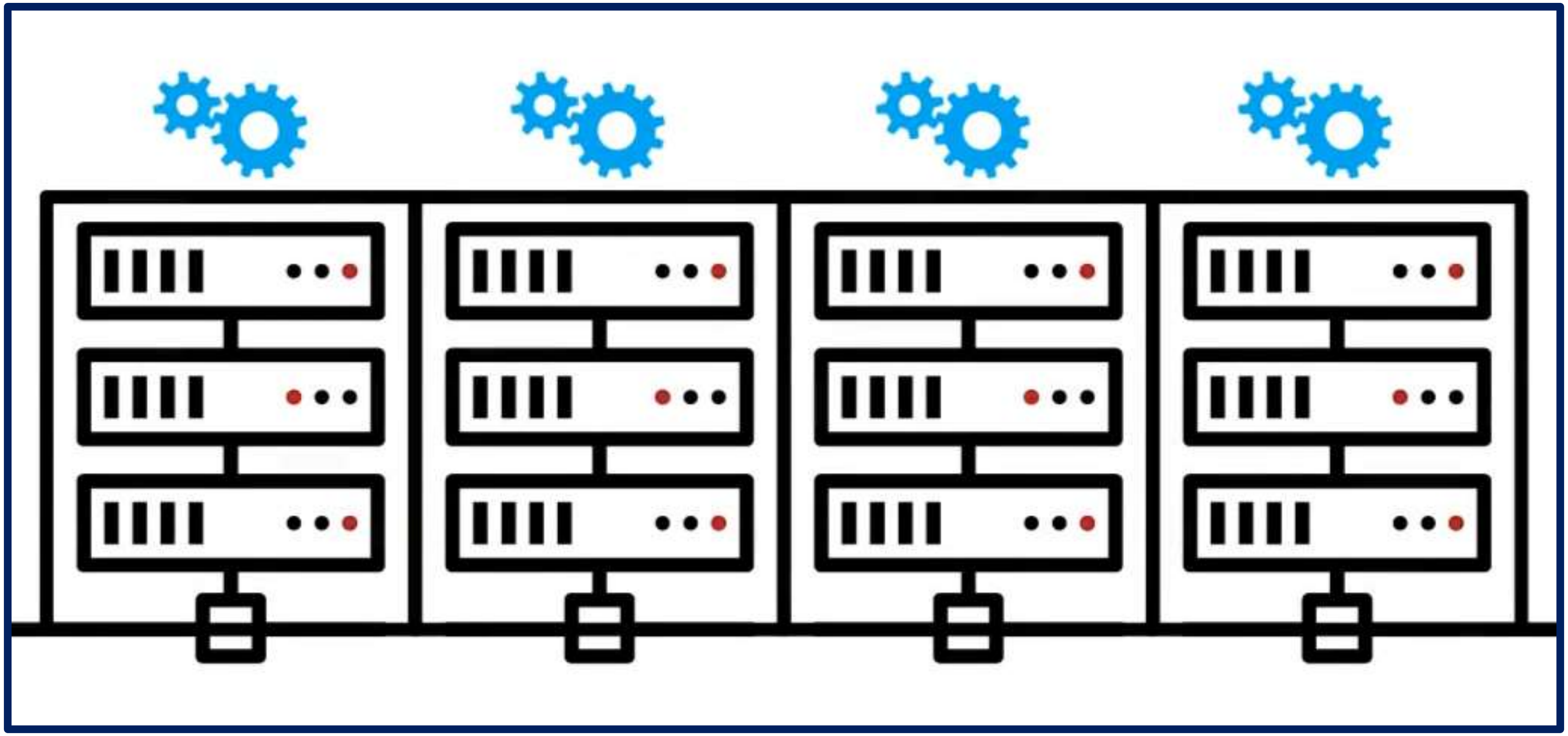
Conclusions

- Perceptions of individual characteristics
  - Often consistent with current attacks
  - Some crucial differences
- Huge variance in perceptions of attackers

Conclusions

- Perceptions of individual characteristics
  - Often consistent with current attacks
  - Some crucial differences
- Huge variance in perceptions of attackers
- Current user feedback is insufficient

Better Password Scoring



William Melicher, Blase Ur, Sean M. Segreti, Saranga Komanduri, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor. Fast, Lean, and Accurate: Modeling Password Guessability Using Neural Networks. In *Proc. USENIX Security Symposium*, 2016.

Better Password Scoring

- Real-time feedback
- Runs entirely client-side
- Accurately models password guessability

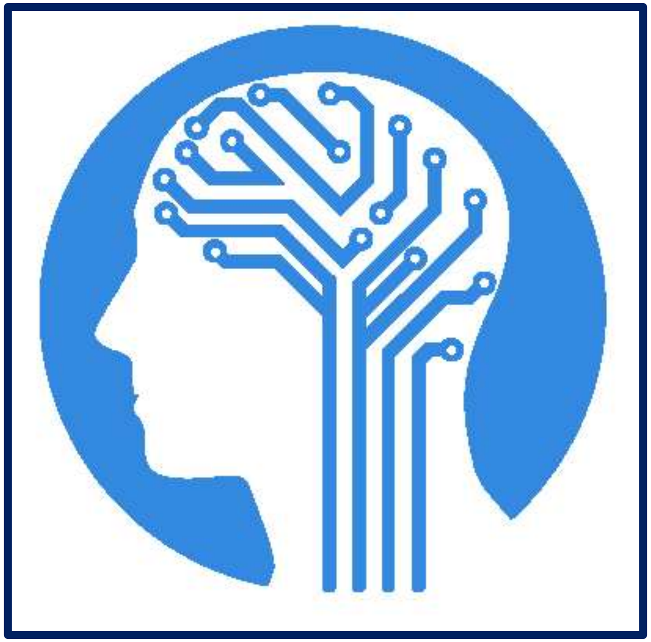


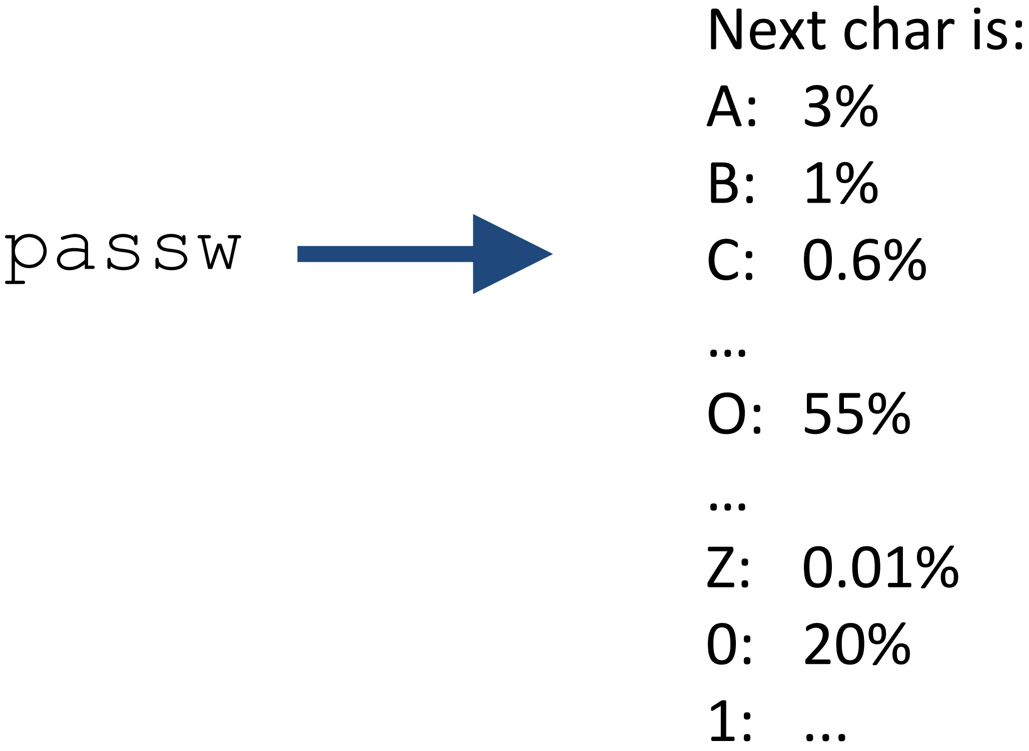
Image CC by Wes Breazell on the Noun Project

Generating Passwords

Generating Passwords

`passw` → o or maybe 0 or O or ...

Generating Passwords



`passw`

Next char is:

A:	3%
B:	1%
C:	0.6%
…	
O:	55%
…	
Z:	0.01%
0:	20%
1:	…

Generating Passwords

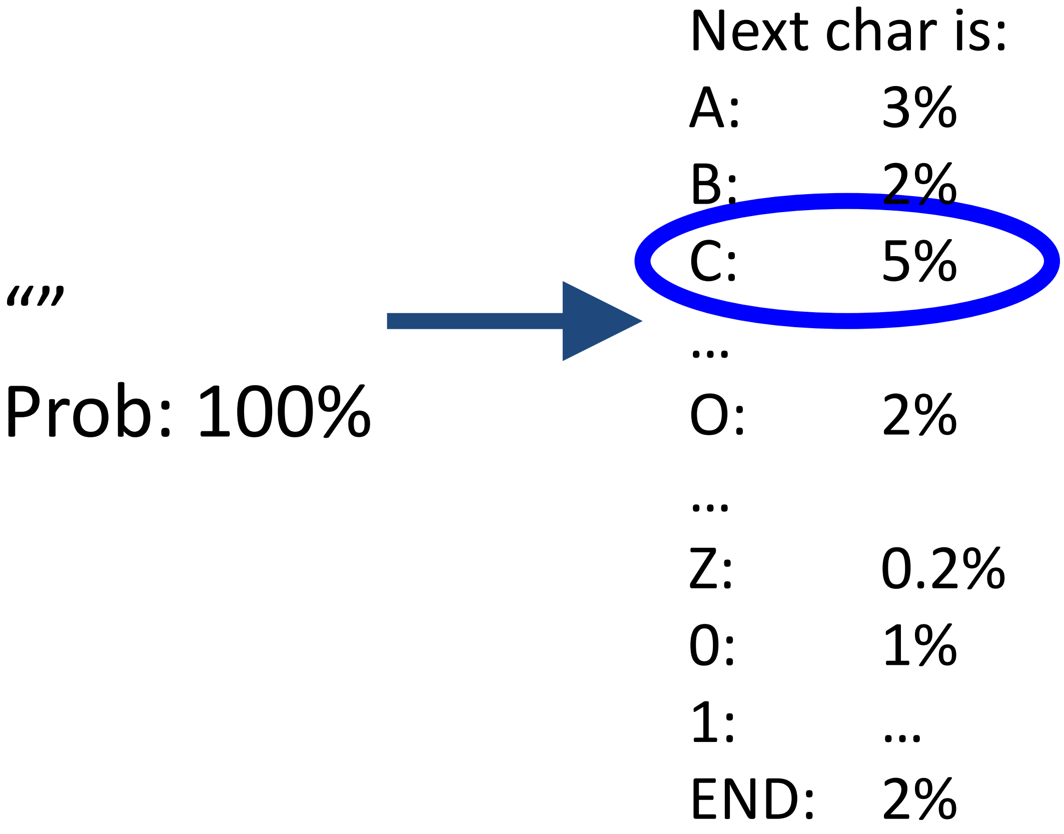
“”

Prob: 100%

Next char is:

A:	3%
B:	2%
C:	5%
…	
O:	2%
…	
Z:	0.2%
0:	1%
1:	…
END:	2%

Generating Passwords



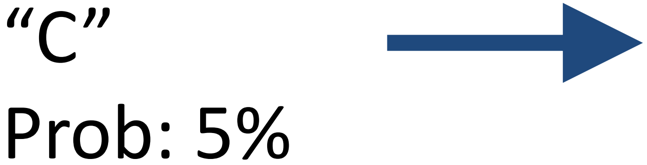
“”

Prob: 100%

Next char is:

A:	3%
B:	2%
C:	5%
…	
O:	2%
…	
Z:	0.2%
0:	1%
1:	…
END:	2%

Generating Passwords



“C”
Prob: 5%

Generating Passwords

"C"

Prob: 5%

Next char is:

A:	10%
B:	1%
C:	4%
…	
O:	8%
…	
Z:	0.02%
0:	3%
1:	…
END:	6%

Generating Passwords

"C"

Prob: 5%

Next char is:

A:	10%
B:	1%
C:	4%
…	
O:	8%
…	
Z:	0.02%
0:	3%
1:	…
END:	6%

Generating Passwords

“CA”

Prob: 0.5%

Next char is:

A:	3%
B:	10%
C:	7%
…	
O:	1%
…	
Z:	0.03%
0:	2%
1:	…
END:	12%

Generating Passwords

“CAB”

Prob: 0.05%

→

Next char is:

A:	3%
B:	10%
C:	7%
…	
O:	1%
…	
Z:	0.03%
0:	2%
1:	…
END:	3%

Generating Passwords

“CAB”

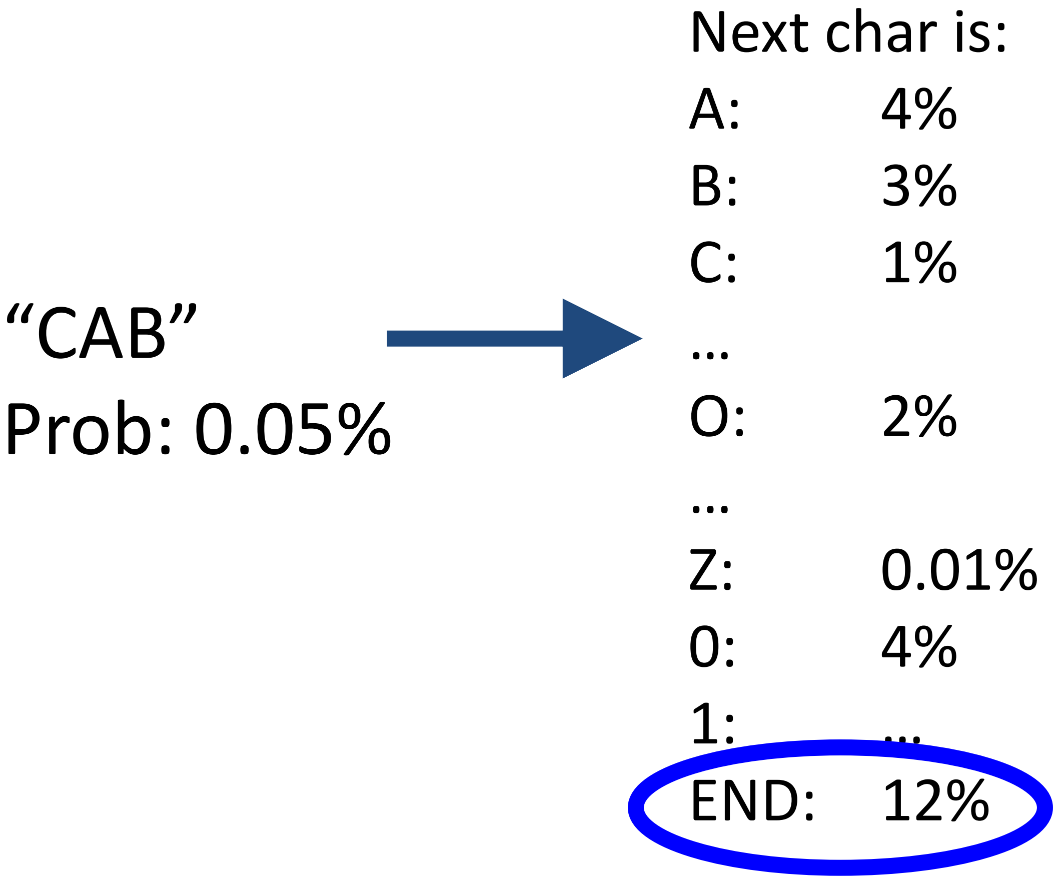
Prob: 0.05%

→

Next char is:

A:	4%
B:	3%
C:	1%
…	
O:	2%
…	
Z:	0.01%
0:	4%
1:	…
END:	12%

Generating Passwords



“CAB”

Prob: 0.05%

Next char is:

A:	4%
B:	3%
C:	1%
…	
O:	2%
…	
Z:	0.01%
0:	4%
1:	…
END:	12%

Generating Passwords

“CAB”

Prob: 0.006%

Generating Passwords

CAB -	0.006%
CAC -	0.0042%
ADD1 -	0.002%
CODE -	0.0013%

…

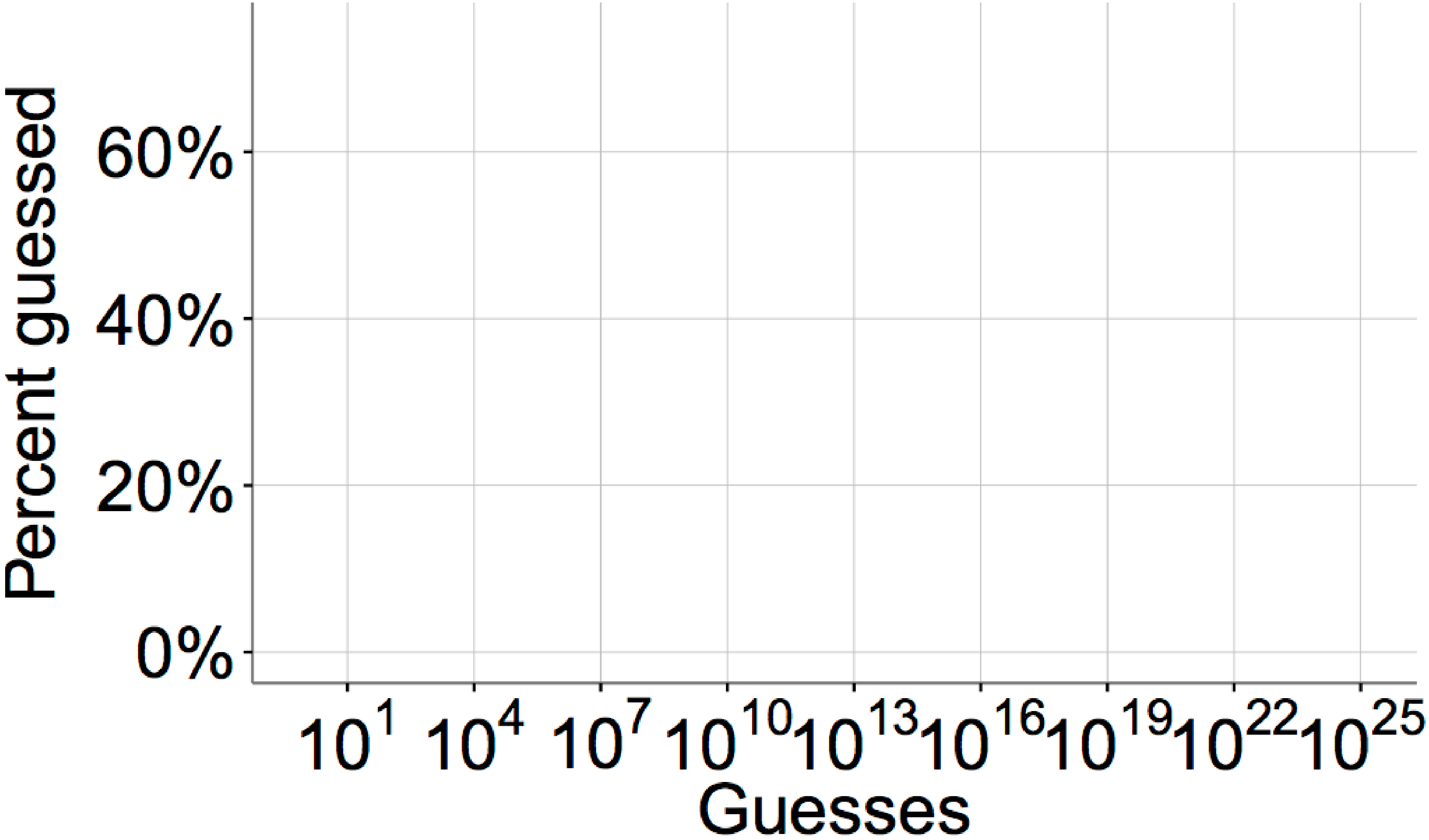
Design Space

- Model size: 3mb (browser) vs. 60mb (GPU)
- Transference learning
  - Novel password-composition policies
- Training data
  - Natural language
- (Many others)

