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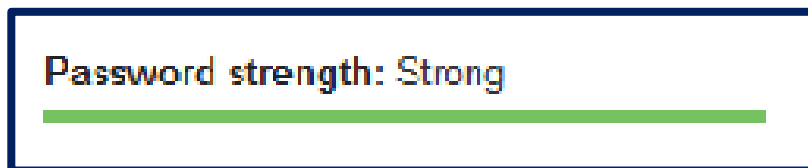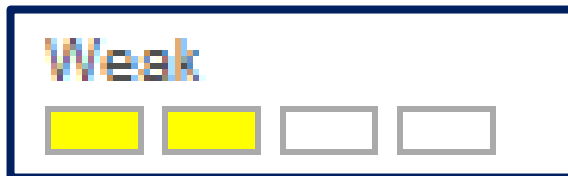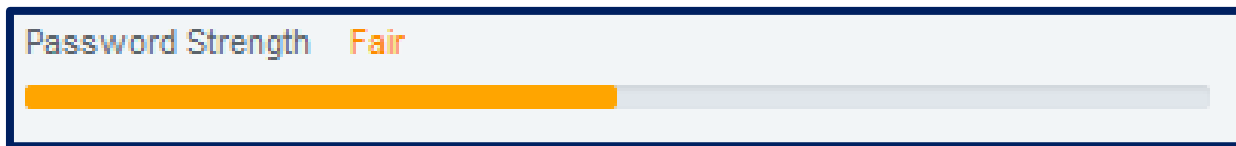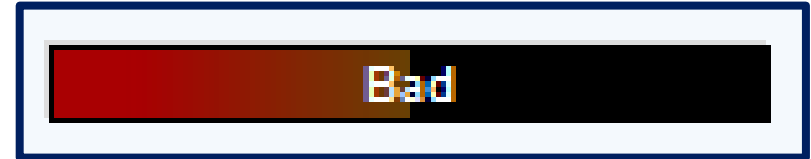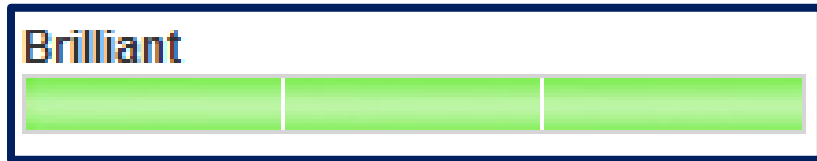
Blase Ur, Felicia Alfieri, Maung Aung, Lujo Bauer, Nicolas Christin, Jessica Colnago, Lorrie Faith Cranor, Henry Dixon, Pardis Emami Naeini, Hana Habib, Noah Johnson, William Melicher

THE UNIVERSITY OF CHICAGO

SUPER GROUP

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

Carnegie Mellon University

123 robert twitter jennifer iloveu spongebob chocolate charlie america
rangers monica dragon hottie cookie steven lovers beautiful angel
bubbles 654321 000000 michelle samantha hannah orange 123456 pizza thomas alejandro carlos superman whatever
babygirl william monkey jessica eminem 789456
tigger buster shadow purple melissa nicole liverpool naruto password flower soccer computer
rockyou princess michael christian andrea rachel tinkerbell junior 12345678 ashley password1
softball matthew 123456789 daniel anthony mickey
playboy 666666 jasmine jesus poohbear elizabeth brandon
chelsea jordan football friends loveme
dancer pretty barbie secret lovely danielle angels justin qwerty iloveyou jasmine sandra basketball
abc123 hello sunshine angel superman butterfly miguel

Password Meters Are Ubiquitous

Brilliant

Bad

Password Strength   Fair

Weak

Fair
- ✓ Include at least 8 characters
- ✓ Don't use your name or email address
- ▪ Use a mix of uppercase and lowercase letters, numbers, and symbols
- ✓ Make your password hard to guess - even for a close friend

Password strength: Strong

Problem 1: Inaccurate Scoring

Problem 2: Unhelpful Feedback

✗ Please enter a stronger password.

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

Neural Network to Estimate Strength
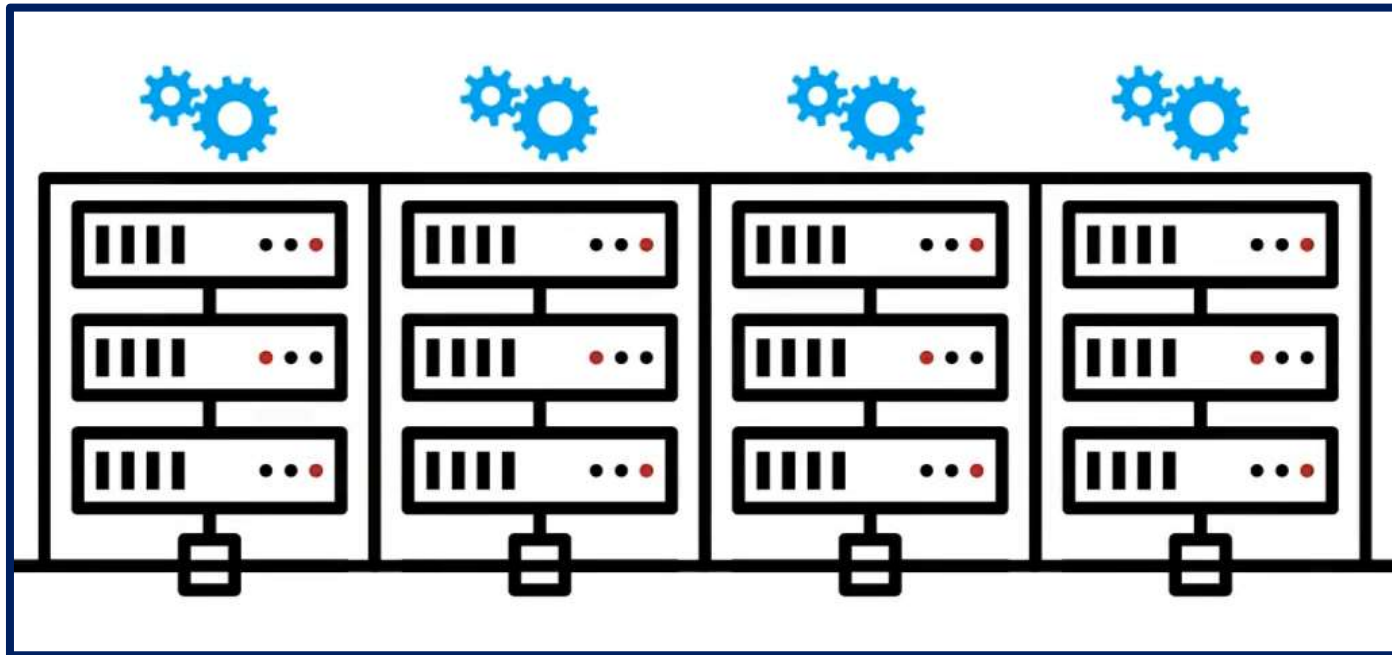
W. Melicher, B. Ur, S. Segreti, S. Komanduri,
L. Bauer, N. Christin, L. Cranor.
Fast, Lean, and Accurate: Modeling Password
Guessability Using Neural Networks.
In Proc. USENIX Security, 2016.