Method

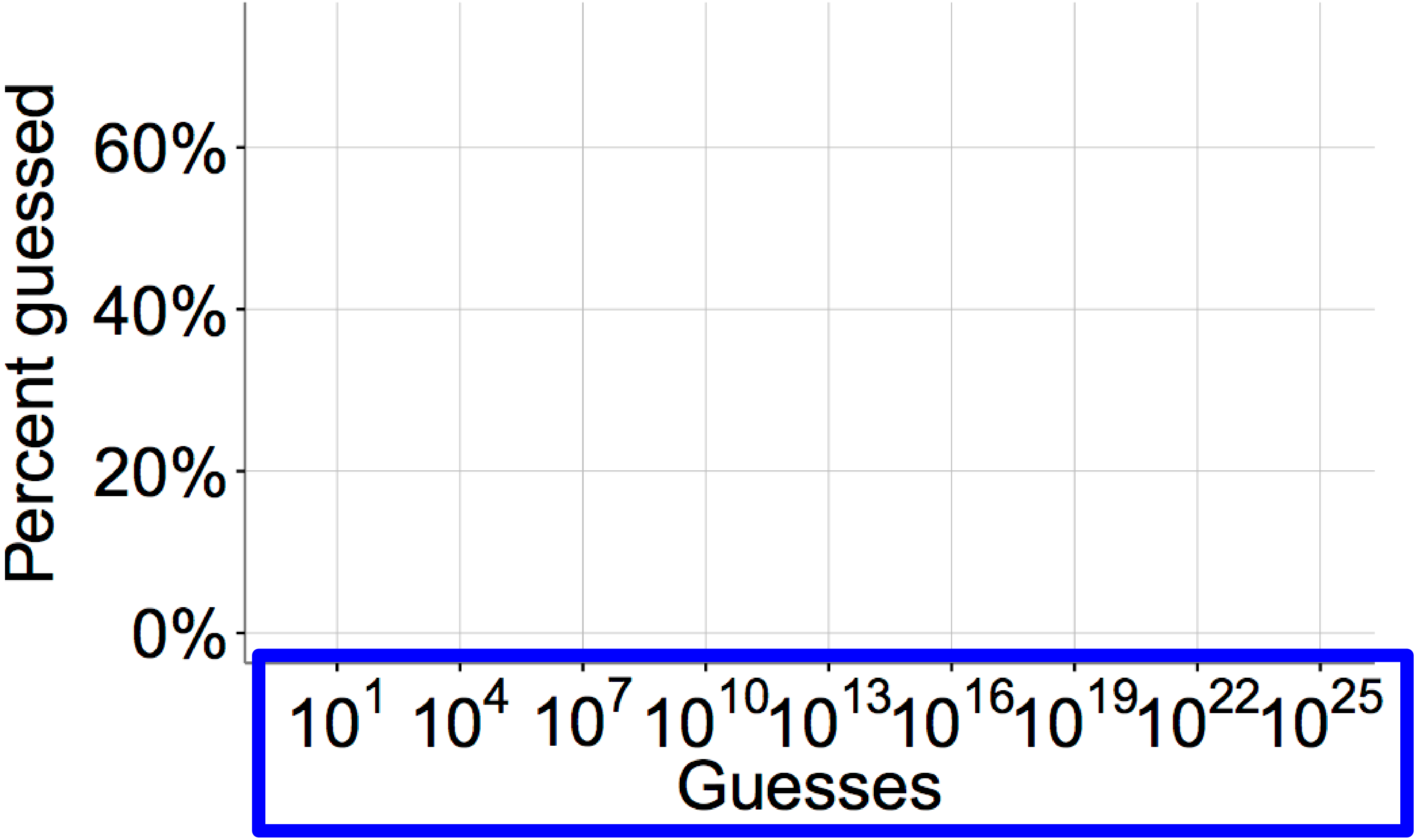
- Test on many password sets
- Monte Carlo methods to estimate guess #

Results

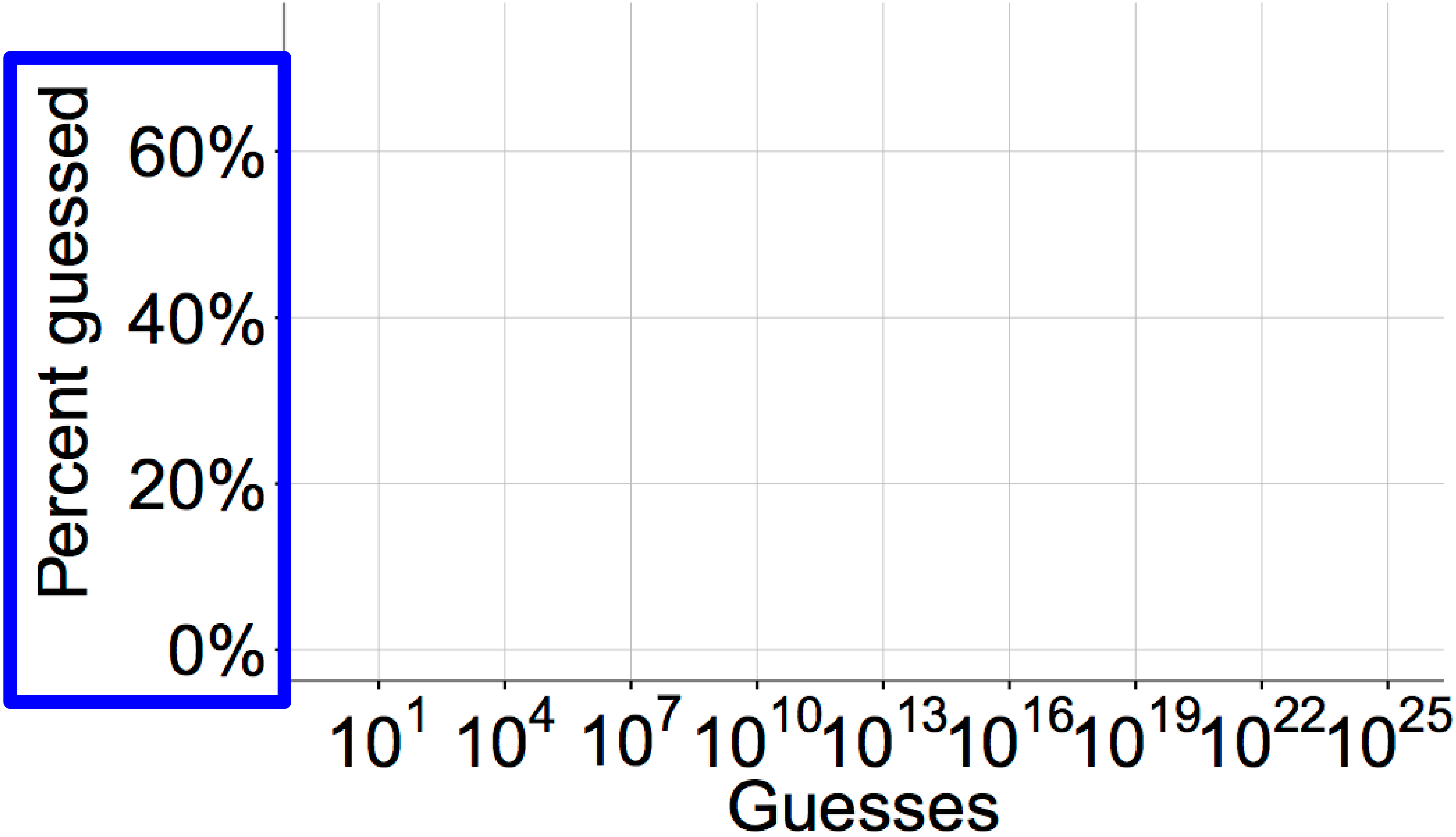


Percent guessed
60%
40%
20%
0%
10^1
10^4
10^7
10^{10}
10^{13}
10^{16}
10^{19}
10^{22}
10^{25}
Guesses

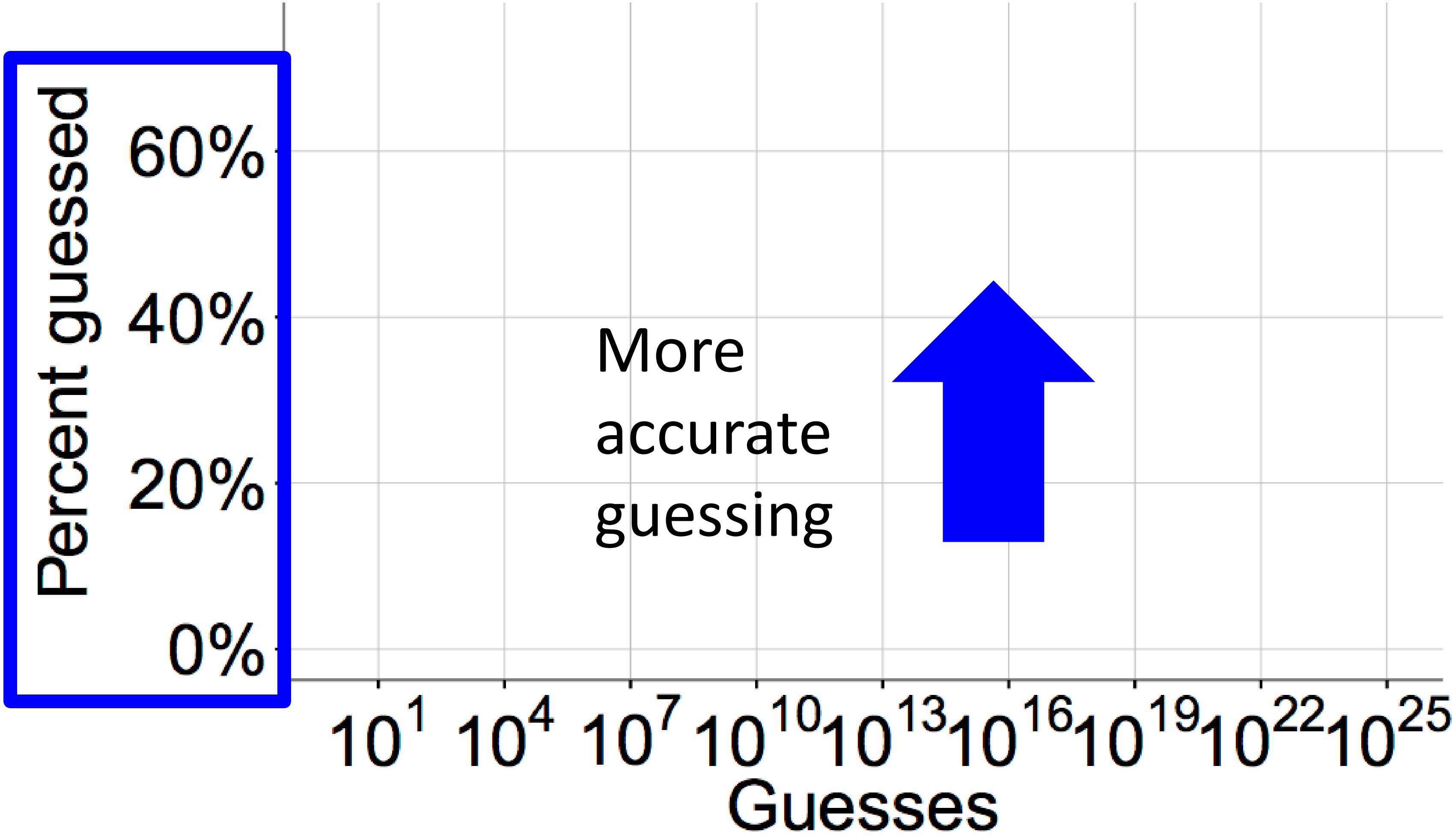
Results


Percent guessed
60%
40%
20%
0%
10^1
10^4
10^7
10^{10}
10^{13}
10^{16}
10^{19}
10^{22}
10^{25}
Guesses

Results

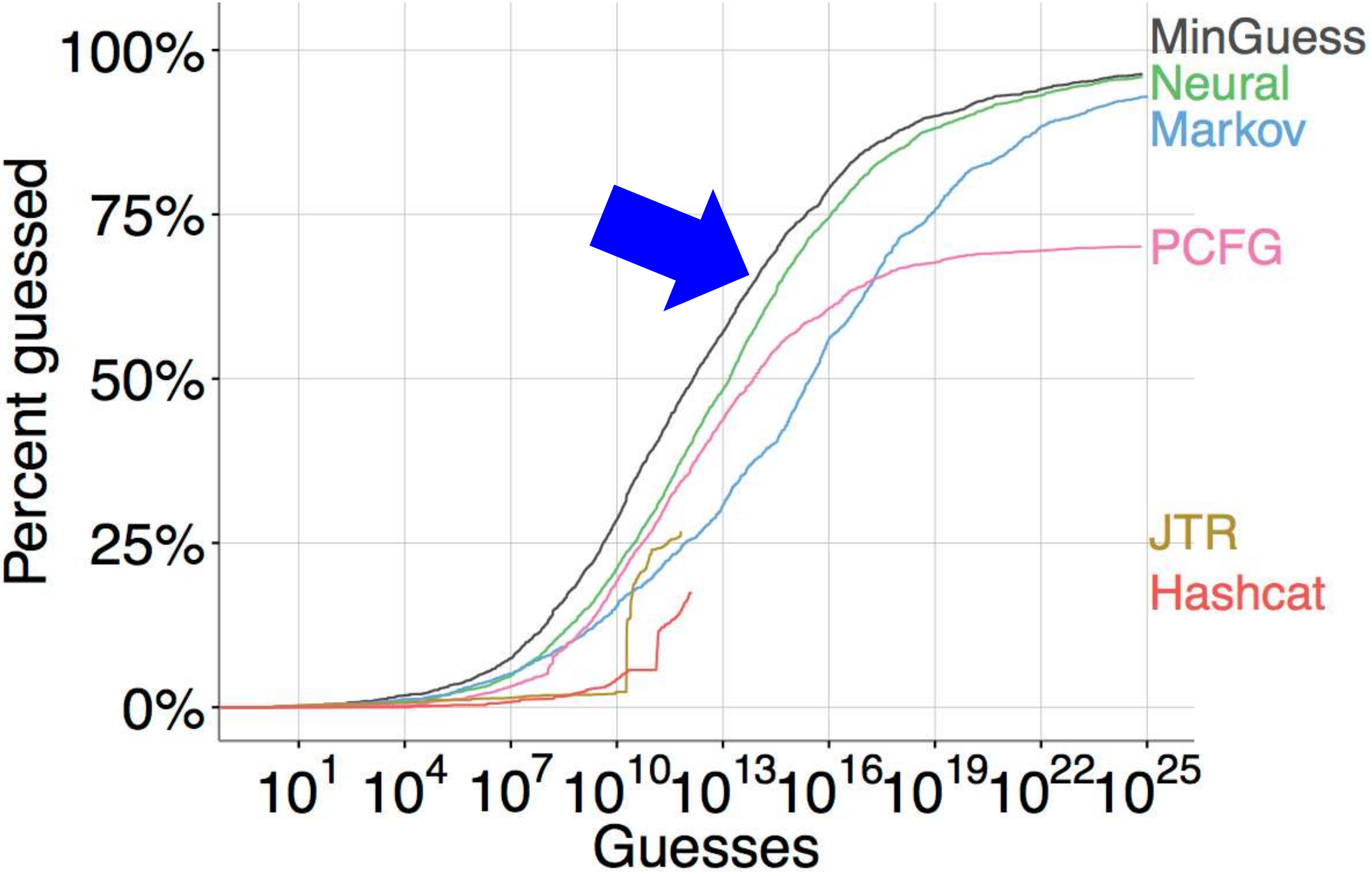

Percent guessed
60%
40%
20%
0%
10^1
10^4
10^7
10^{10}
10^{13}
10^{16}
10^{19}
10^{22}
10^{25}
Guesses