8

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 ☐

Continue

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

Your password <u>must</u>:

☐ 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 ☐

Continue

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

Your password <u>must</u>:

☐ 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

••••••••

Show Password ☐

Continue

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

Your password <u>must</u>:

☐ 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

…Provides Text Feedback

Create Your Password

Username

blase

Password

....

Show Password & Detailed Feedback ☐

Confirm Password

Continue

Your password could be better.

- Don't use dictionary words or (Why?) words used on Wikipedia

- Consider inserting digits into (Why?) the middle

- Consider making your (Why?) password longer

See Your Password With Our Improvements

How to make strong passwords

18

…Gives Detail (Password Shown)

Create Your Password

Username

blase

Password

CryptoUnicorn3|

Show Password & Detailed Feedback ☑

Confirm Password

Continue

Your password could be better.

■ Don't use dictionary words (Why?) (**Unicorn**) or words used on Wikipedia (**Crypto**)

■ Consider inserting digits into (Why?) the middle, not just at the end

■ Consider making your (Why?) password longer than 14 characters

A better choice: **C3ryptoUniCorn@**

How to make strong passwords

…Offers Explanations

Create Your Password

Username

blase

Password

CryptoUnicorn3|

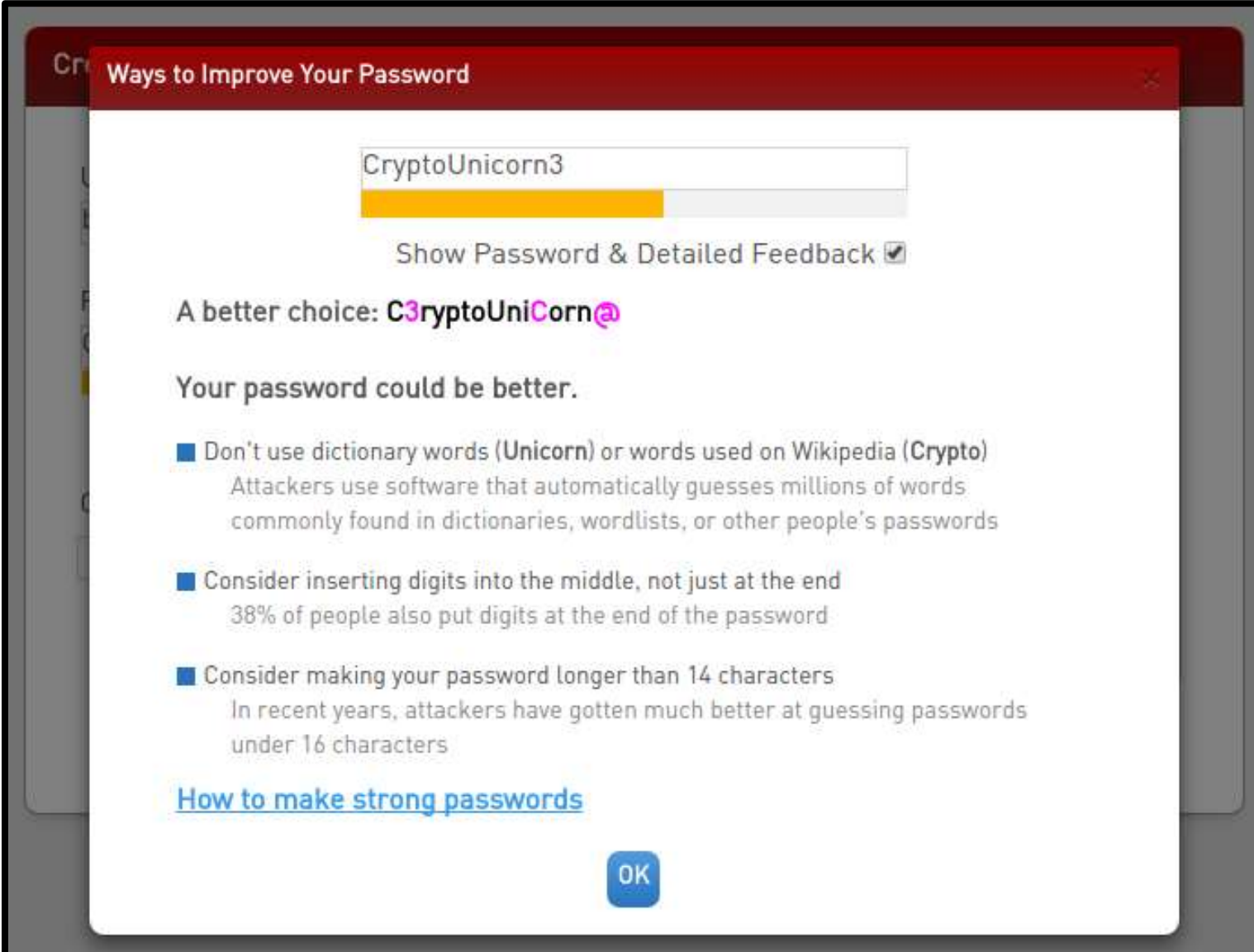Show Password & Detailed Feedback ☑

Confirm Password

Continue

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

20

Explanations Shown in Modal

Cr... **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

OK

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

Continue

Bar Only

Create Your Password

Username

blase

Password

....

Show Password & Detailed Feedback

Confirm Password

Continue

Public (Non-Sensitive) Feedback

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

Standard Feedback

Create Your Password

Username

blase

Password

CryptoUnicorn3

Show Password & Detailed Feedback ✔

Confirm Password

Continue

Your password could be better.

■ Don't use dictionary words   (Why?)
   (**Unicorn**) or words used on
   Wikipedia (**Crypto**)

■ Consider inserting digits into   (Why?)
   the middle, not just at the end

■ Consider making your   (Why?)
   password longer than 14
   characters

A better choice: **C3ryptoUniCorn@**

How to make strong passwords

32

Standard Feedback

Create Your Password

Username

blase

Password

CryptoUnicorn3|

Show Password & Detailed Feedback ☑

Confirm Password

Continue

Your password could be better.

■ Don't use dictionary words (Why?)
(**Unicorn**) or words used on
Wikipedia (**Crypto**)

■ Consider inserting digits into (Why?)
the middle, not just at the end

■ Consider making your (Why?)
password longer than 14
characters

A better choice: **C3ryptoUniCorn@**

How to make strong passwords

Standard Feedback

Create Your Password

Username

blase

Password

A better choice: C3ryptoUniCorn@

Your password could be better.

- Don't use dictionary words   (Why?)
  (**Unicorn**) or words used on
  Wikipedia (**Crypto**)

Confirm Password

- Consider making your   (Why?)
  password longer than 14
  characters

A better choice: **C3ryptoUniCorn@**

Continue

How to make strong passwords

Standard, No Suggested Improvement

Create Your Password

Username

blase

Password

CryptoUnicorn3|

Show Password & Detailed Feedback ☑

Confirm Password

Continue

Your password could be better.

■ Don't use dictionary words (Why?) (**Unicorn**) or words used on Wikipedia (**Crypto**)

■ Consider inserting digits into (Why?) the middle, not just at the end

■ Consider making your (Why?) password longer than 14 characters

How to make strong passwords

Standard, No Bar

Create Your Password

Username

blase

Password

CryptoUnicorn3|

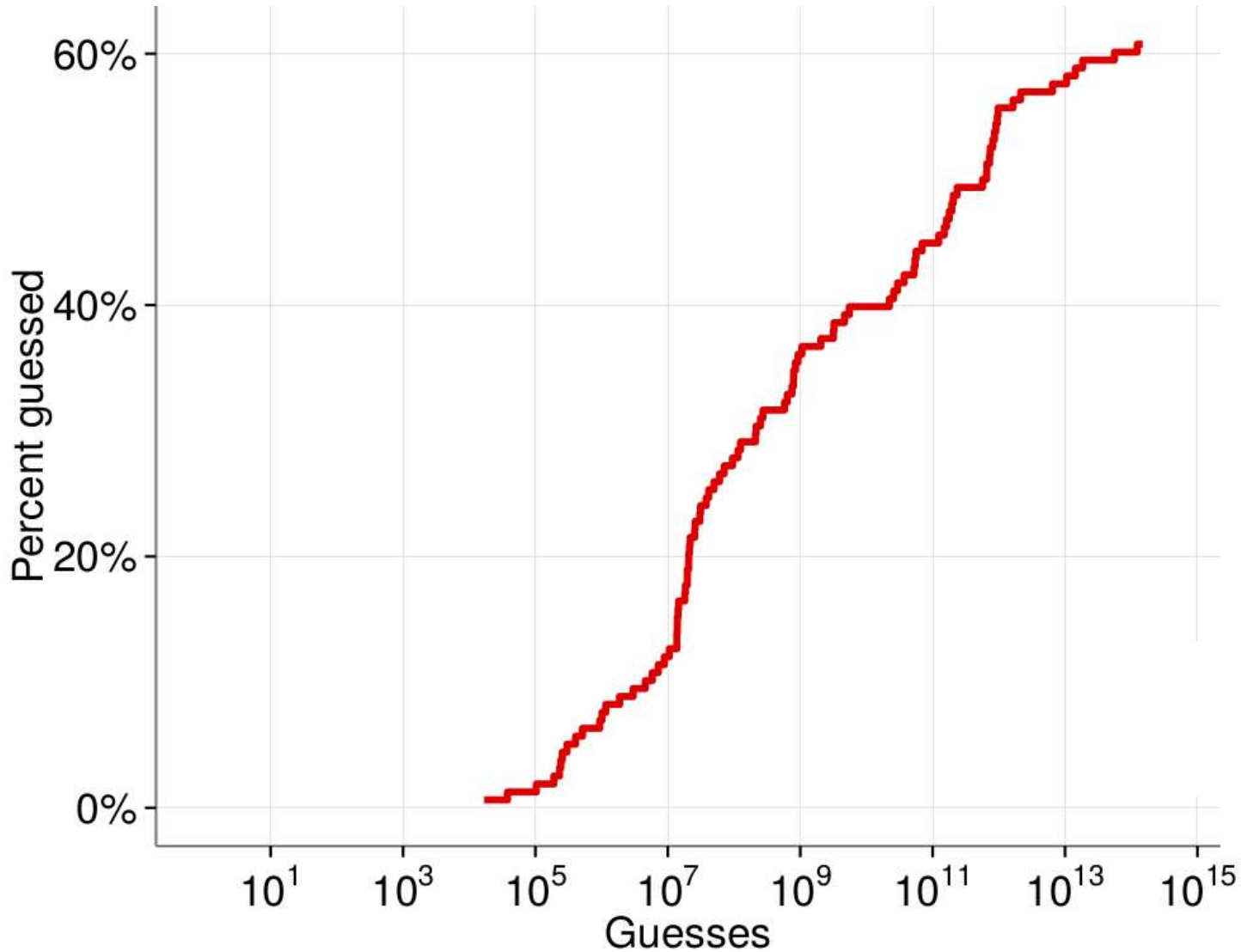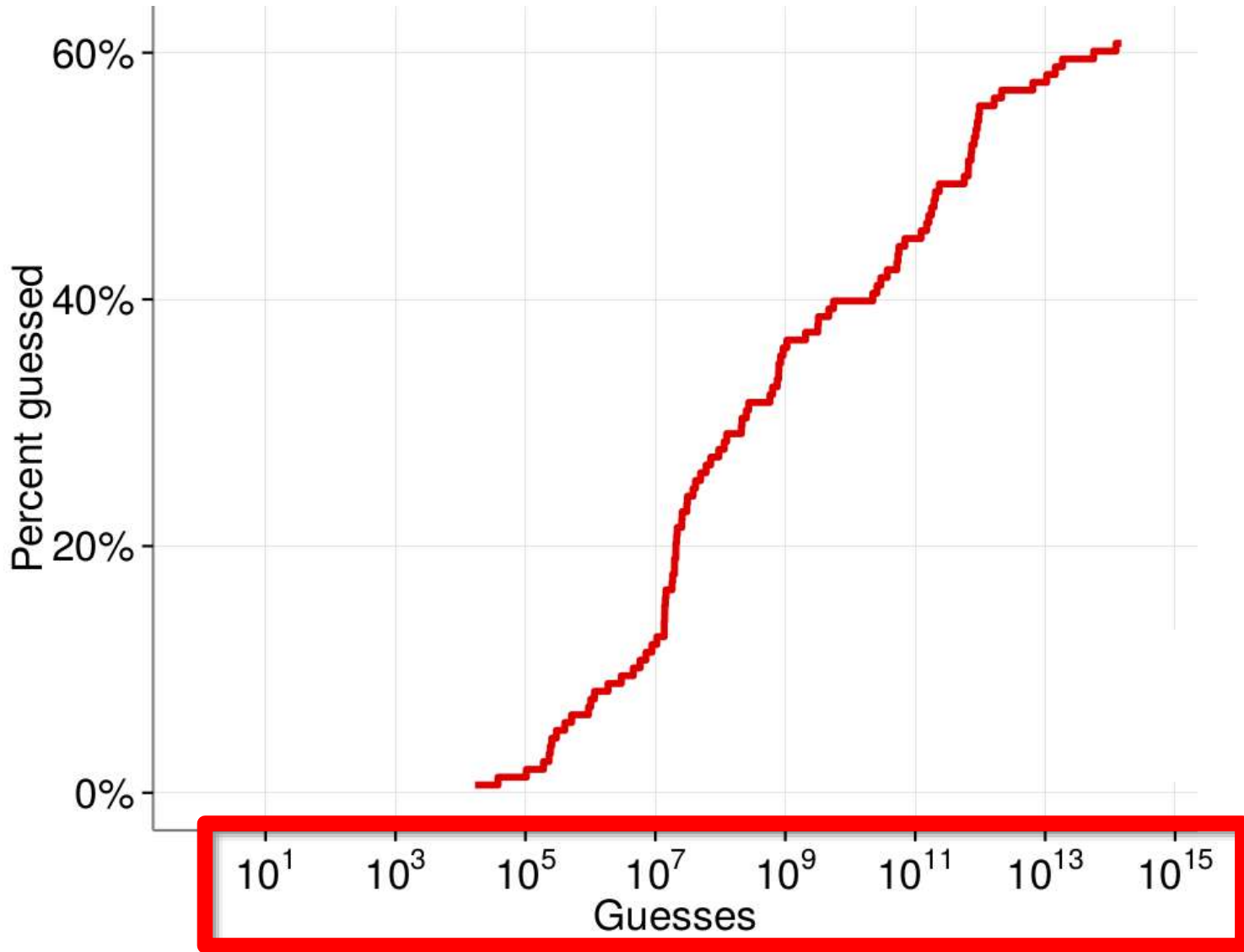Show Password & Detailed Feedback ☑

Confirm Password

Continue

Your password could be better.