Results

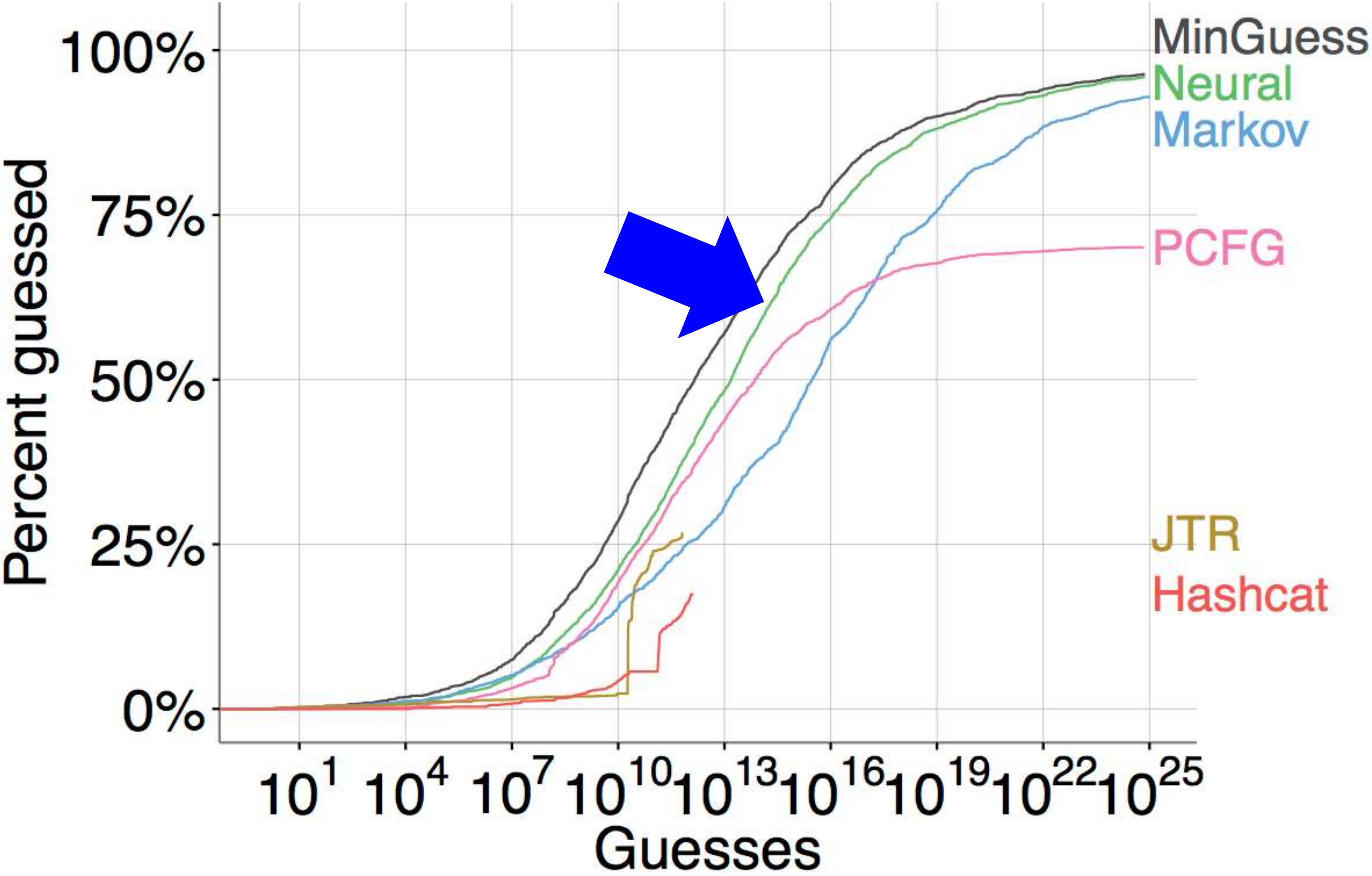


More accurate guessing

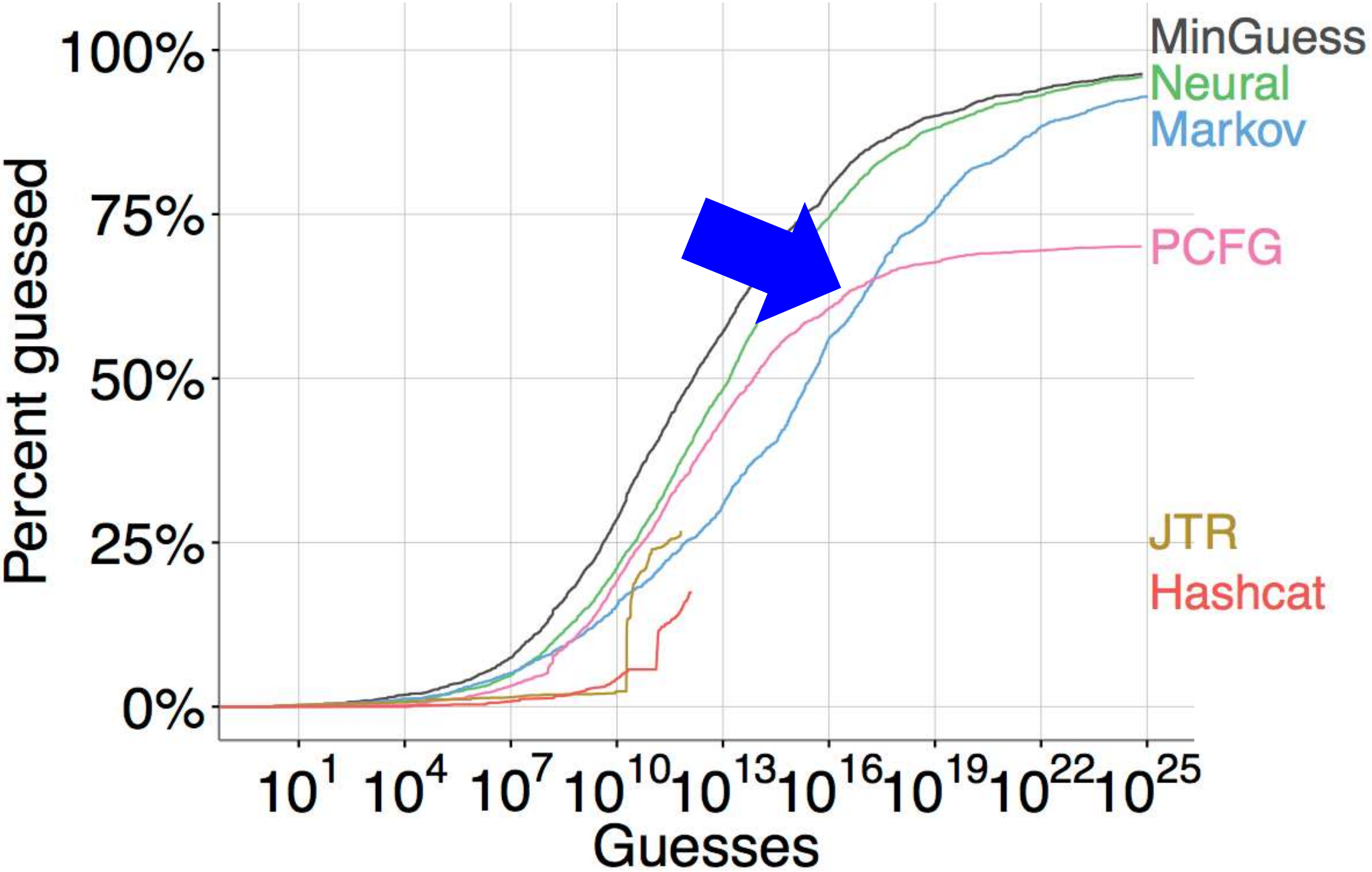
Neural Networks Guess Better



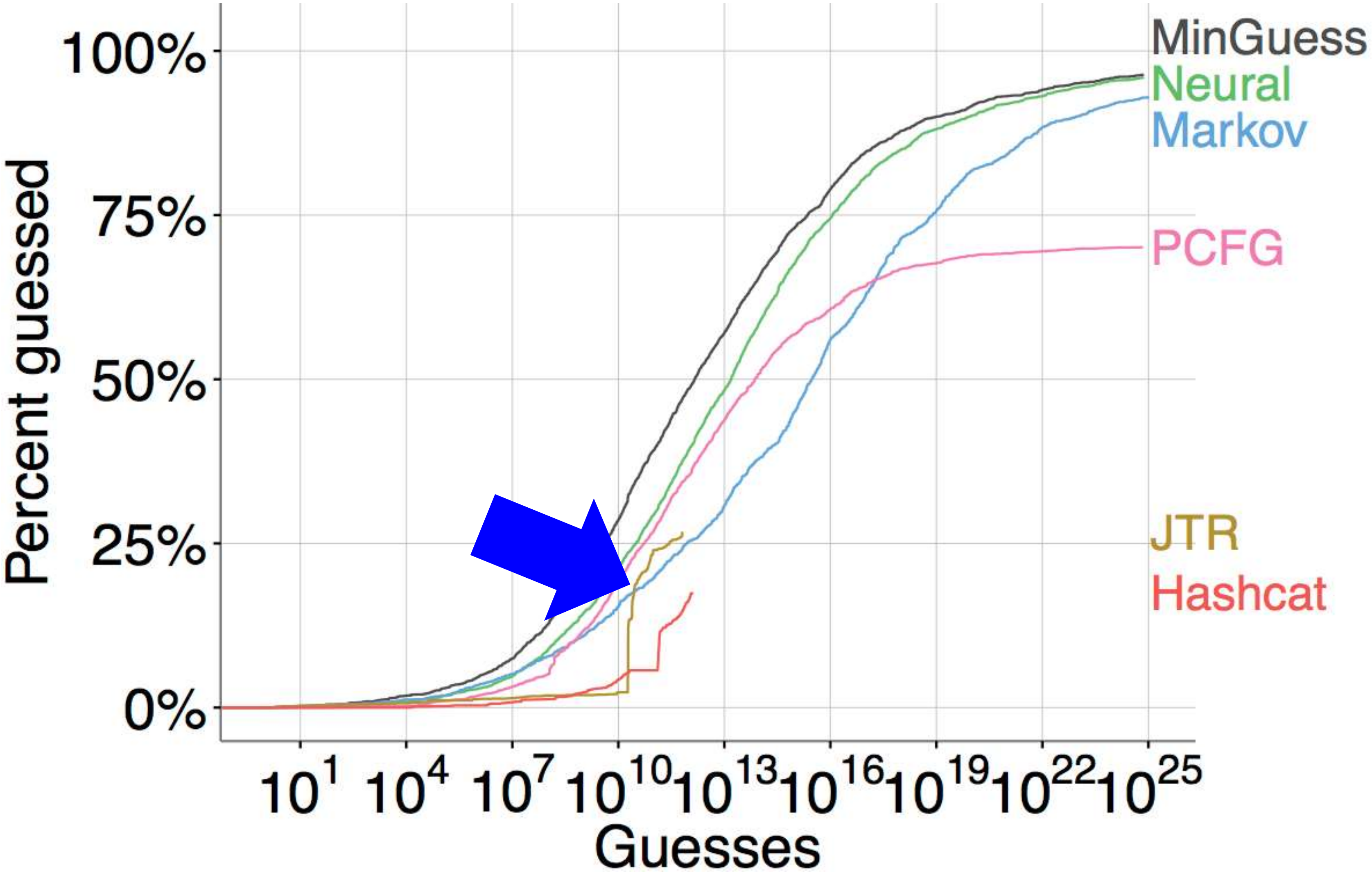
Neural Networks Guess Better



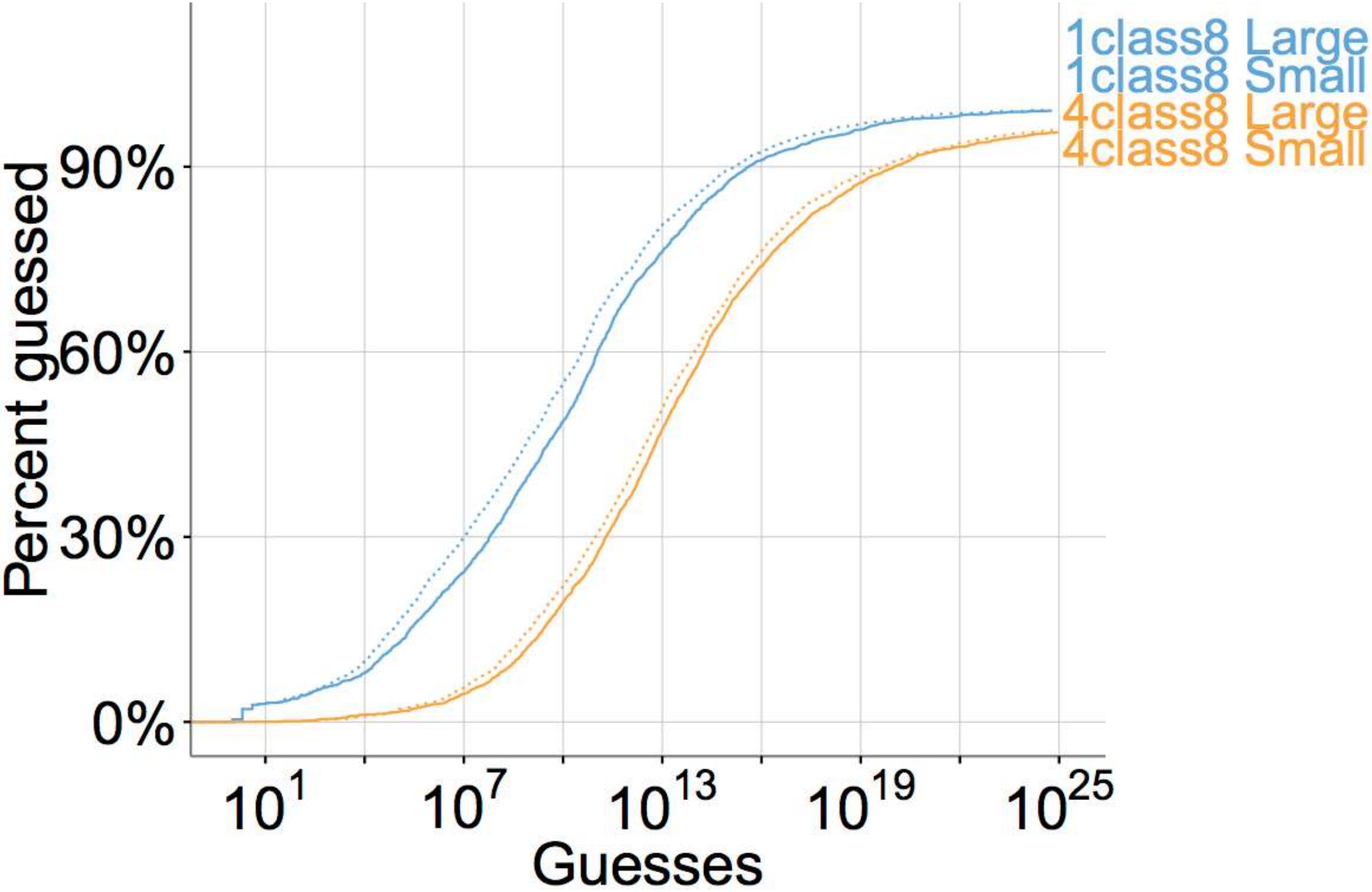
Neural Networks Guess Better



Neural Networks Guess Better



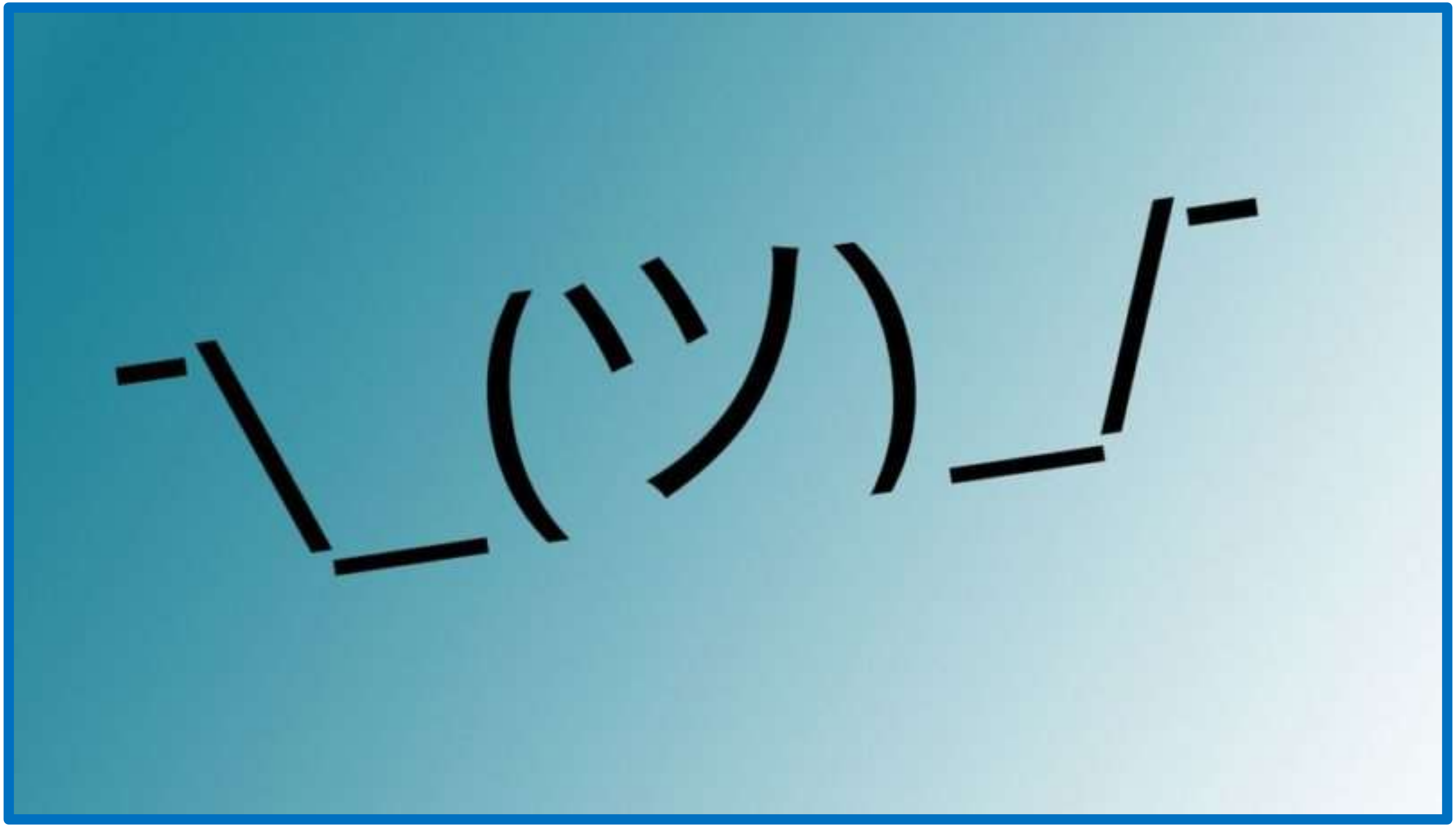
Larger Model Not Major Advantage



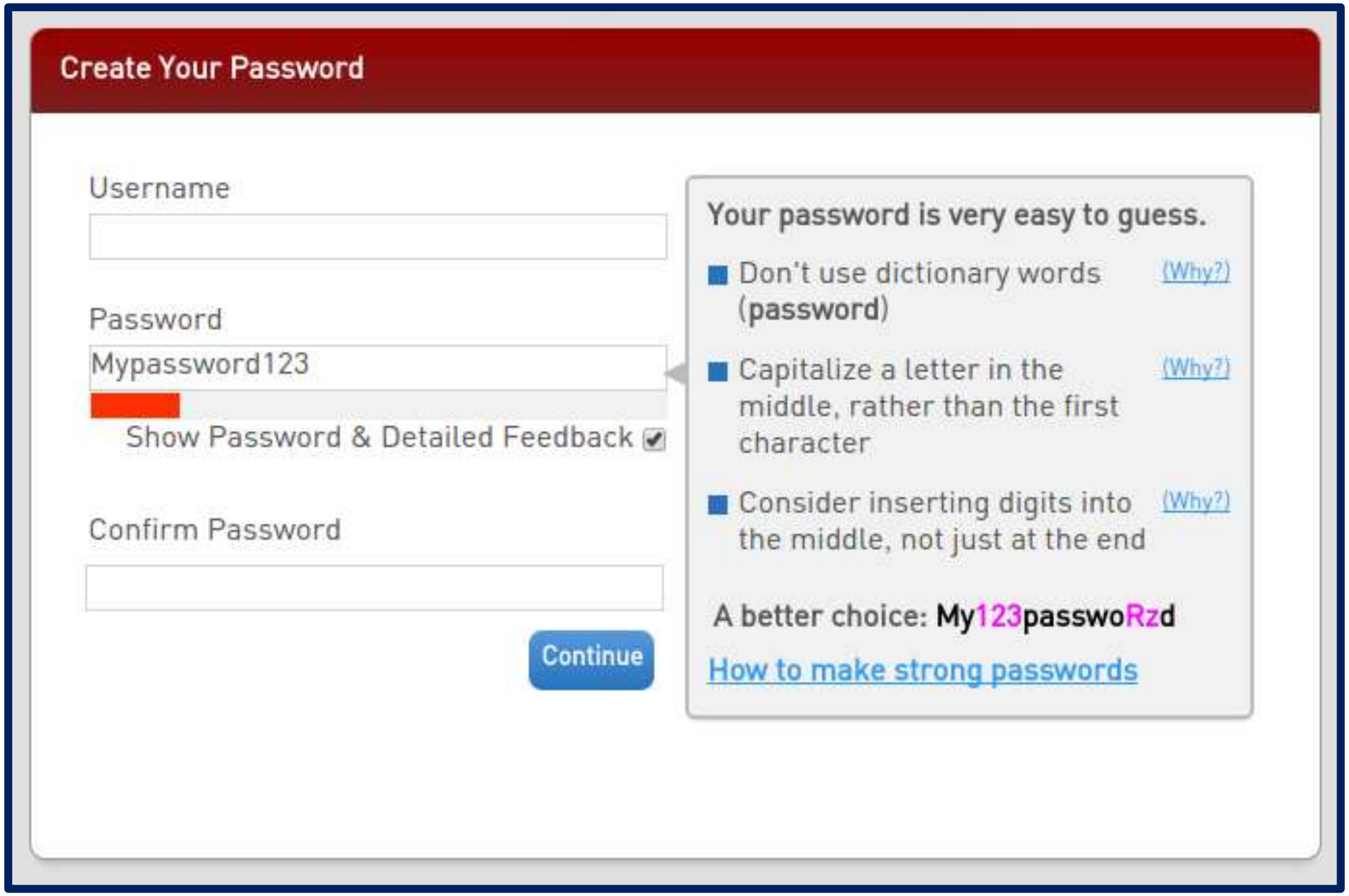
Browser Implementation

- Start with smaller model
- Quantize parameters
- Lossless compression
- Pre-compute inexact mapping of probabilities → guess #
- Cache intermediate results
- <1mb, ~ 17ms per character

Intelligibility



Building a Data-Driven Meter



Create Your Password

Username

Password

Mypassword123

Show Password & Detailed Feedback ☑

Confirm Password

Your password is very easy to guess.

- Don't use dictionary words (**password**) (Why?)
- Capitalize a letter in the middle, rather than the first character (Why?)
- Consider inserting digits into the middle, not just at the end (Why?)

A better choice: **My123passwoRzd**

How to make strong passwords

Blase Ur, Felicia Alfieri, Maung Aung, Lujo Bauer, Nicolas Christin, Jessica Colnago, Lorrie Faith Cranor, Henry Dixon, Pardis Emami Naeini, Hana Habib, Noah Johnson, William Melicher. Development and Evaluation of a Data-Driven Password Meter. In *Proc. CHI*, 2017.

We designed & tested a meter with:

1) Principled strength estimates

2) Data-driven feedback to users

We designed & tested a meter with:

1) Principled strength estimates

2) Data-driven feedback to users

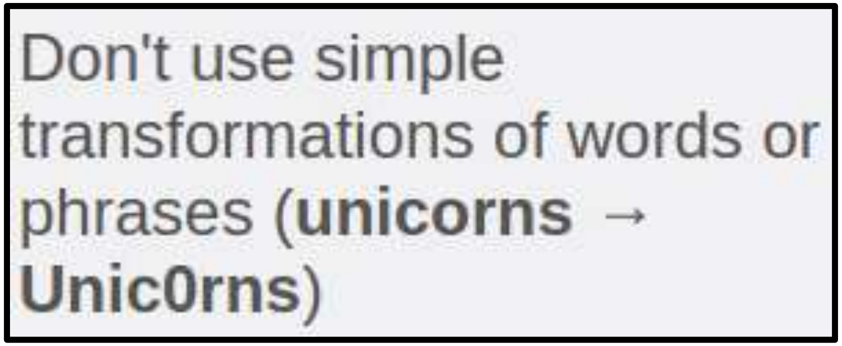
We designed & tested a meter with:

1) Principled strength estimates

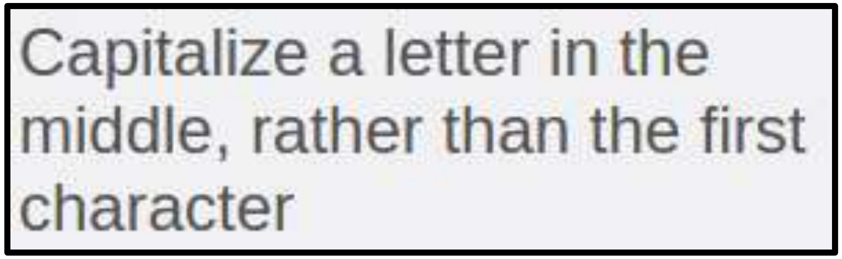
2) Data-driven feedback to users

Provide Intelligible Explanations

Unic0rns



Don't use simple transformations of words or phrases (**unicorns** → **Unic0rns**)



Capitalize a letter in the middle, rather than the first character

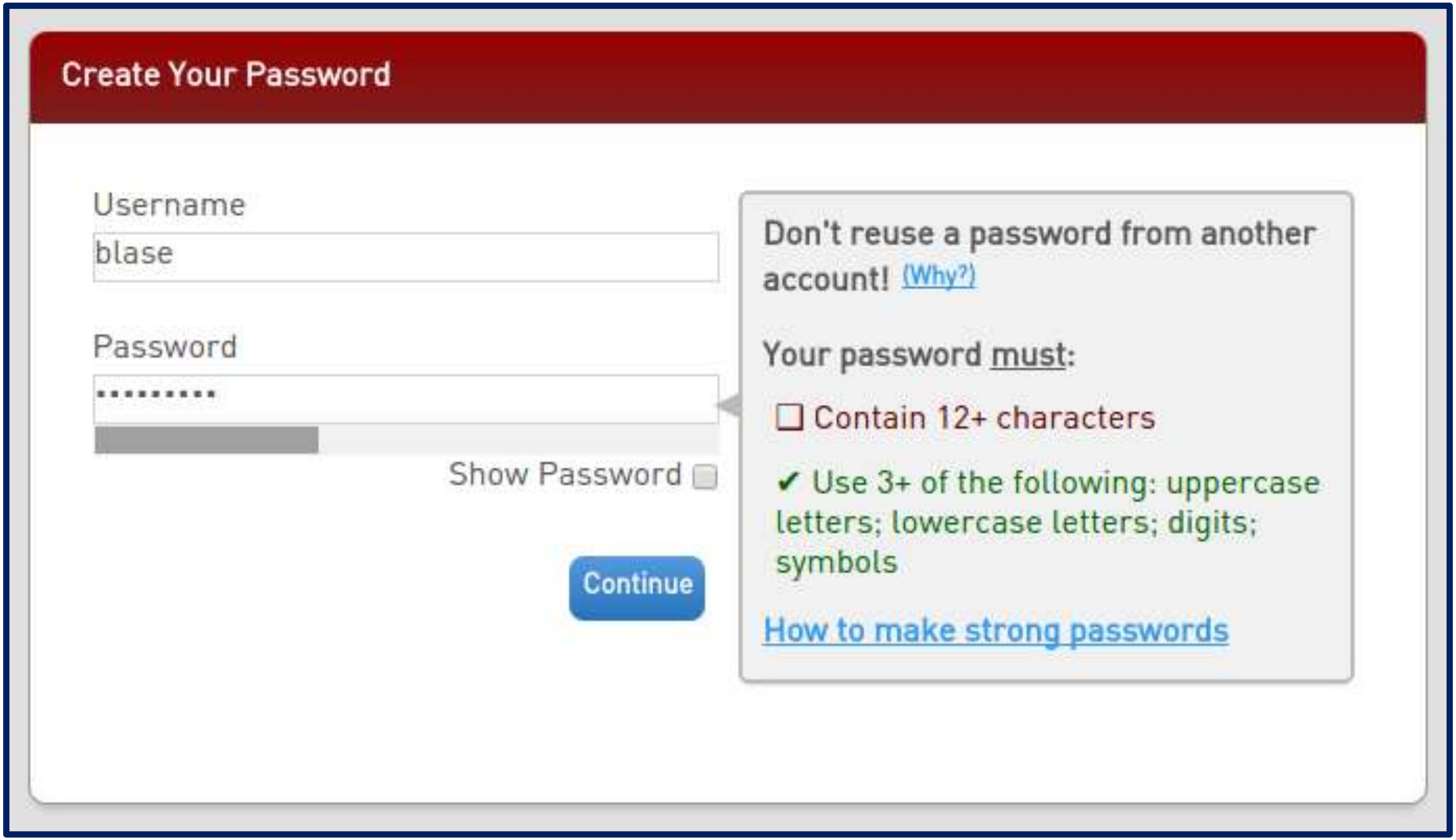
- 21 characteristics
- Weightings determined with regression

We designed & tested a meter with:

1) Principled strength estimates

2) Data-driven feedback to users

Main Screen…



Create Your Password

Username

blase

Password

••••••••••

Show Password □

Continue

Don't reuse a password from another account! (Why?)