■ Don't use dictionary words   (Why?)
   (**Unicorn**) or words used on
   Wikipedia (**Crypto**)

■ Consider inserting digits into   (Why?)
   the middle, not just at the end

■ Consider making your   (Why?)
   password longer than 14
   characters

A better choice: **C3ryptoUniCorn@**
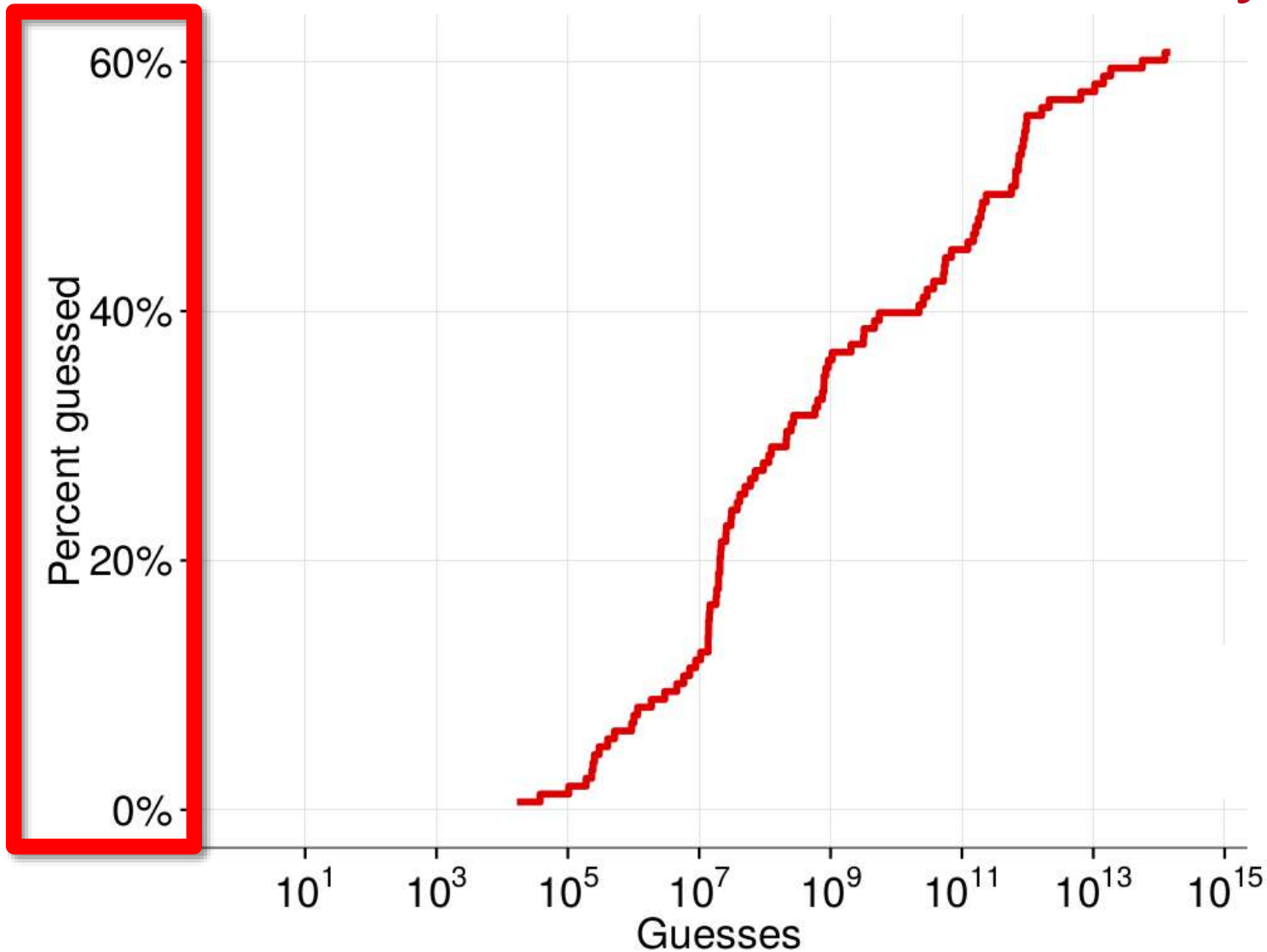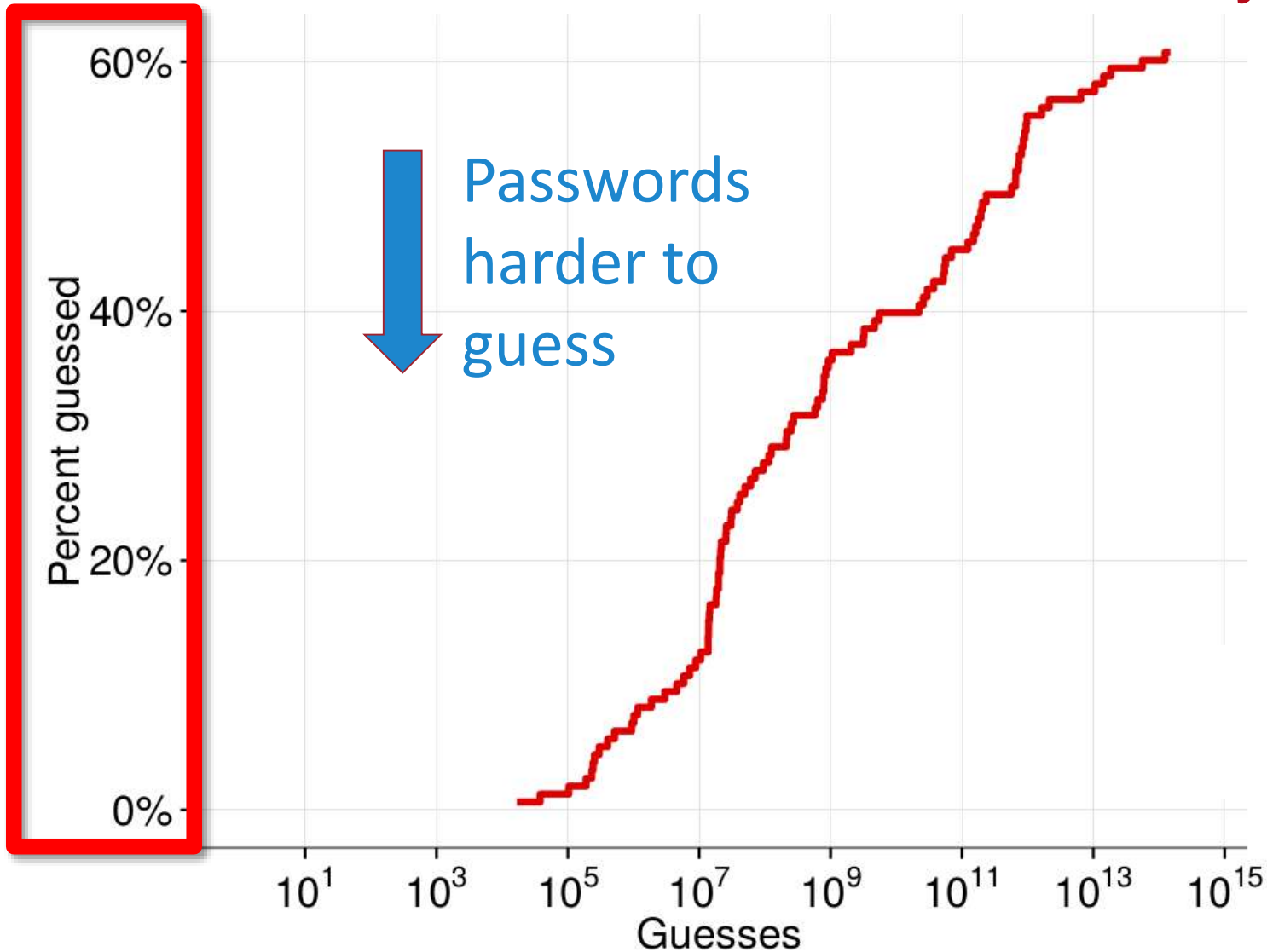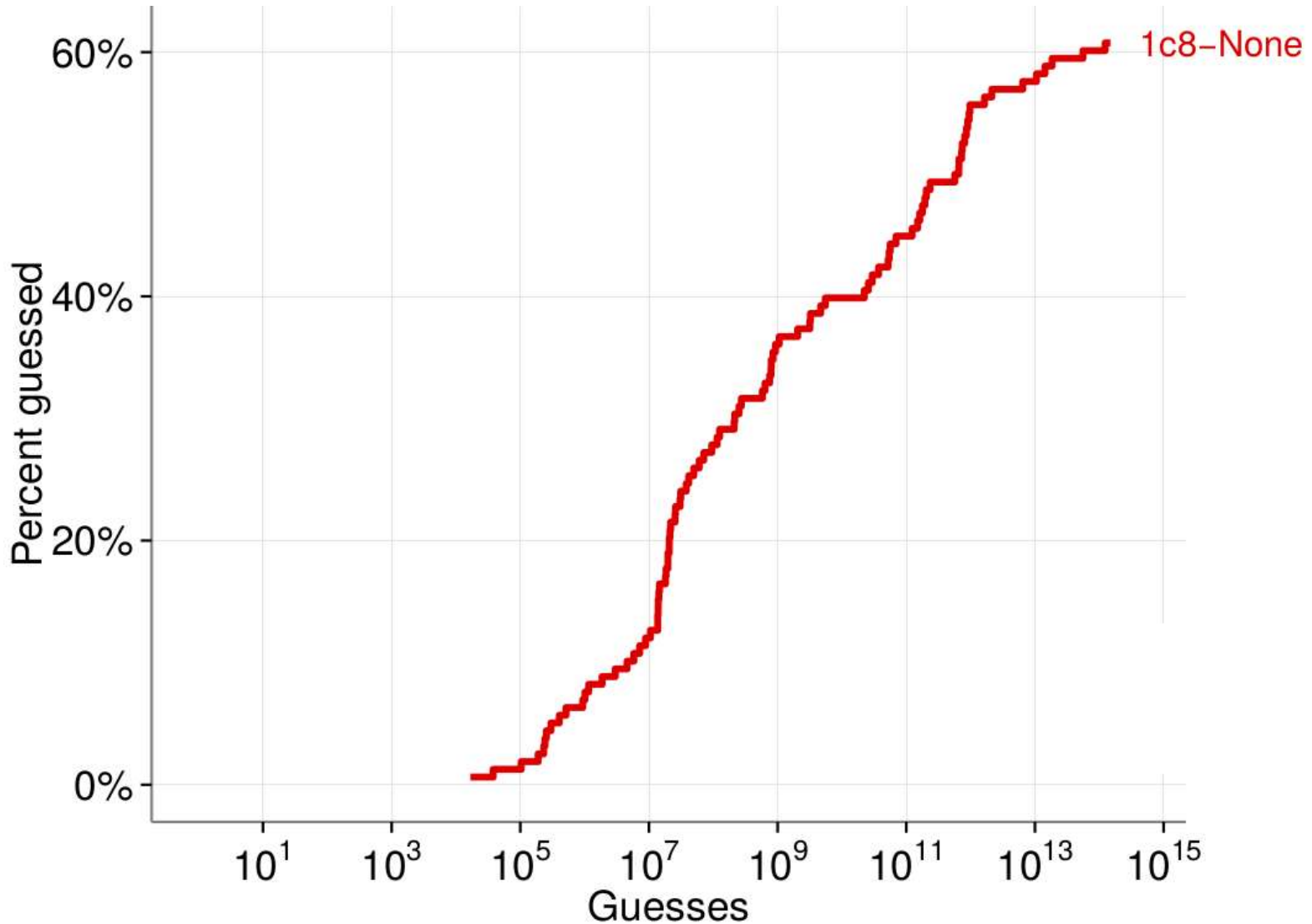
How to make strong passwords