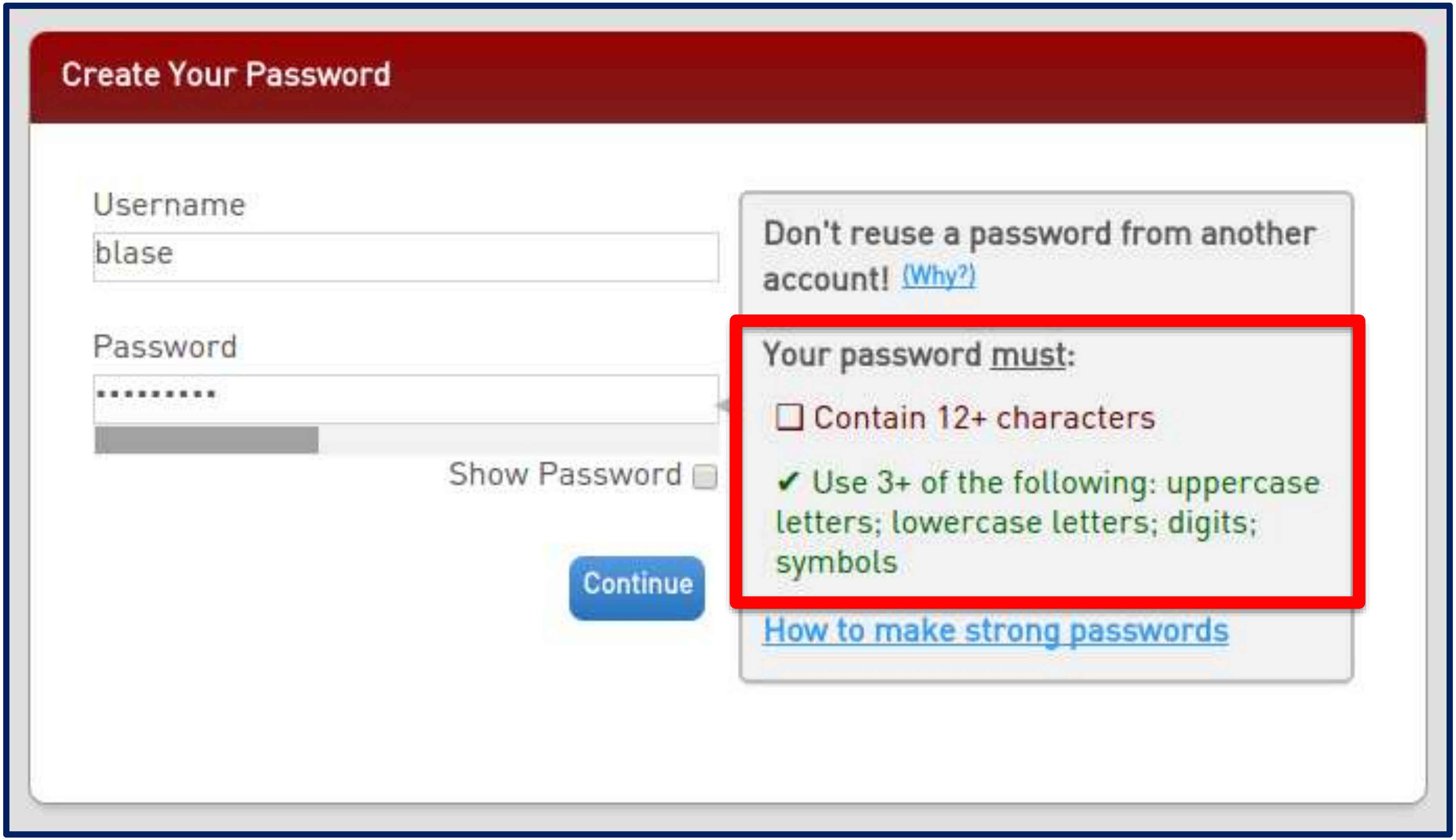
Your password must:

□ Contain 12+ characters

✓ Use 3+ of the following: uppercase letters; lowercase letters; digits; symbols

How to make strong passwords

…Shows Requirements



Create Your Password

Username

blase

Password

••••••••••

Show Password □

Don't reuse a password from another account! (Why?)

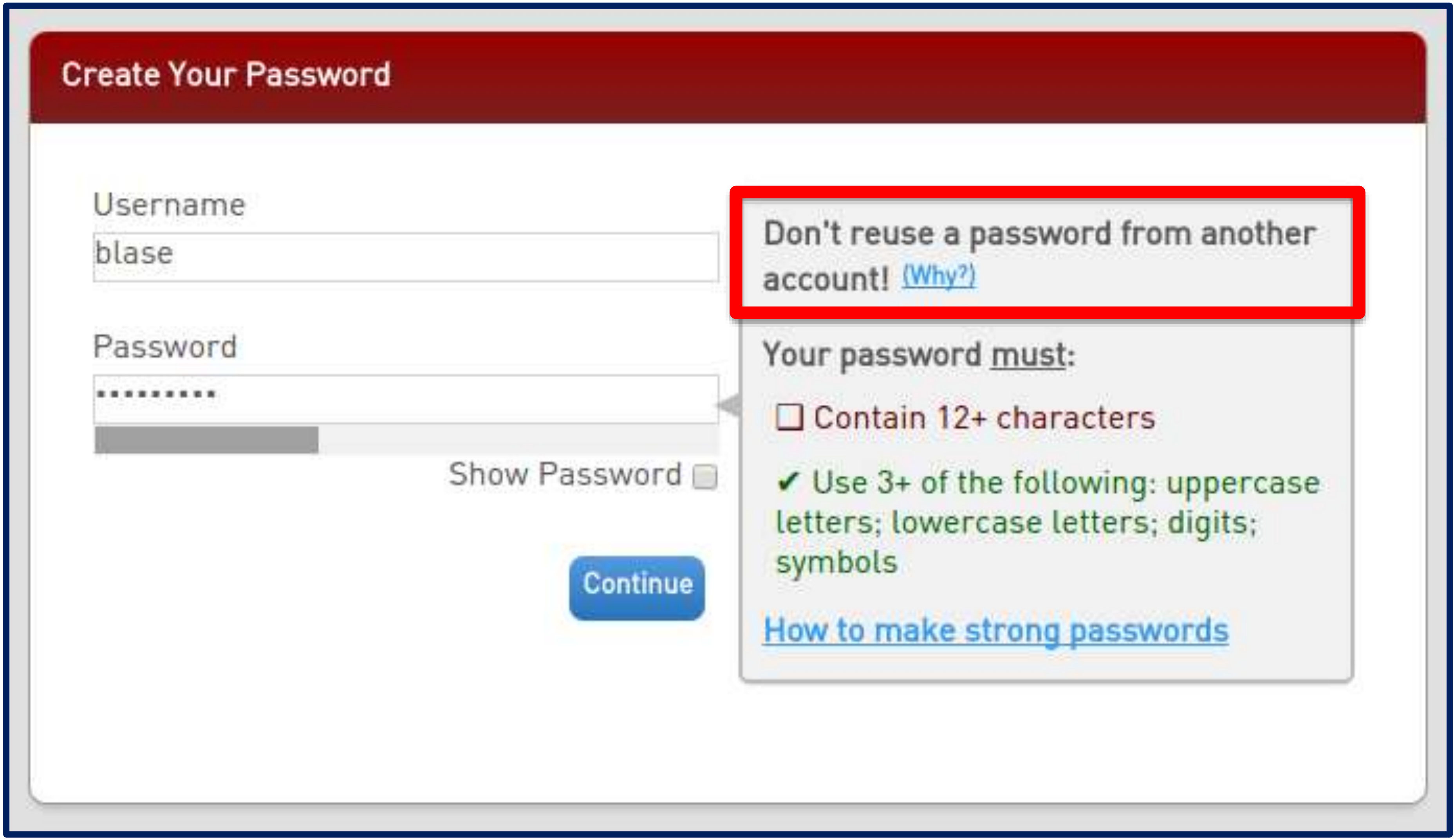
Your password must:

□ Contain 12+ characters

✓ Use 3+ of the following: uppercase letters; lowercase letters; digits; symbols

How to make strong passwords

…Emphasizes Avoiding Reuse



Create Your Password

Username

blase

Password

••••••••••

Show Password □

Don't reuse a password from another account! (Why?)

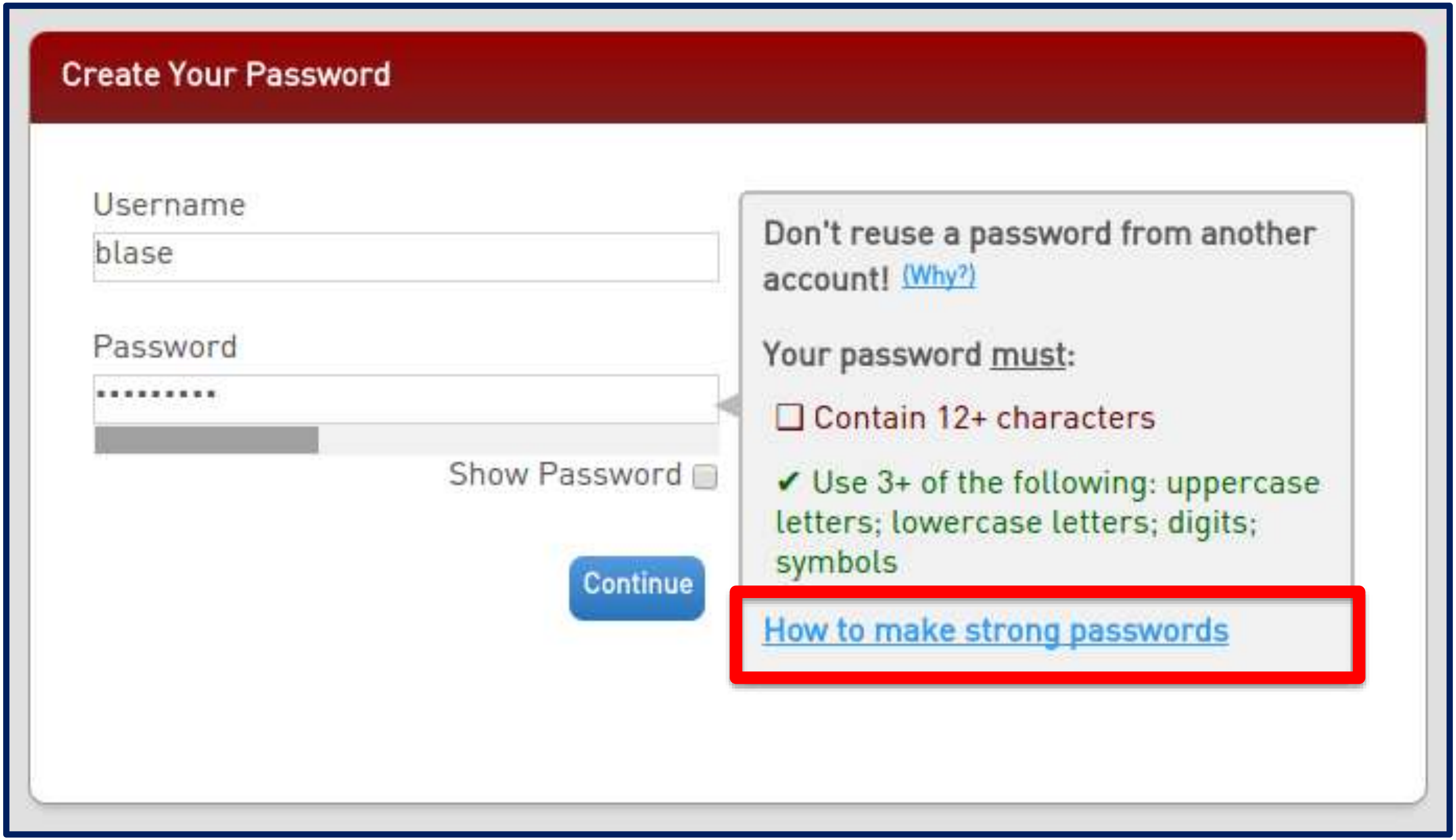
Your password must:

□ Contain 12+ characters

✓ Use 3+ of the following: uppercase letters; lowercase letters; digits; symbols

How to make strong passwords

…Provides Abstract Advice



Create Your Password

Username

blase

Password

••••••••••

Don't reuse a password from another account! (Why?)

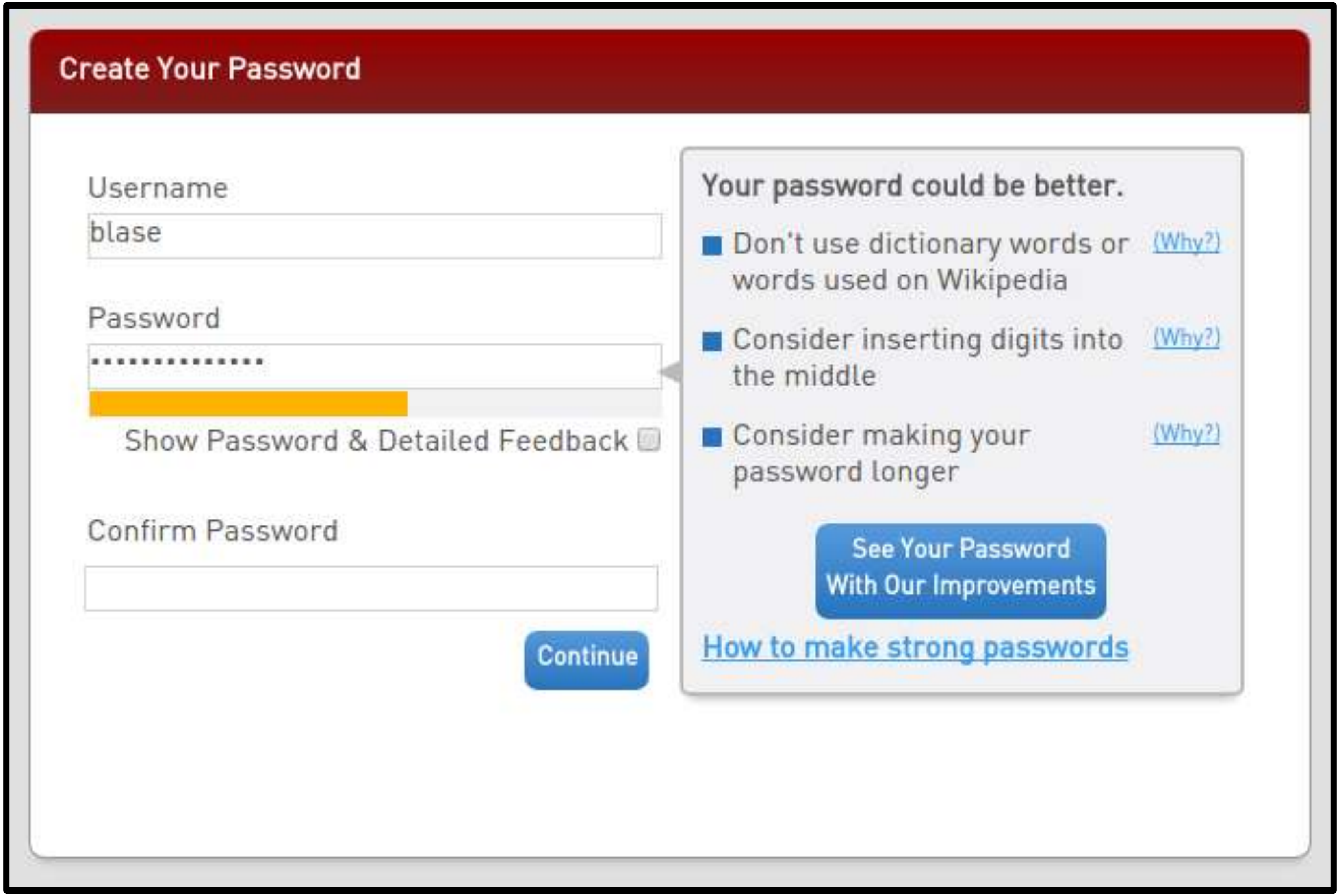
Your password must:

☐ Contain 12+ characters

✓ Use 3+ of the following: uppercase letters; lowercase letters; digits; symbols

How to make strong passwords

After Requirements Are Met…



Create Your Password

Username

blase

Password

••••••••••••••

Show Password & Detailed Feedback □

Confirm Password

Continue

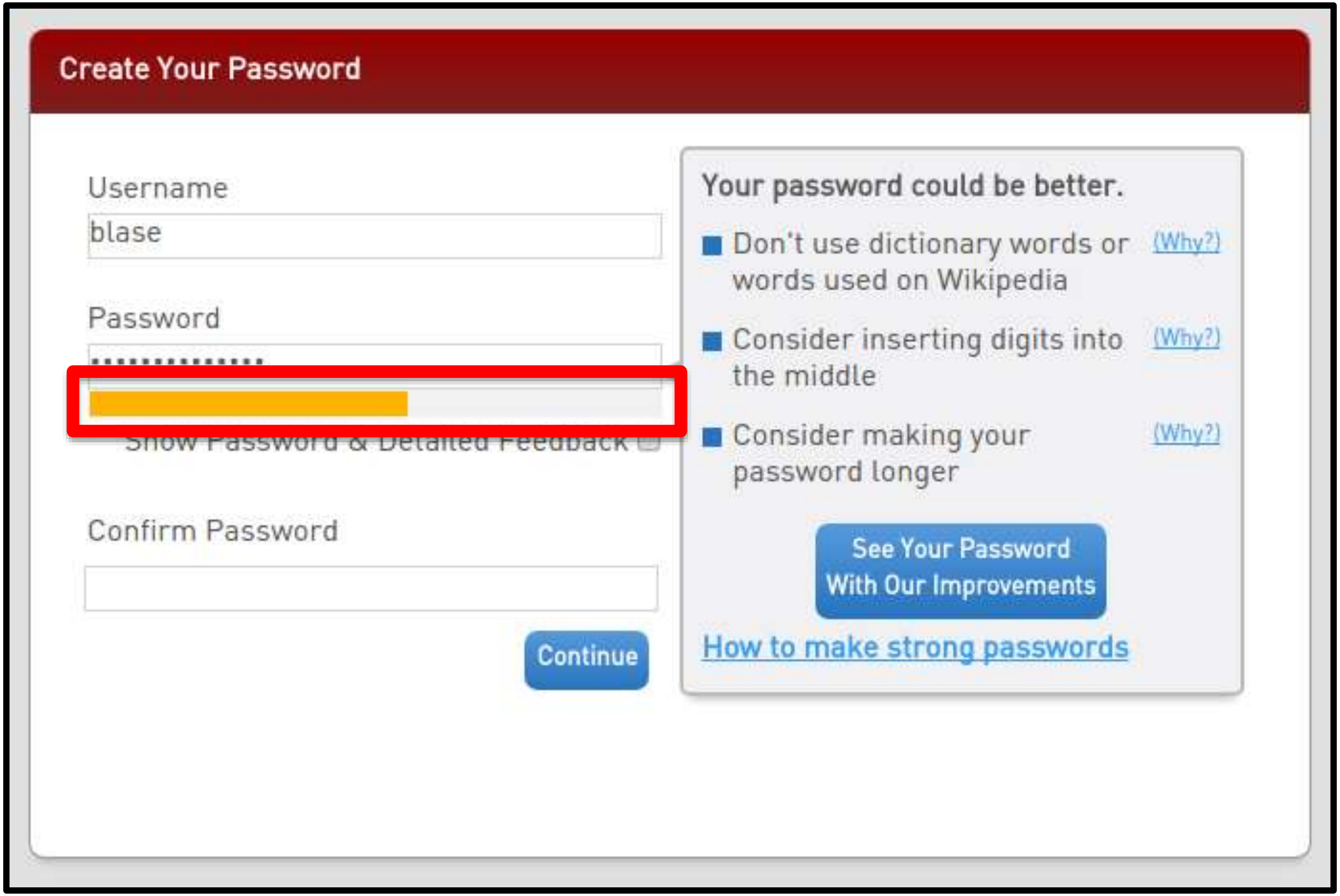
Your password could be better.

- Don't use dictionary words or words used on Wikipedia (Why?)
- Consider inserting digits into the middle (Why?)
- Consider making your password longer (Why?)

See Your Password With Our Improvements

How to make strong passwords

…Displays Score Visually



Create Your Password

Username

blase

Password

•••••••••••••••

Show Password & Detailed Feedback □

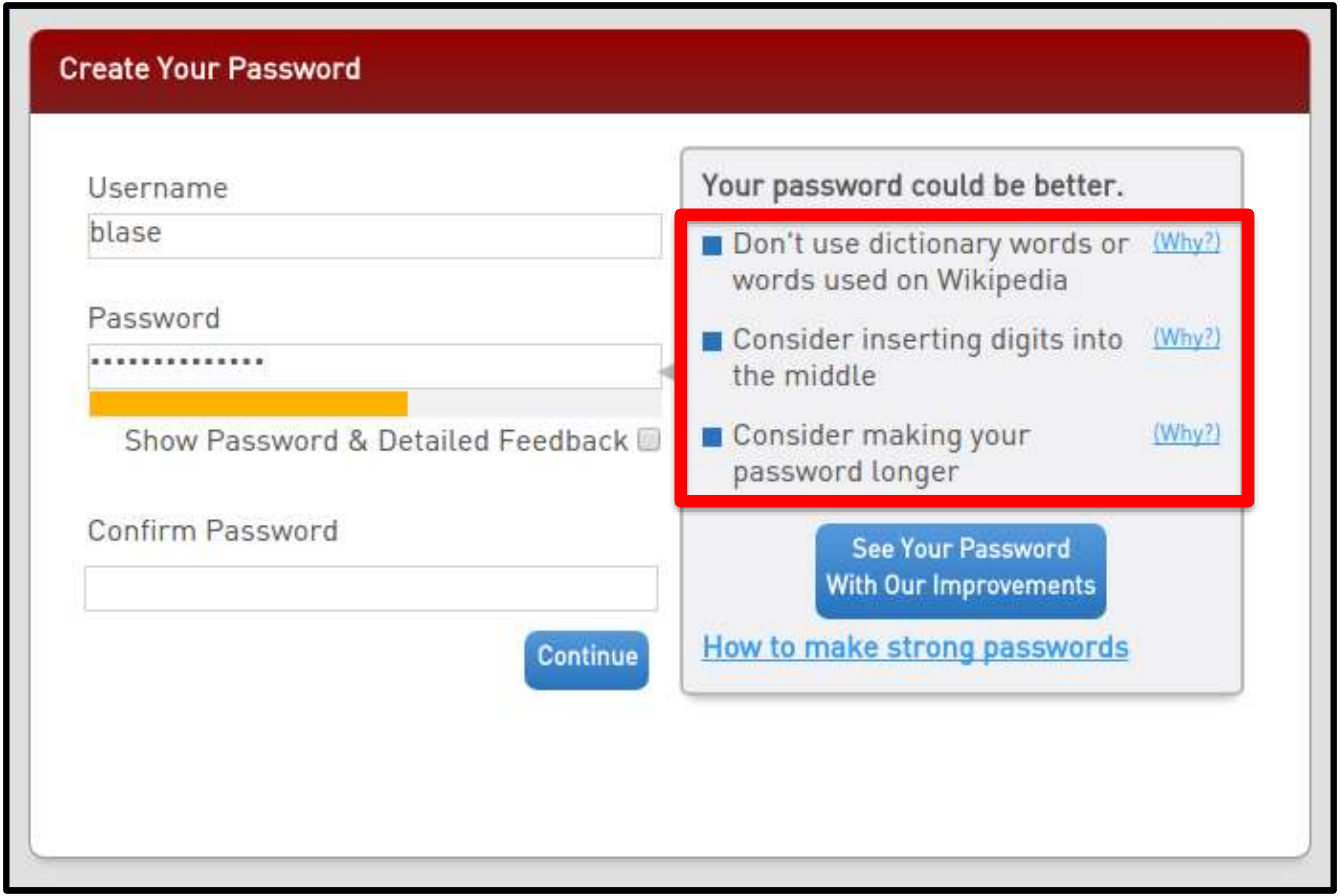
Confirm Password

Your password could be better.

- Don't use dictionary words or words used on Wikipedia (Why?)
- Consider inserting digits into the middle (Why?)
- Consider making your password longer (Why?)

How to make strong passwords

…Provides Text Feedback



Create Your Password

Username

blase

Password

•••••••••••••••

Show Password & Detailed Feedback □

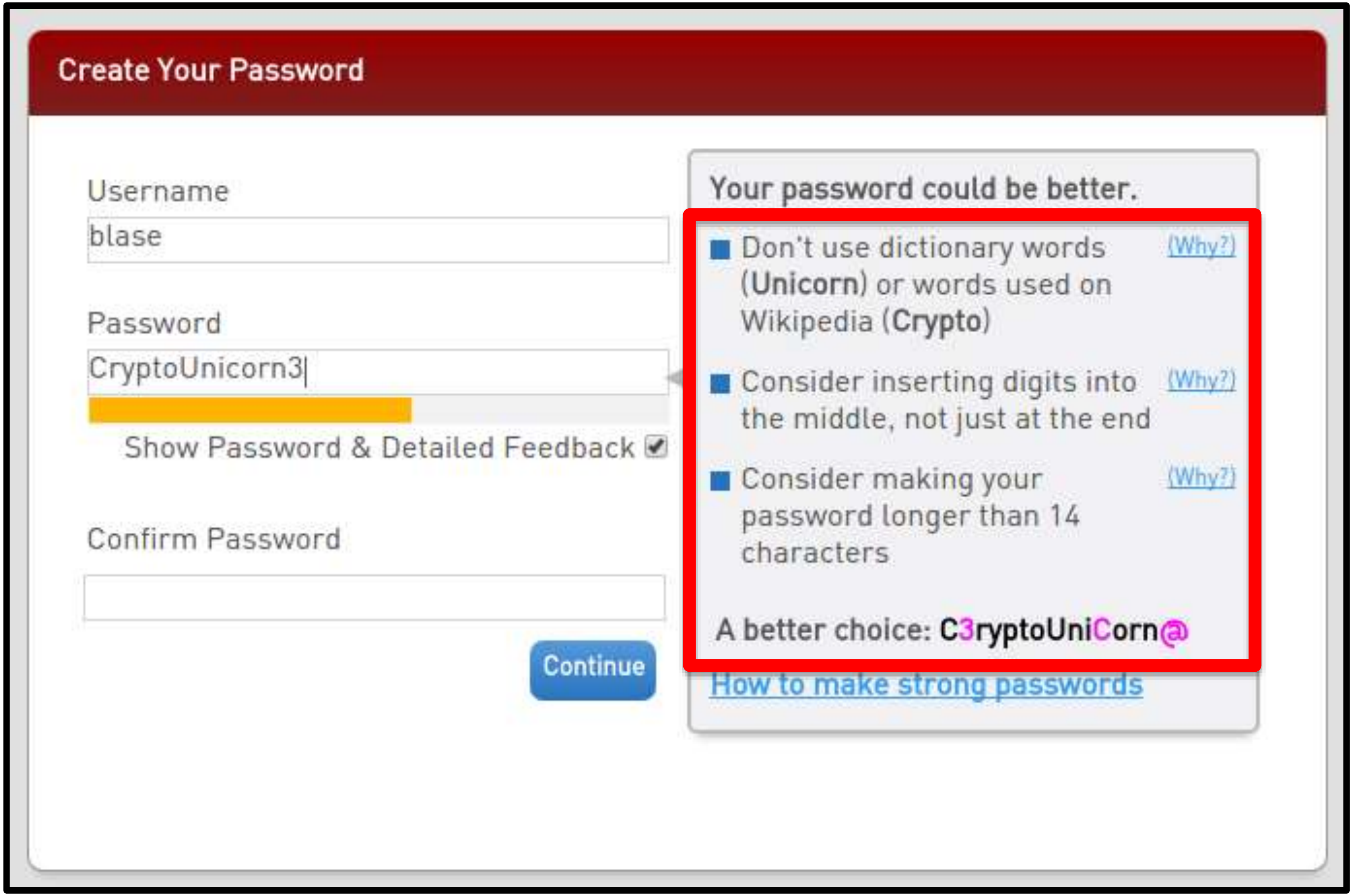
Confirm Password

Your password could be better.

- Don't use dictionary words or words used on Wikipedia (Why?)
- Consider inserting digits into the middle (Why?)
- Consider making your password longer (Why?)

How to make strong passwords

…Gives Detail (Password Shown)



Create Your Password

Username

blase

Password

CryptoUnicorn3

Show Password & Detailed Feedback ☑

Confirm Password

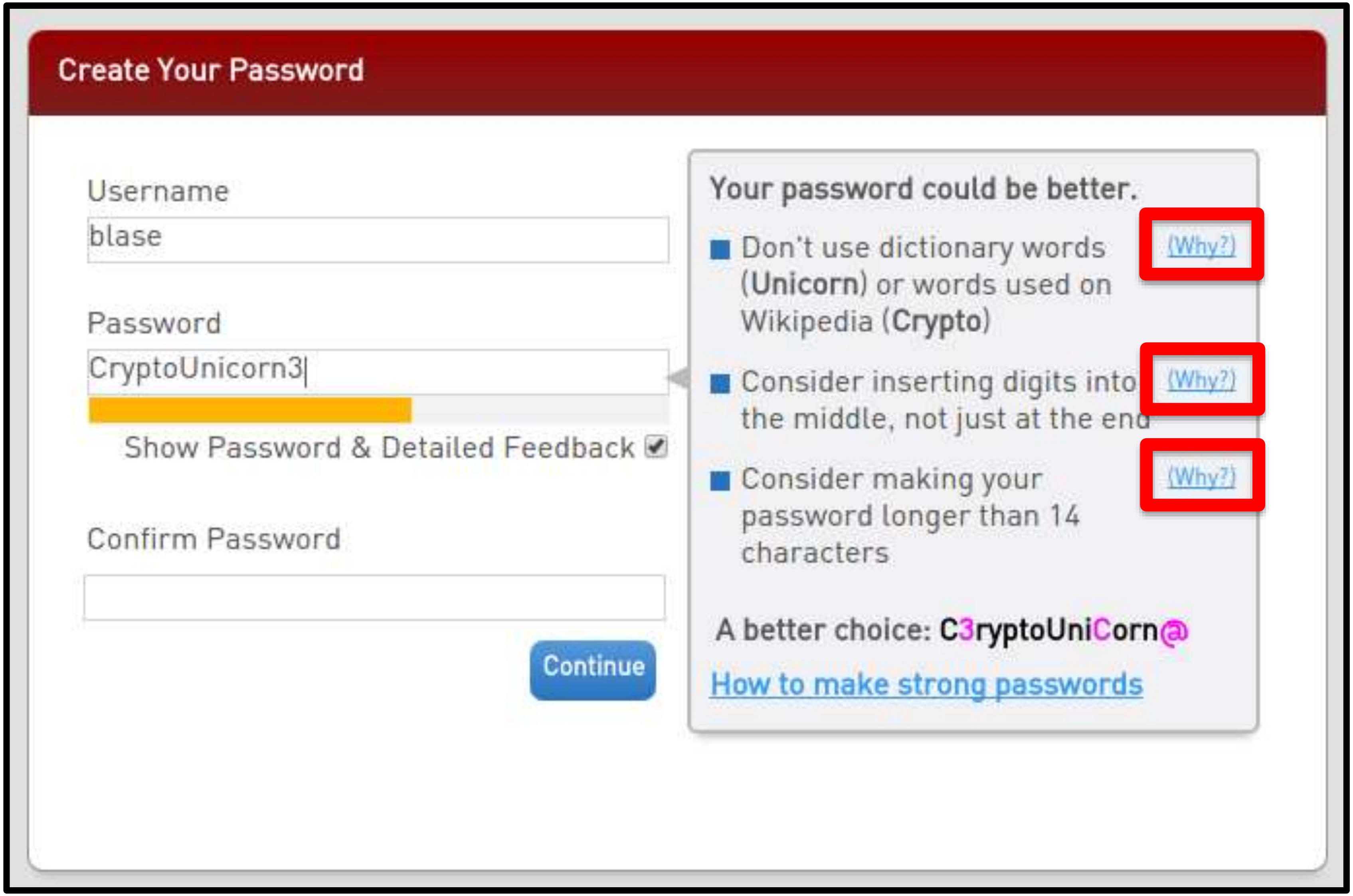
Your password could be better.

- Don't use dictionary words (**Unicorn**) or words used on Wikipedia (**Crypto**) (Why?)
- Consider inserting digits into the middle, not just at the end (Why?)
- Consider making your password longer than 14 characters (Why?)

A better choice: **C3ryptoUniCorn@**

How to make strong passwords

…Offers Explanations



Create Your Password

Username

blase

Password

CryptoUnicorn3|

Show Password & Detailed Feedback ☑

Confirm Password

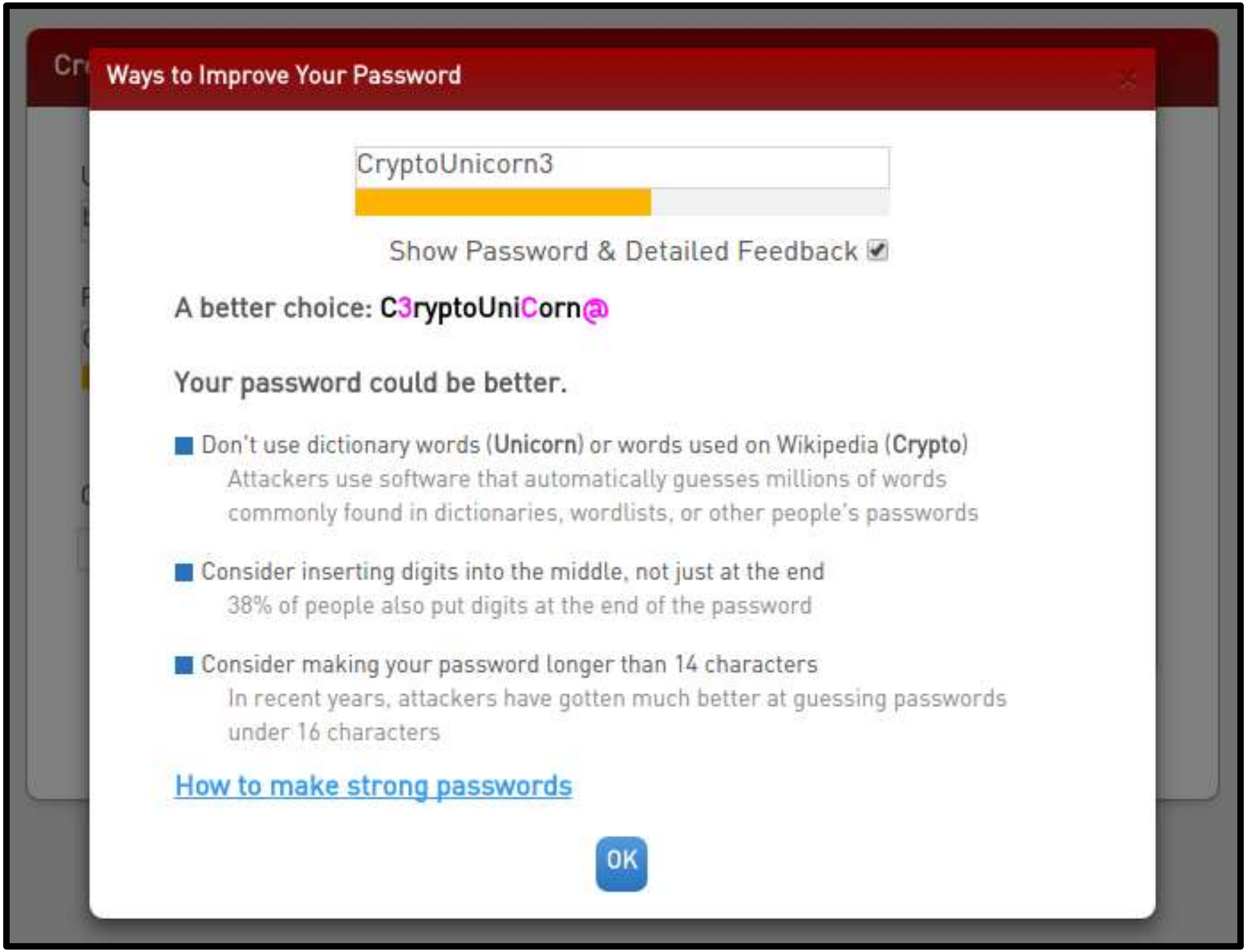
Your password could be better.

- Don't use dictionary words (**Unicorn**) or words used on Wikipedia (**Crypto**) (Why?)
- Consider inserting digits into the middle, not just at the end (Why?)
- Consider making your password longer than 14 characters (Why?)

A better choice: C3ryptoUniCorn@

How to make strong passwords

Explanations Shown in Modal



Ways to Improve Your Password

CryptoUnicorn3

Show Password & Detailed Feedback ☑

A better choice: **C3ryptoUniCorn@**

Your password could be better.

- Don't use dictionary words (**Unicorn**) or words used on Wikipedia (**Crypto**)
  Attackers use software that automatically guesses millions of words commonly found in dictionaries, wordlists, or other people's passwords
- Consider inserting digits into the middle, not just at the end
  38% of people also put digits at the end of the password
- Consider making your password longer than 14 characters
  In recent years, attackers have gotten much better at guessing passwords under 16 characters

How to make strong passwords

We designed & tested a meter with:

1) Principled strength estimates

2) Data-driven feedback to users

Evaluation

- 2-part online study
  1) Create password; survey; recall password
  (48 hours later, send automated email)
  2) Recall password; survey
- 4,509 Mechanical Turk participants
  - Between-subjects
  - Full-factorial design along three dimensions

Dimension 1: Composition Policy

- 8+ characters (1class8)

password

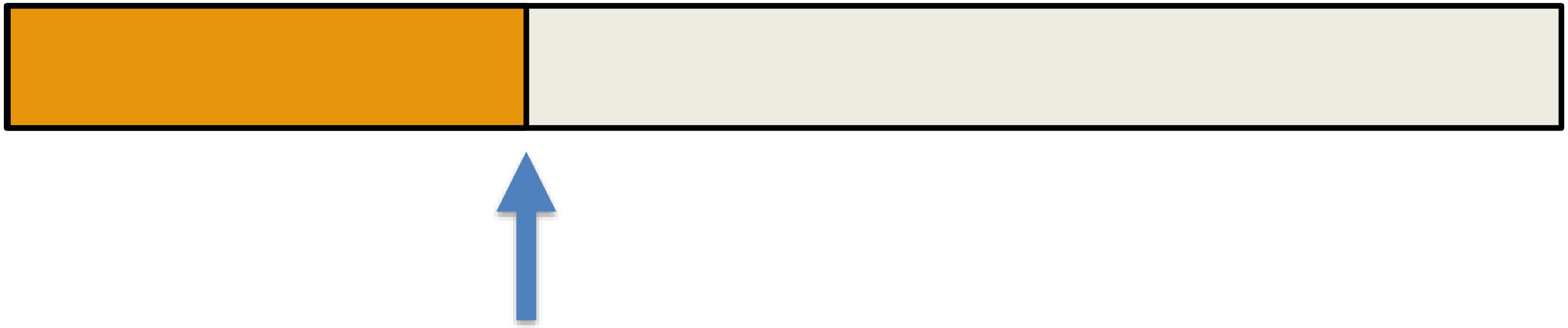
- 12+ characters, 3+ classes (3class12)