Measure Password Guessability

Measure Password Guessability

Measure Password Guessability
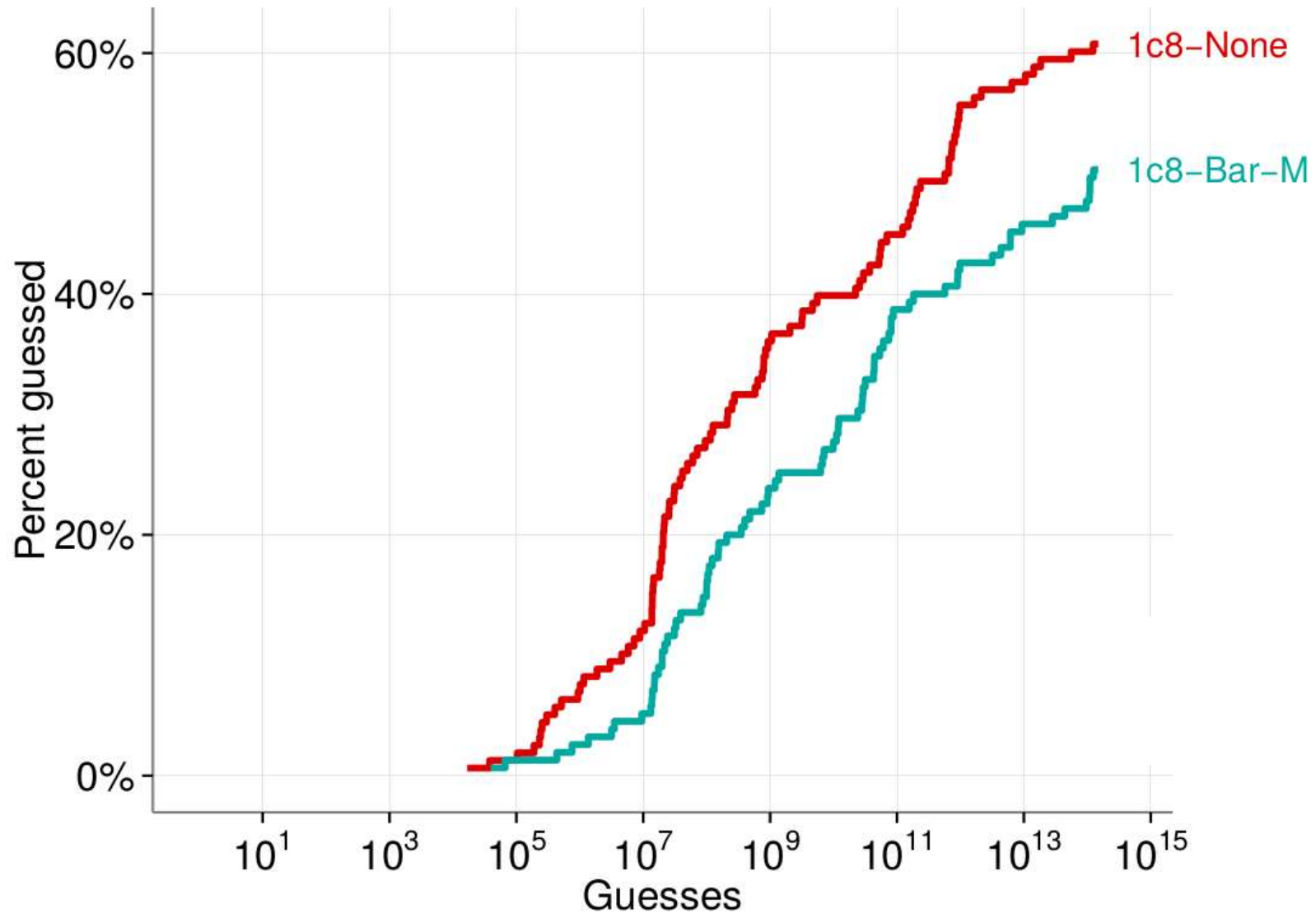
Measure Password Guessability
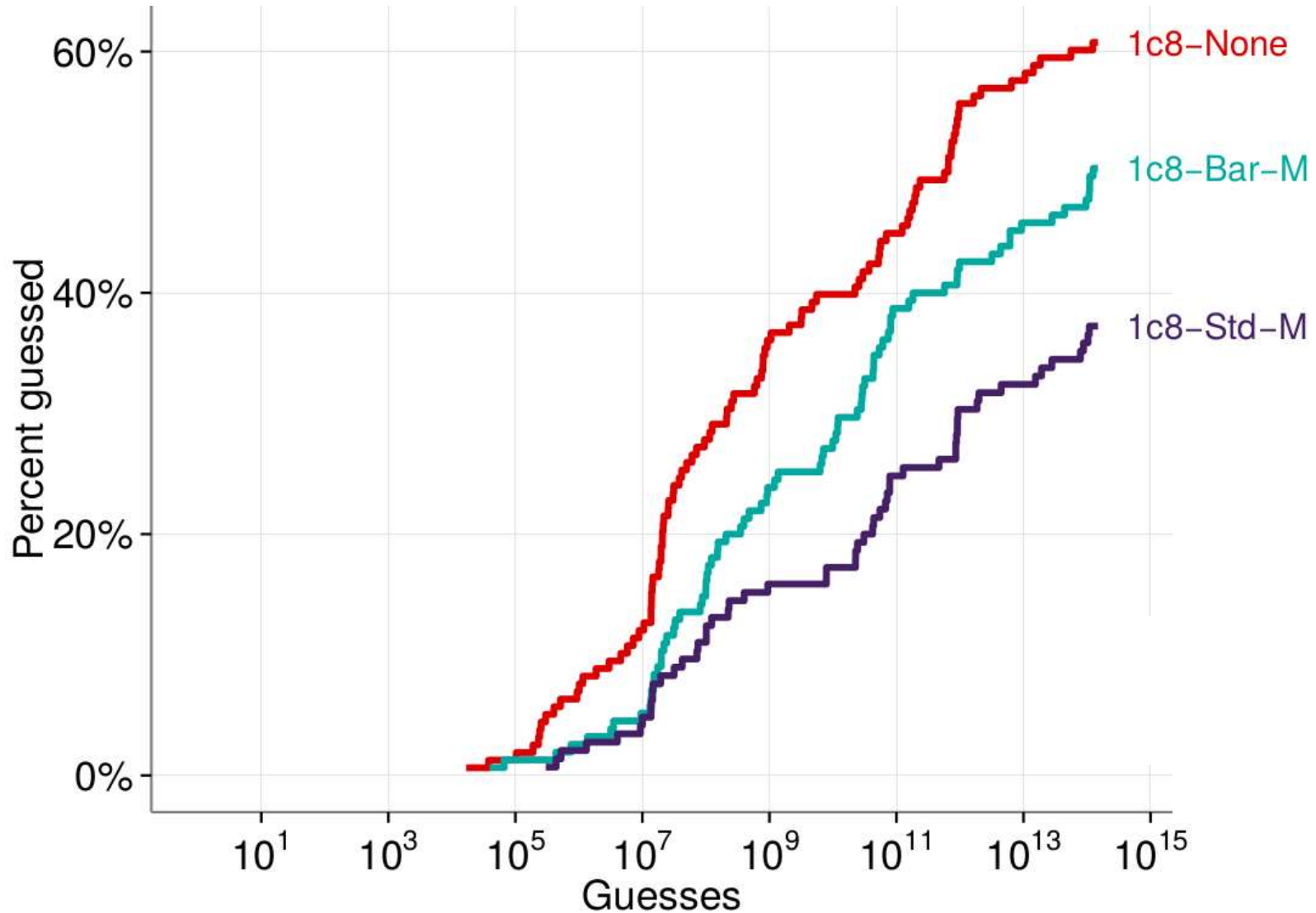