Password1234

Dimension 2: Stringency

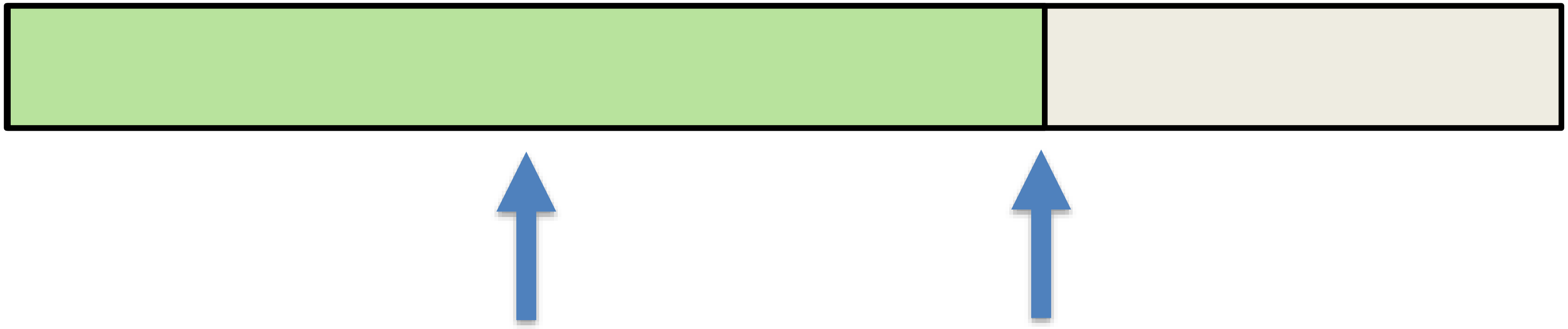
- Low
- Medium
- High

Dimension 2: Stringency



• Low	10^4 guesses
• Medium	10^6 guesses
• High	10^8 guesses

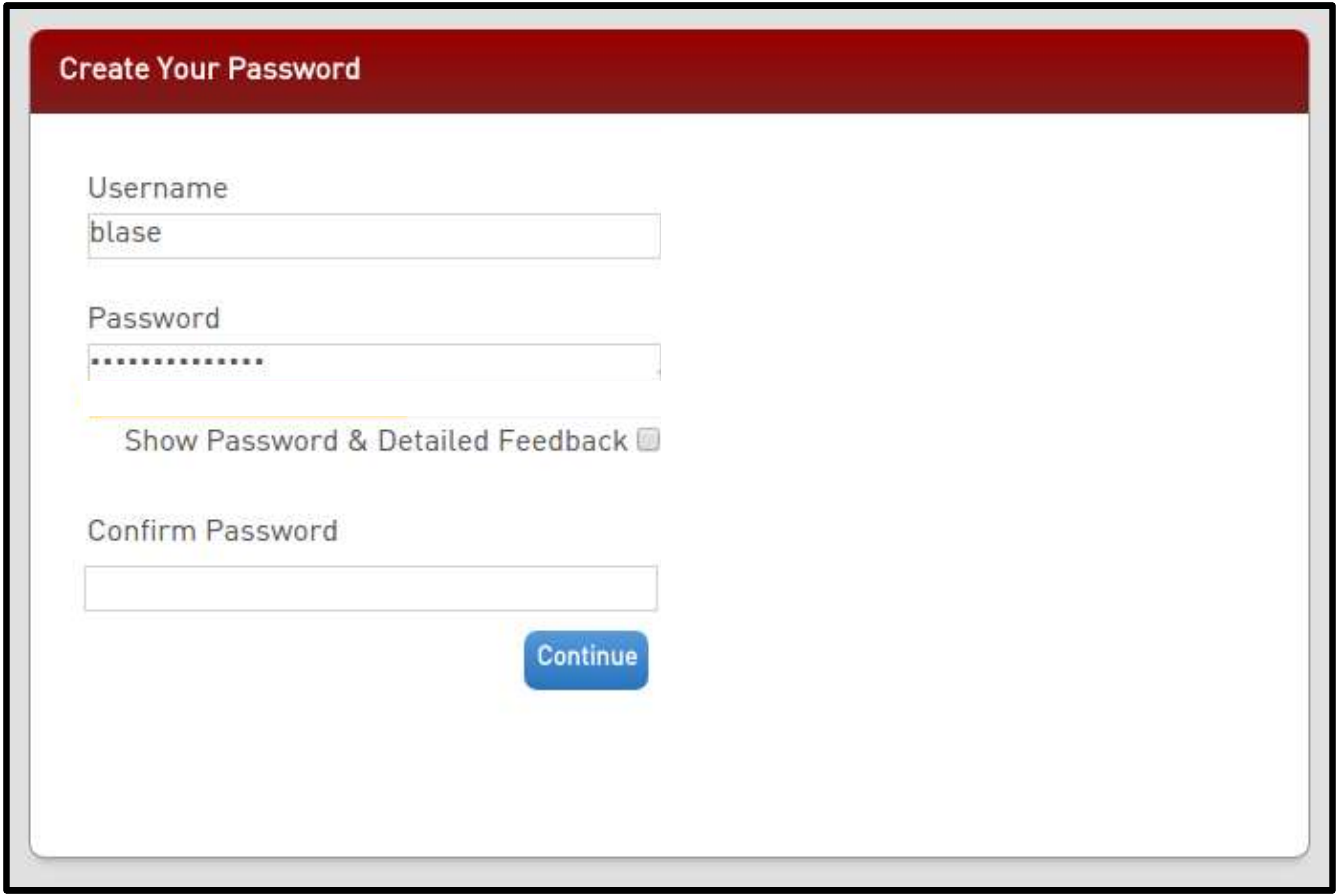
Dimension 2: Stringency



• Low	10^4 guesses	10^8 guesses
• Medium	10^6 guesses	10^{12} guesses
• High	10^8 guesses	10^{16} guesses

Dimension 3: Feedback

No Feedback



Create Your Password

Username

blase

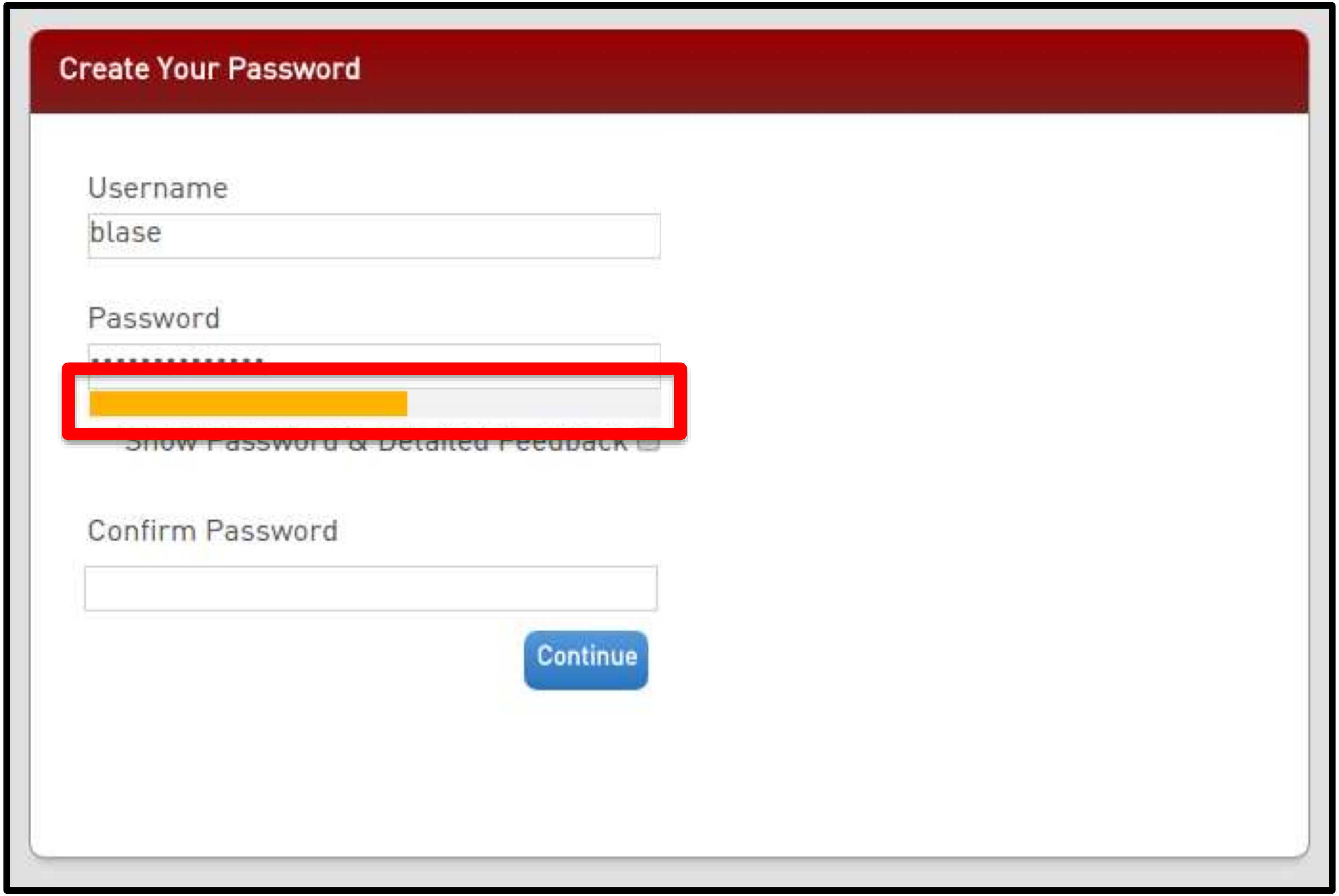
Password

••••••••••••••

Show Password & Detailed Feedback □

Confirm Password

Bar Only



Create Your Password

Username

blase

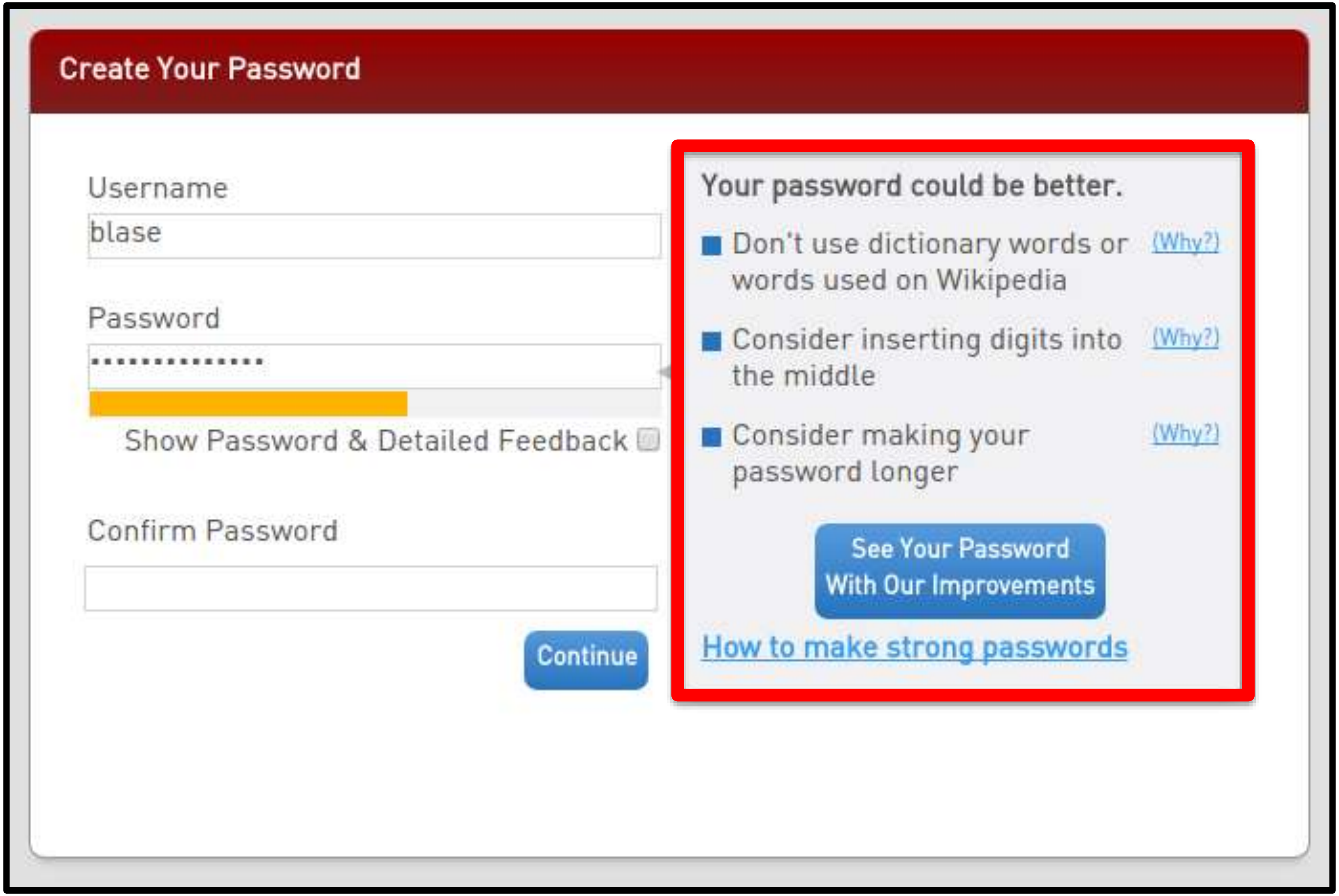
Password

••••••••••••••

Show Password & Detailed Feedback □

Confirm Password

Public (Non-Sensitive) Feedback



Create Your Password

Username

blase

Password

••••••••••••••

Show Password & Detailed Feedback □

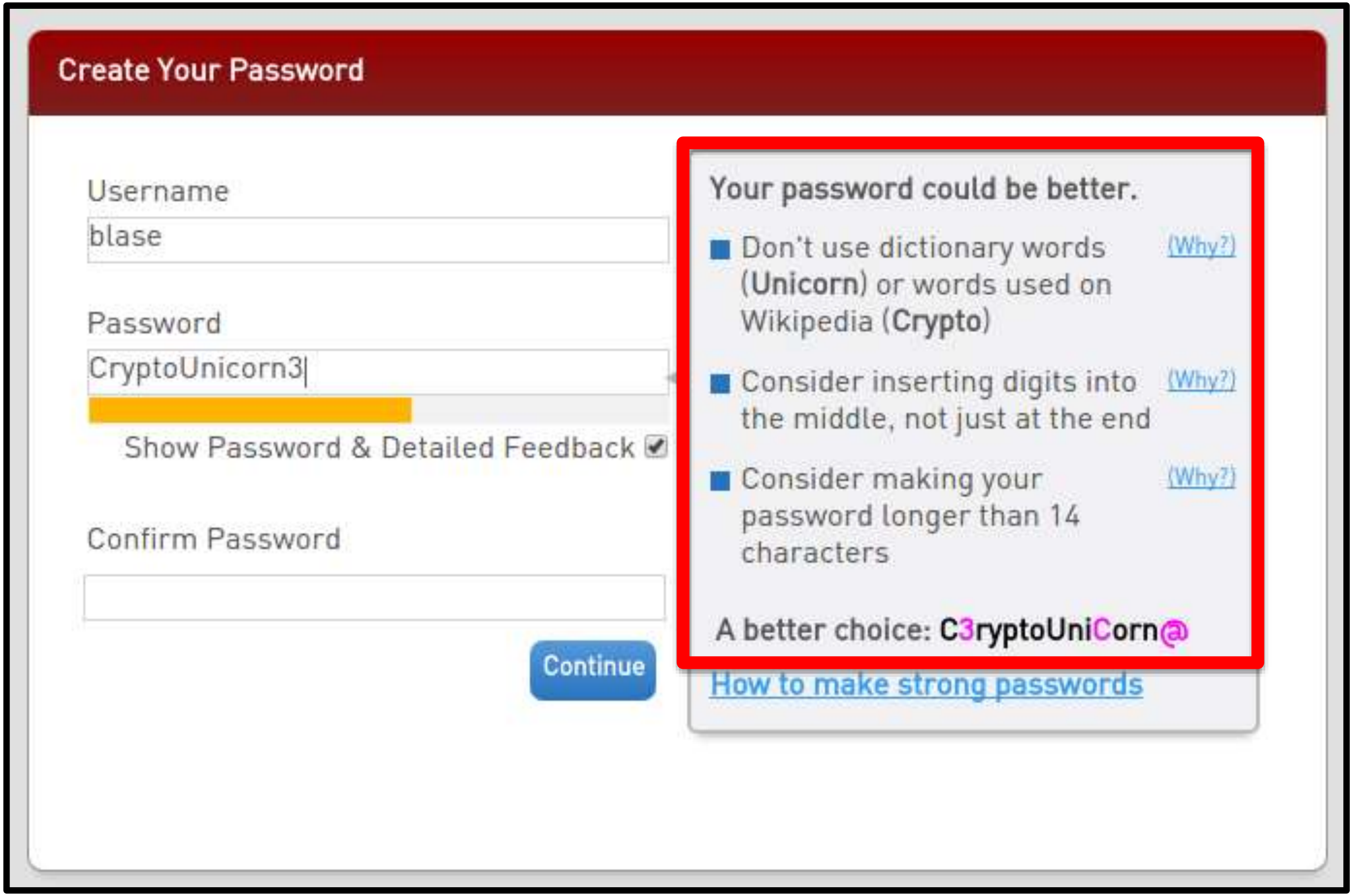
Confirm Password

Your password could be better.

- Don't use dictionary words or words used on Wikipedia (Why?)
- Consider inserting digits into the middle (Why?)
- Consider making your password longer (Why?)

How to make strong passwords

Standard Feedback



Create Your Password

Username

blase

Password

CryptoUnicorn3

Show Password & Detailed Feedback ☑

Confirm Password

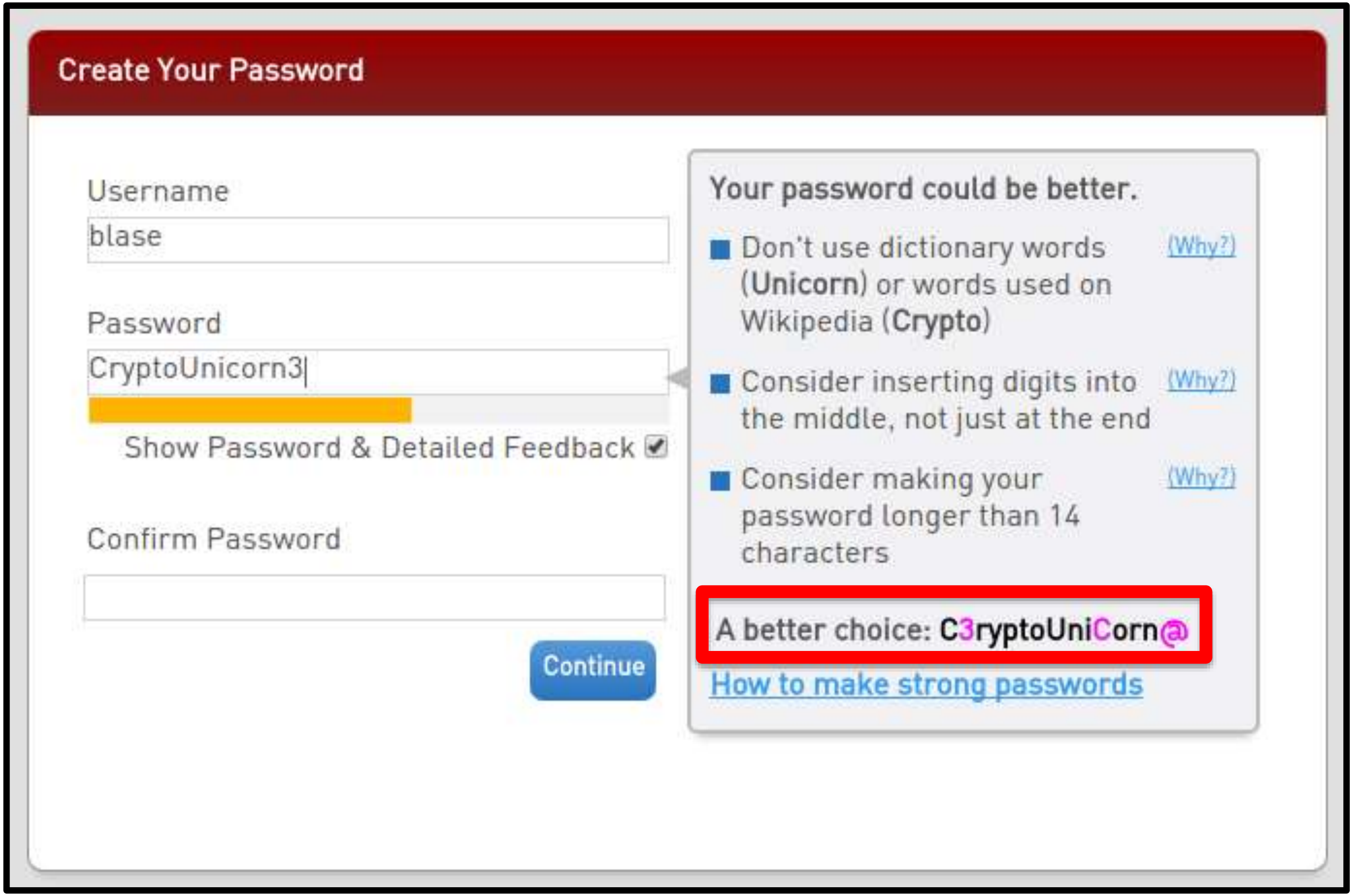
Your password could be better.

- Don't use dictionary words (**Unicorn**) or words used on Wikipedia (**Crypto**) (Why?)
- Consider inserting digits into the middle, not just at the end (Why?)
- Consider making your password longer than 14 characters (Why?)

A better choice: **C3ryptoUniCorn@**

How to make strong passwords

Standard Feedback



Create Your Password

Username

blase

Password

CryptoUnicorn3

Show Password & Detailed Feedback ☑

Confirm Password

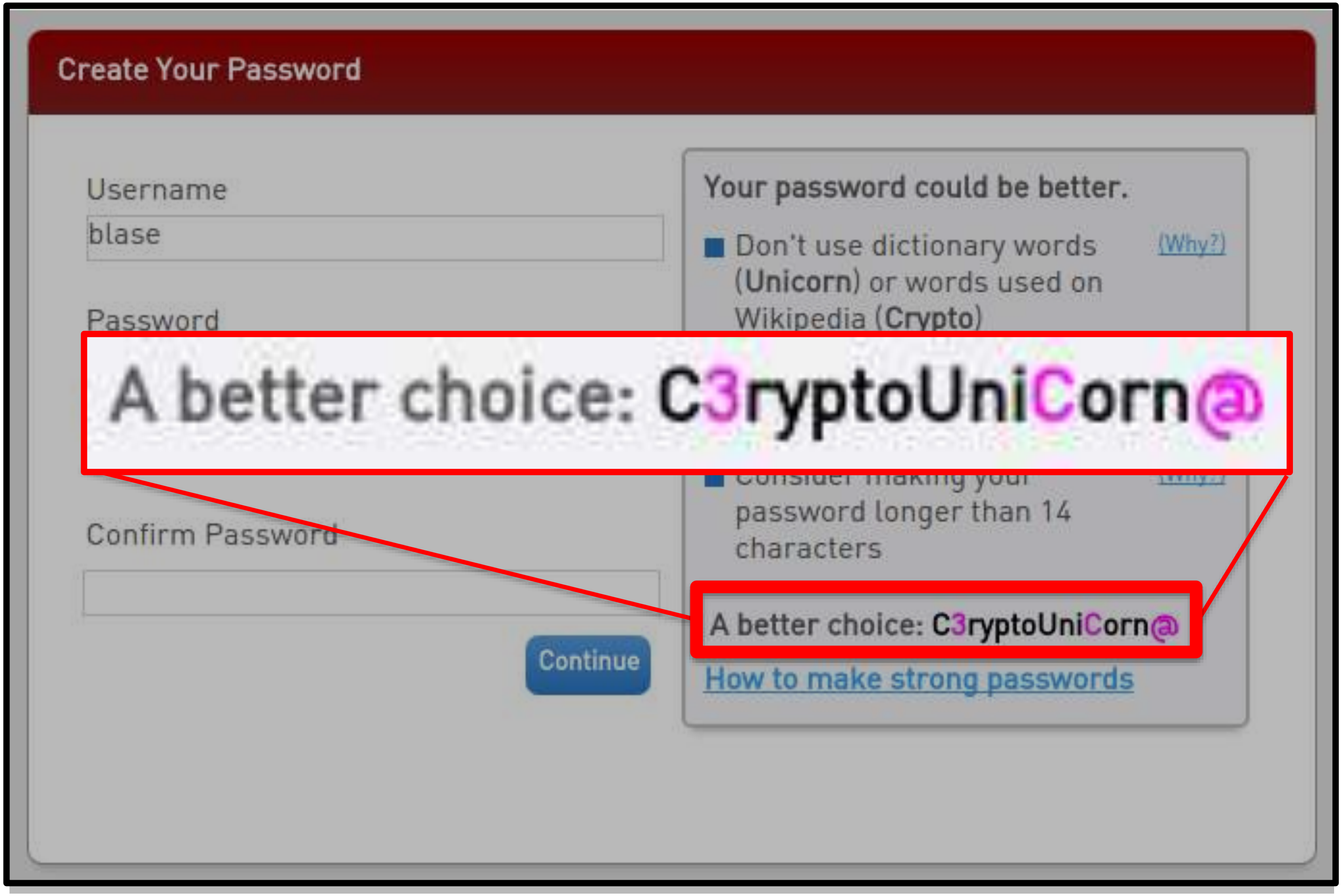
Your password could be better.

- Don't use dictionary words (**Unicorn**) or words used on Wikipedia (**Crypto**) (Why?)
- Consider inserting digits into the middle, not just at the end (Why?)
- Consider making your password longer than 14 characters (Why?)

A better choice: **C3ryptoUniCorn@**

How to make strong passwords

Standard Feedback



A better choice: C3ryptoUniCorn@

Create Your Password

Username

blase

Password

Confirm Password

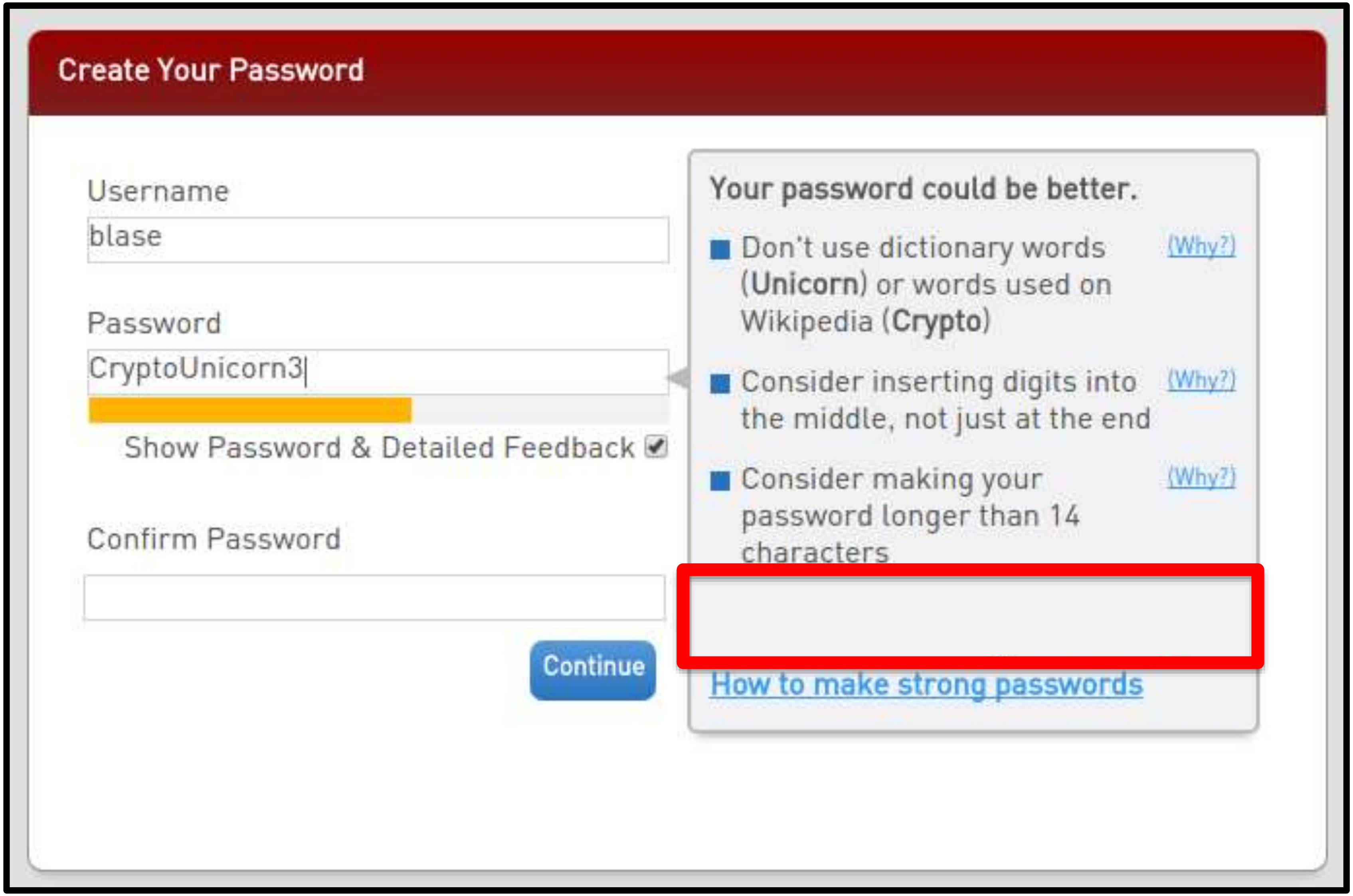
Your password could be better.

- Don't use dictionary words (**Unicorn**) or words used on Wikipedia (**Crypto**)
- Consider making your password longer than 14 characters

A better choice: C3ryptoUniCorn@

How to make strong passwords

Standard, No Suggested Improvement



Create Your Password

Username

blase

Password

CryptoUnicorn3

Show Password & Detailed Feedback ☑

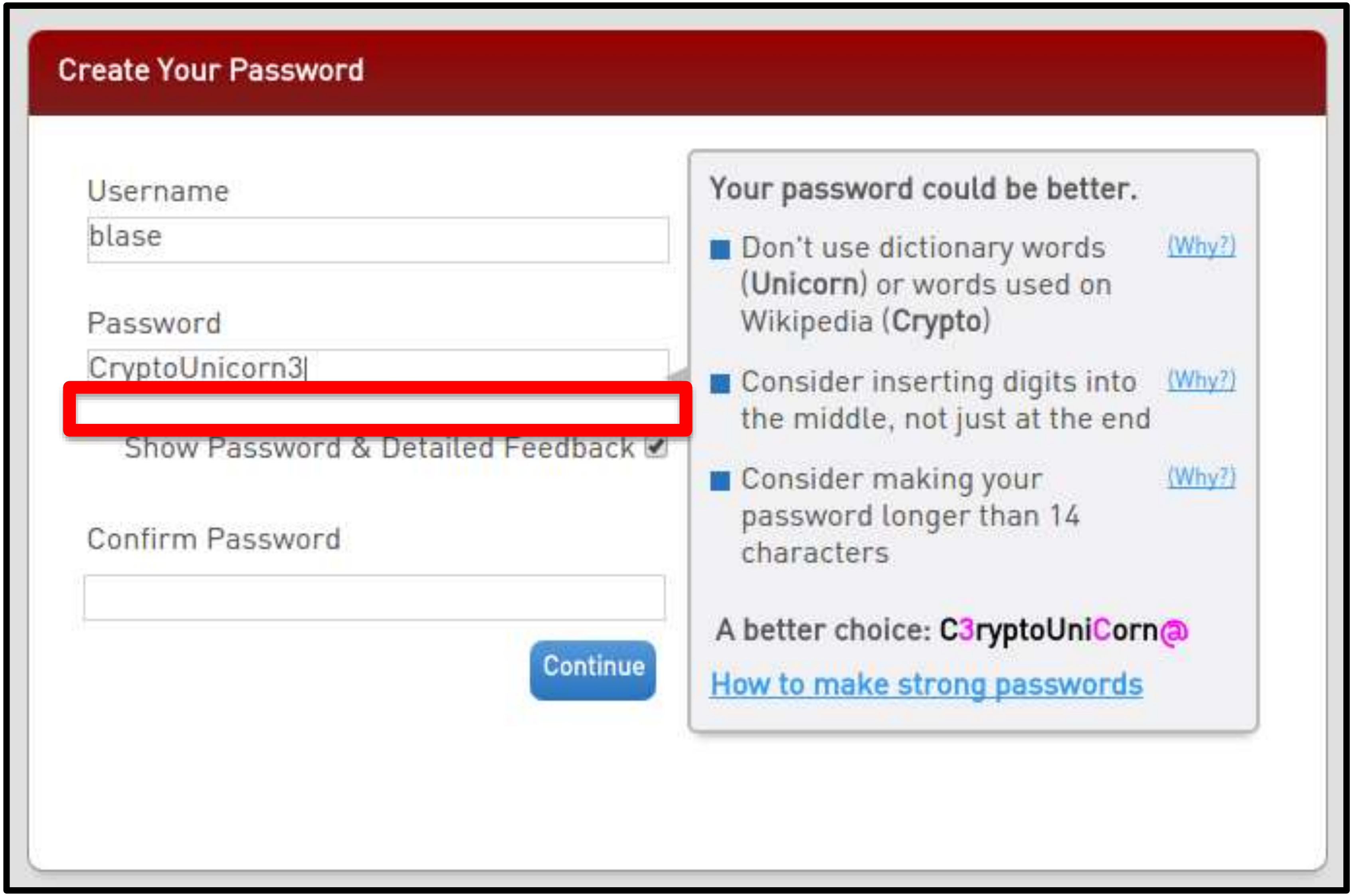
Confirm Password

Your password could be better.

- Don't use dictionary words (**Unicorn**) or words used on Wikipedia (**Crypto**) (Why?)
- Consider inserting digits into the middle, not just at the end (Why?)
- Consider making your password longer than 14 characters (Why?)

How to make strong passwords

Standard, No Bar



Create Your Password

Username

blase

Password

CryptoUnicorn3

Show Password & Detailed Feedback ☑

Confirm Password

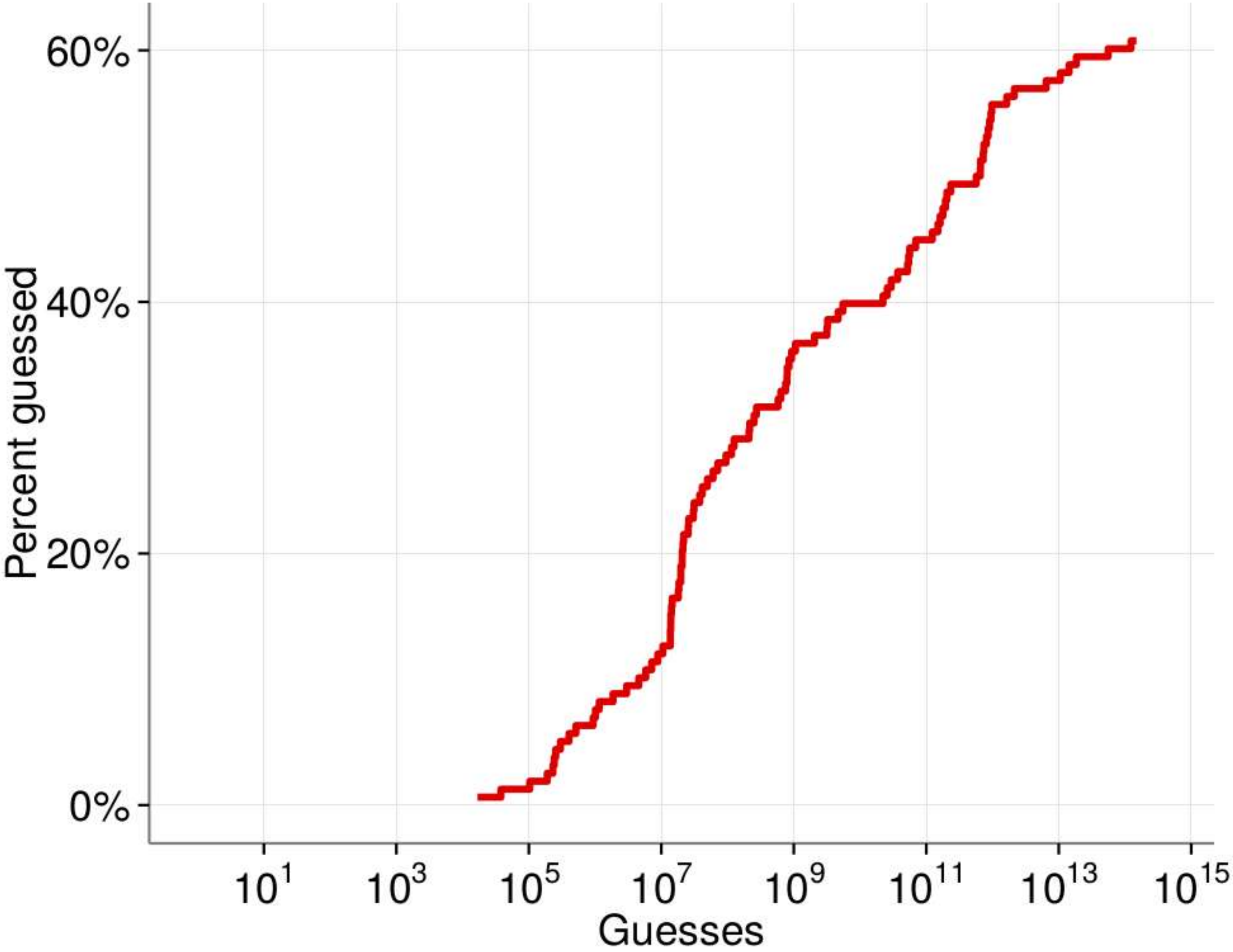
Your password could be better.

- Don't use dictionary words (**Unicorn**) or words used on Wikipedia (**Crypto**) (Why?)
- Consider inserting digits into the middle, not just at the end (Why?)
- Consider making your password longer than 14 characters (Why?)