Passwords harder to guess

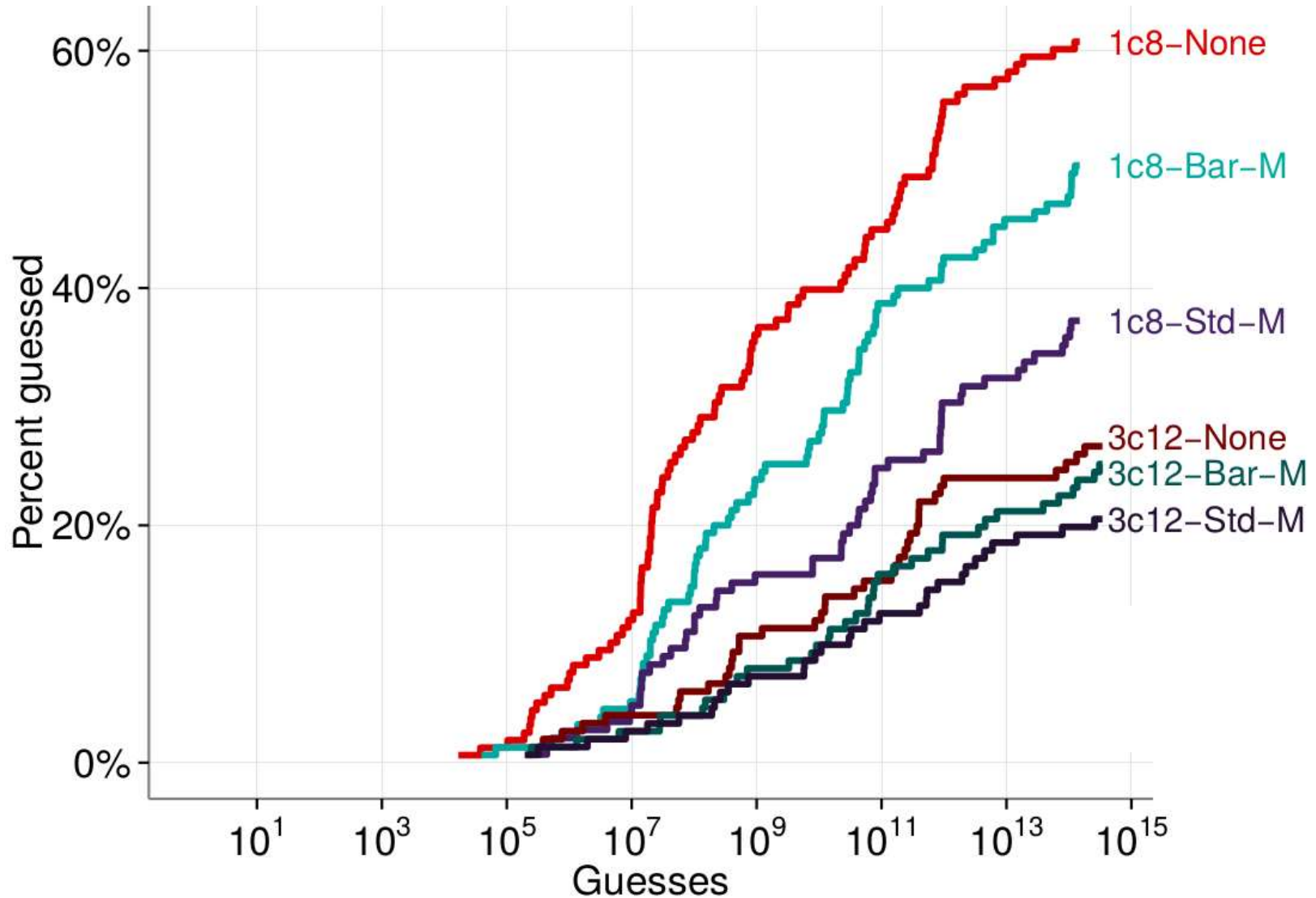# Measure Password Guessability

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

Code Is Open Source

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

- Deploy now for policies like 1class8

- Help us improve the meter

- Demo: **`https://cups.cs.cmu.edu/meter`**

Design and Evaluation of a Data-Driven Password Meter
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