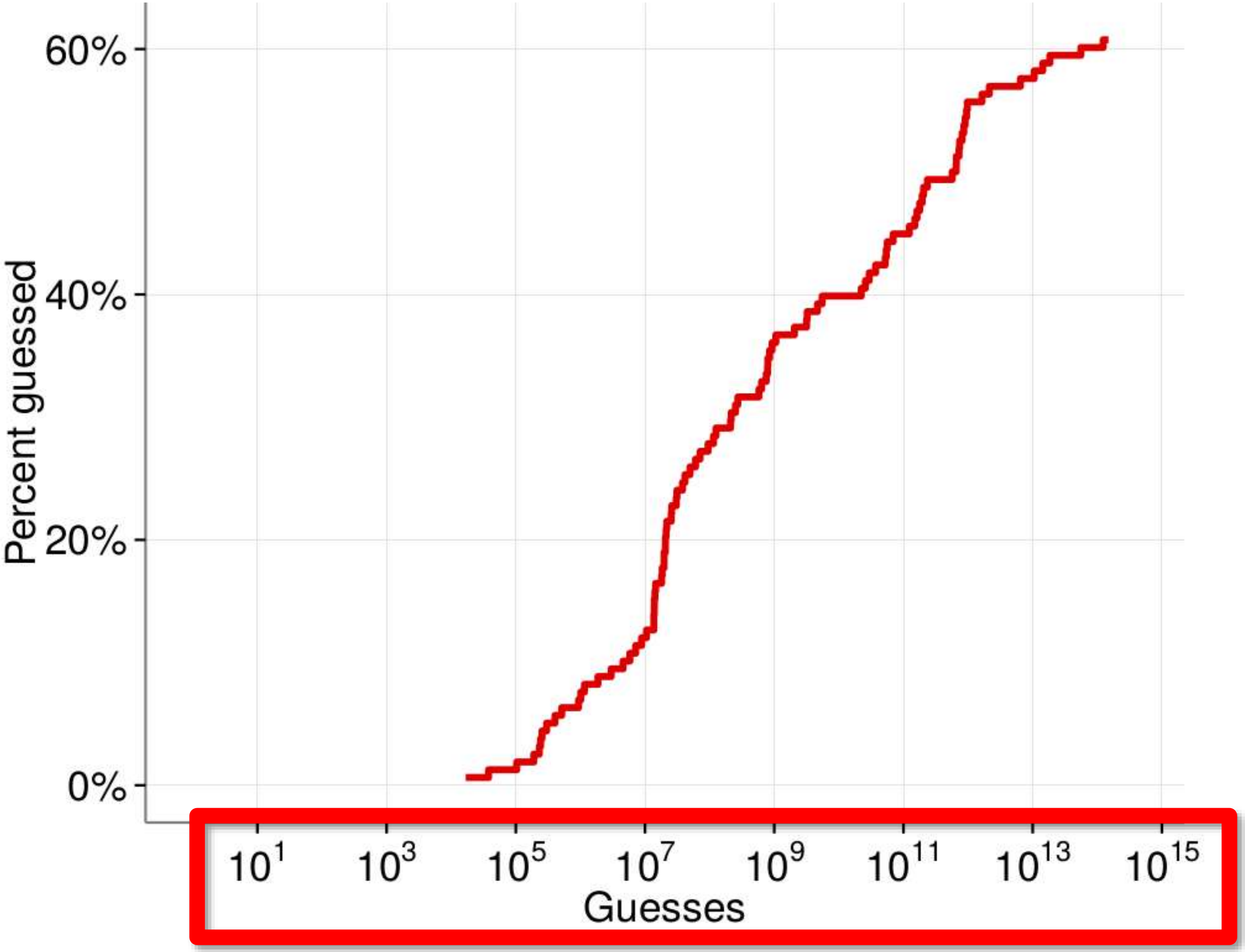
A better choice: C3ryptoUniCorn@

How to make strong passwords

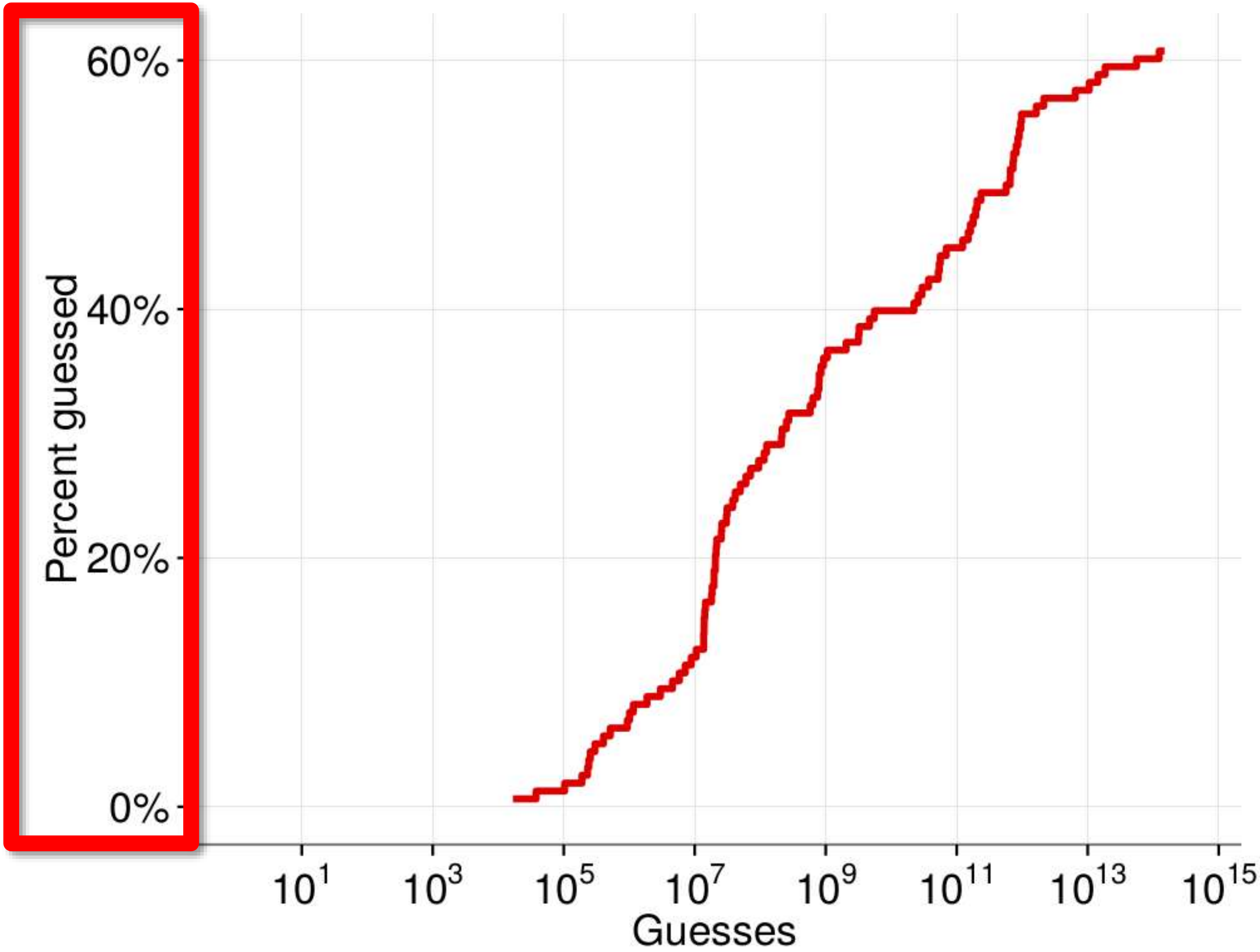
Measure Password Guessability



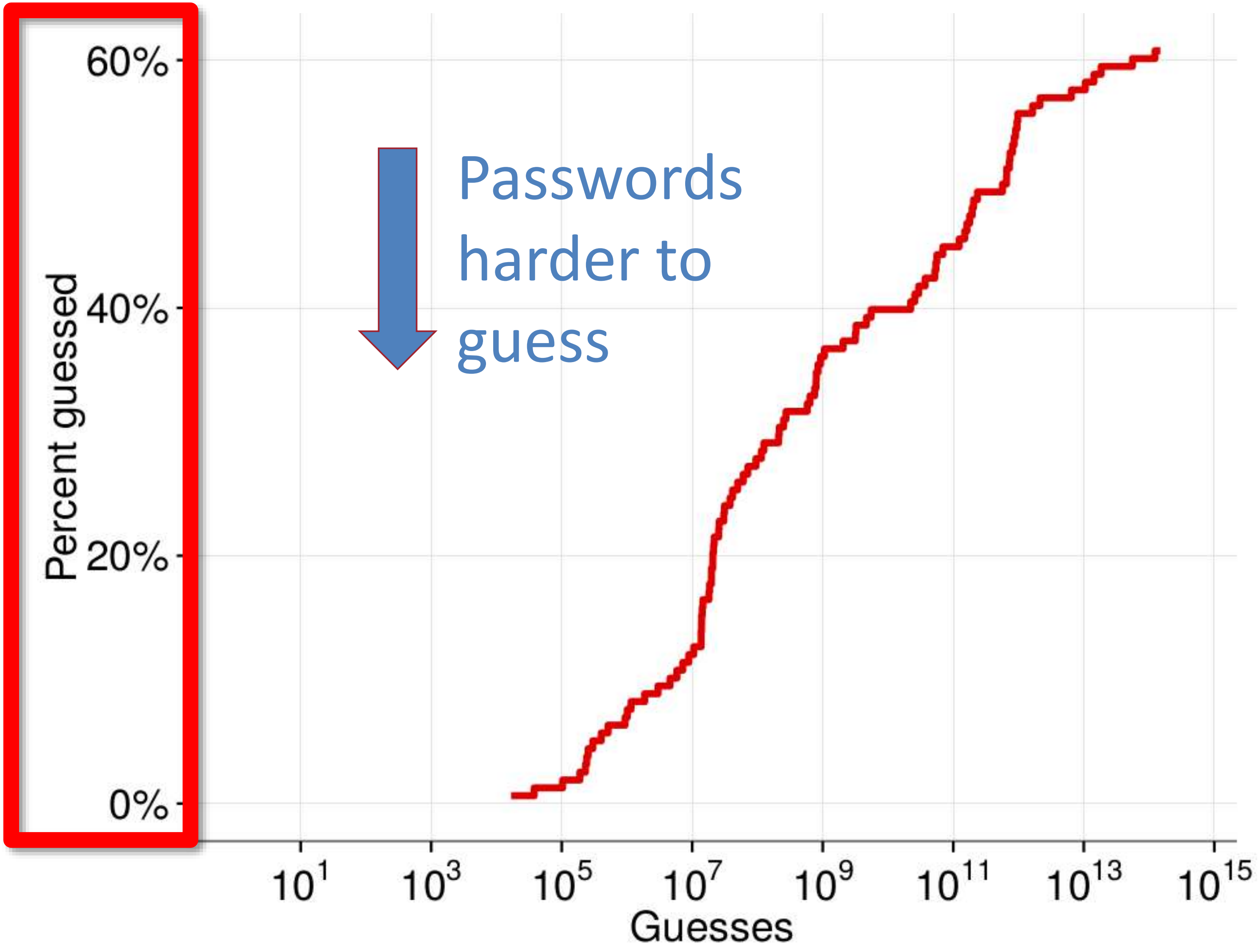
Measure Password Guessability



Measure Password Guessability

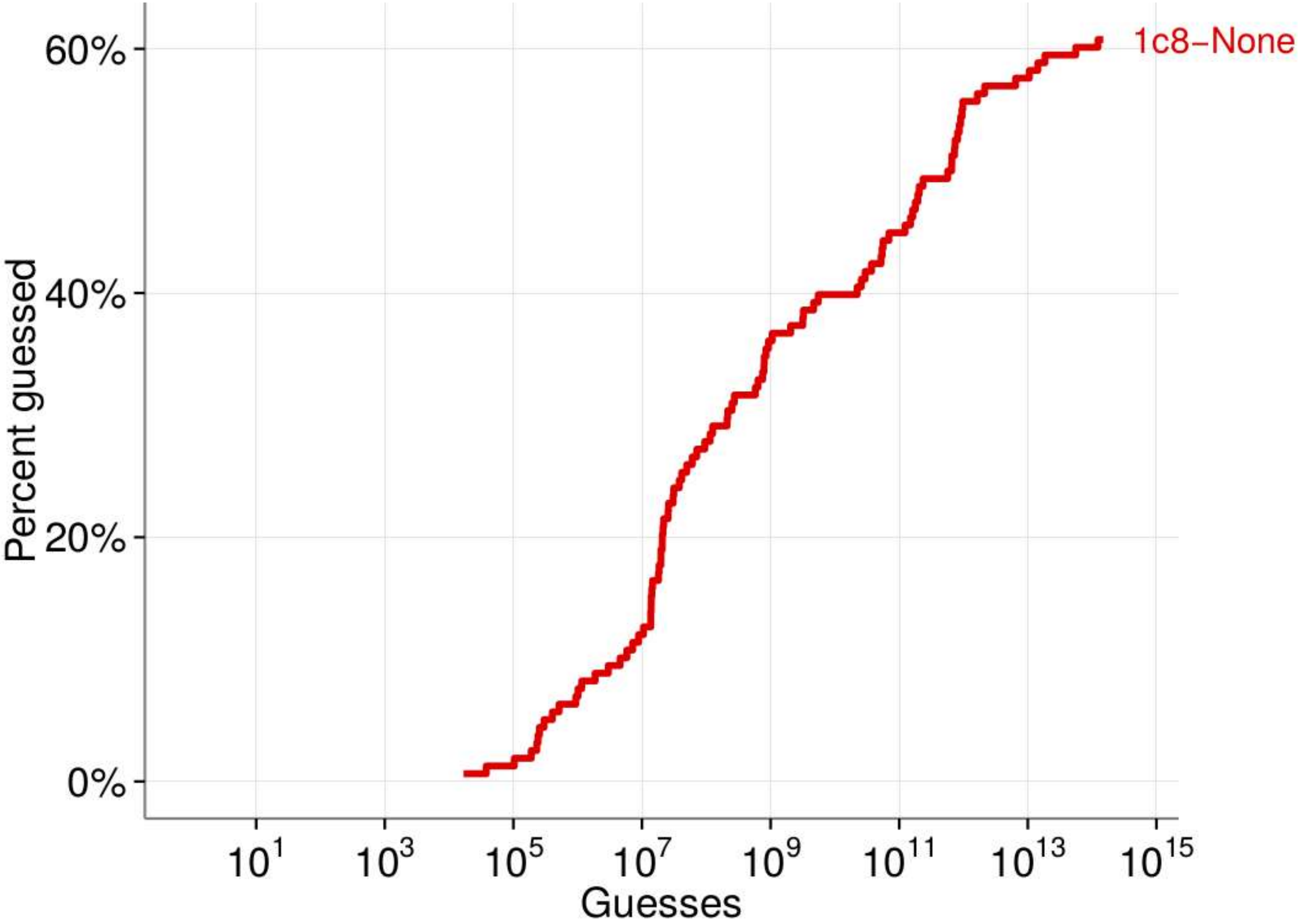


Measure Password Guessability

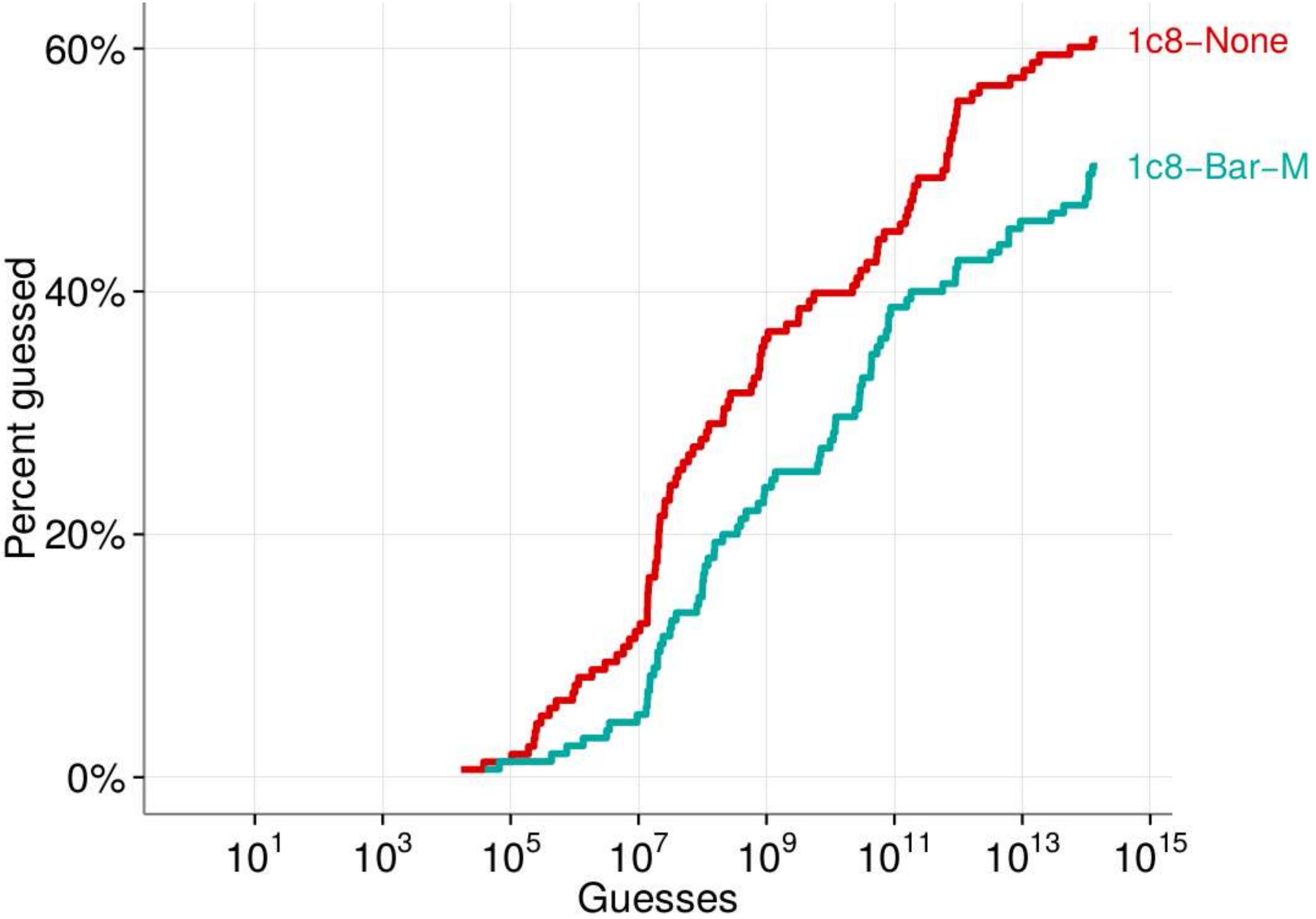


Passwords harder to guess

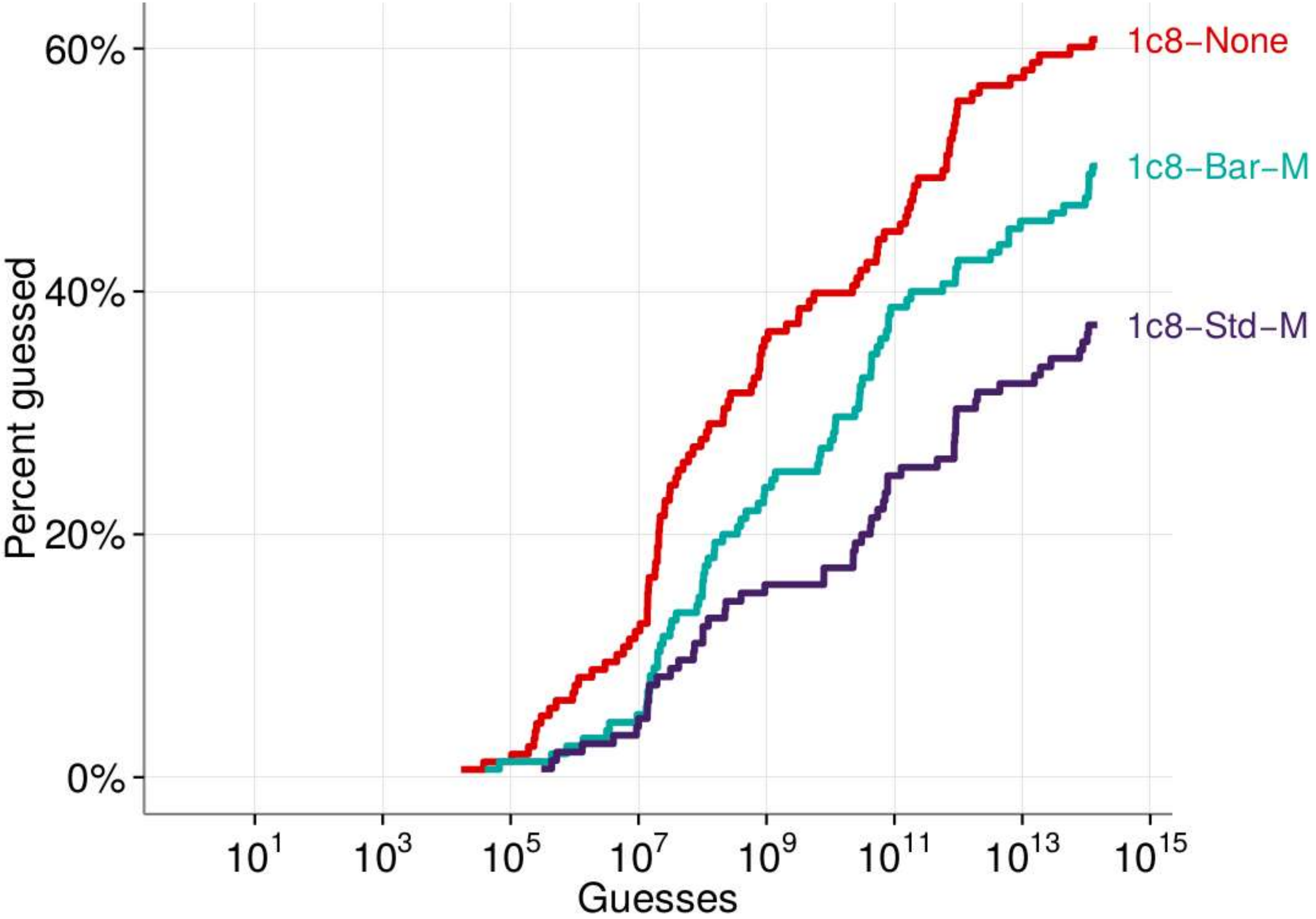
Measure Password Guessability



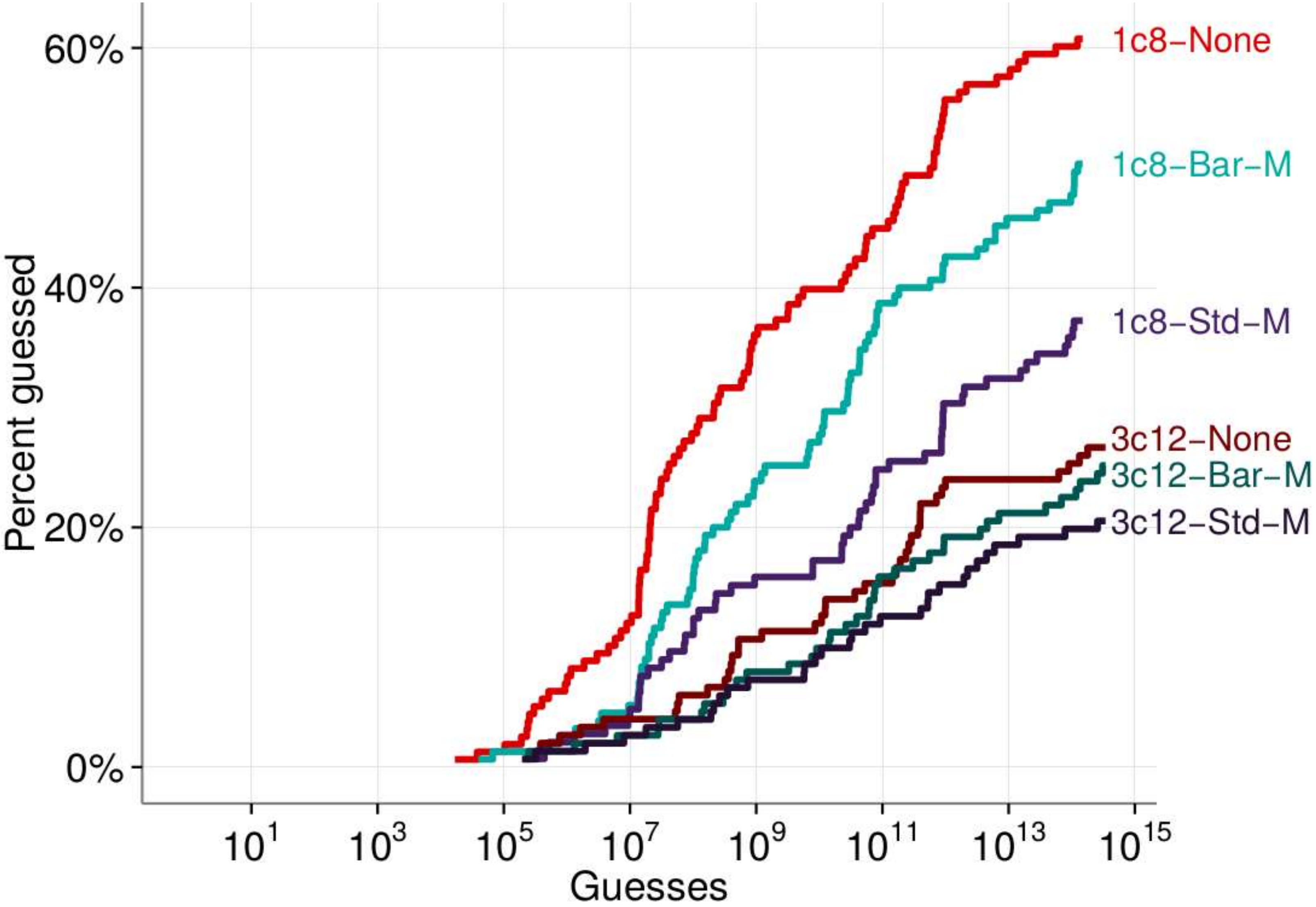
Feedback → More Secure Passwords



Feedback → More Secure Passwords



Feedback → More Secure Passwords



Usability Results

- Feedback did <u>not</u> significantly impact password memorability
- More feedback → more difficult, annoying
- All features had value for some participants

Feedback → More Secure Passwords

`https://github.com/cupslab/password_meter`

- Help us improve the meter
- Demo: `https://cups.cs.cmu.edu/meter`

Blase Ur, Assistant Professor, University of Chicago

THE UNIVERSITY OF CHICAGO

Carnegie Mellon University