Authentication and Access Control

Blase Ur, David Cash, Ben Zhao

UChicago CMSC 23200//33250

THE UNIVERSITY OF CHICAGO

UCHICAGO SUPER GROUP

Who Am I?

- Ben Zhao
  - Distinguished professor
  - Co-director of SAND Lab
  - Fan of pandas

Or Am I?

How (and why) do we authenticate users?

Why We Authenticate

- Verify that **people** or **things** (e.g., a server) are who they claim to be
- Authentication ≠ Authorization
  - *Authorization* is deciding whether an entity should have access to a given resource
- Terminology:
  - **Principal:** the legitimate owner of an identity
  - **Claimant:** entity attempting to be authenticated as the principal

Relationships Among Concepts

- How is **authentication** related to **access control**?
- How is the design of **secure systems** related to **authentication**?
- How is **authentication** related to human factors?

How We Authenticate (1/2)

How We Authenticate (1/2)

- Something you know
  - Password
  - PIN (Personal Identification Number)

How We Authenticate (1/2)

- Something you know
  - Password
  - PIN (Personal Identification Number)
- Something you have
  - Smart card
  - Private key (of a public-private key pair)
  - Phone (running particular software)

How We Authenticate (1/2)

- Something you know
  - Password
  - PIN (Personal Identification Number)
- Something you have
  - Smart card
  - Private key (of a public-private key pair)
  - Phone (running particular software)
- Something you are
  - Biometrics (e.g., iris or fingerprint)

How We Authenticate (2/2)

- Somewhere you are
  - Location-limited channels

How We Authenticate (2/2)

- Somewhere you are
  - Location-limited channels
- Someone you know (social authentication)
  - Someone vouches for you
  - You can identify people you should know

How We Authenticate (2/2)

- Somewhere you are
  - Location-limited channels
- Someone you know (social authentication)
  - Someone vouches for you
  - You can identify people you should know
- Some system vouches for you
  - Single sign-on (e.g., UChicago shib)
  - PKI Certificate Authorities

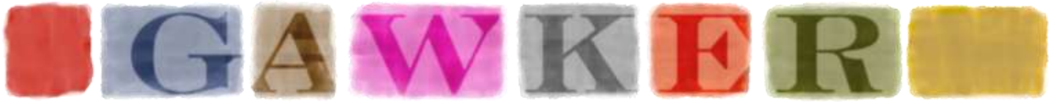
12345
123456789
password
iloveyou
princess
rockyou
1234567
12345678
abc123
nicole
babygirl
654321
monkey
jessica
lovely
michael
ashley
qwerty
111111
daniel
000000
tigger
soccer
angel
carlos
michelle
sunshine
chocolate
password1
anthony
butterfly
jordan
liverpool
purple
football
basketball
superman
playboy
666666
jasmine
elizabeth
brandon
andrea
tinkerbell
softball
matthew
angels
justin
andrew
secret
chelsea
pretty
barbie
hottie
cookie
bubbles
dragon
rangers
robert
jennifer
iloveu
lovers
spongebob
charlie
america
whatever
thomas
flower
eminem
computer
shadow
sakura
princess1
melissa
summer
christian
william
samantha
hannah
orange
rainbow
jesus
mickey
joseph
junior
friends
loveme
patrick
dancer
hello
poohbear
1234567890
onelove
heaven
miguel
buster
steven
alexander
naruto
princesa
987654321

Why Are Passwords So Prevalent?

Why Are Passwords So Prevalent?

- Easy to use
- Easy to deploy
- Nothing to carry
- No “silver-bullet” alternative

Attacks on Passwords Are Common



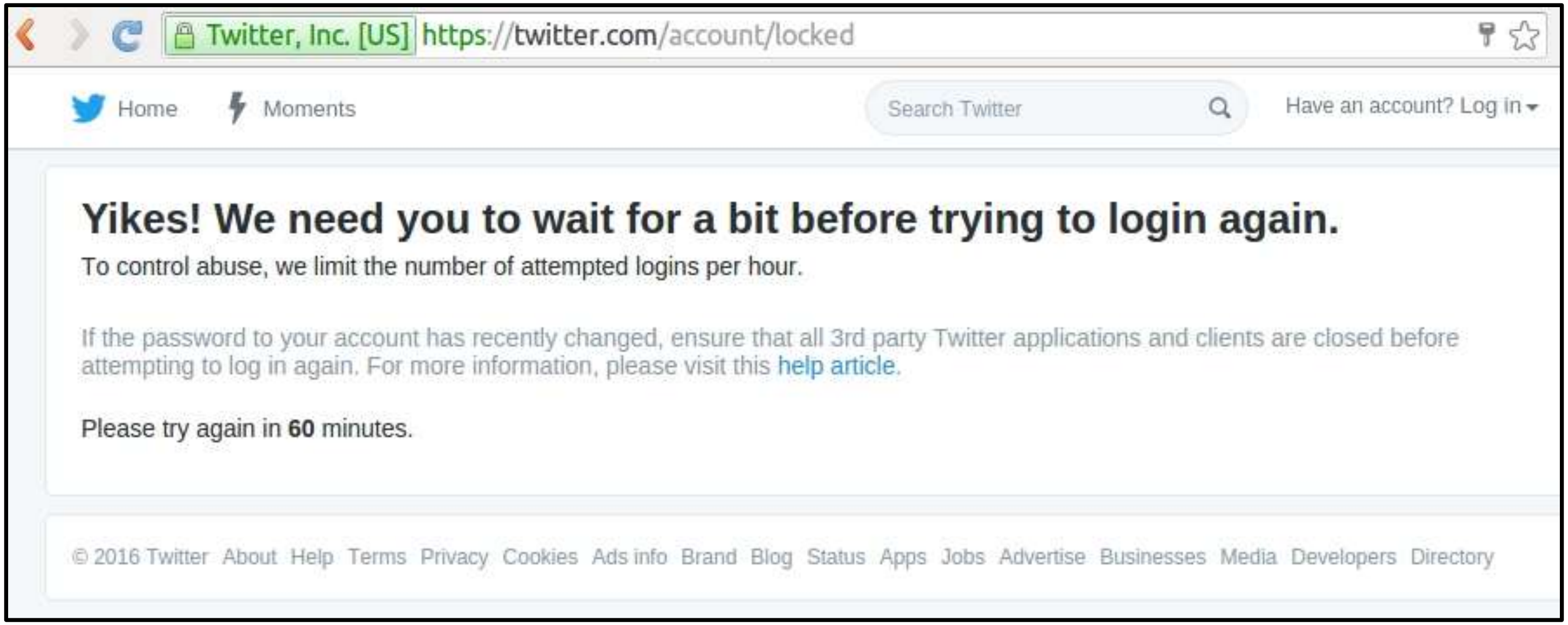
Attacks Against Passwords

Attacks Against Passwords

- Online attack
  - Try passwords on a live system
  - Usually rate-limited

Attacks Against Passwords

- Online attack
  - – Try passwords on a live system
  - – Usually rate-limited



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

Attacks Against Passwords

- Online attack
  - Try passwords on a live system
  - Usually rate-limited
- Offline attack
  - Try to guess passwords from the password store / password database

Some Breached Companies

LinkedIn

Adobe

SONY®

Domino's Pizza

GAWKER

000webhost.com
better than paid hosting

YAHOO!®

STRATFOR
GLOBAL INTELLIGENCE

Attacks Against Passwords

- Online attack
  - Try passwords on a live system
  - Usually rate-limited
- Offline attack
  - Try to guess passwords from the password store / password database
- Phishing attack

Attacks Against Passwords

- Online attack
  - Try passwords on a live system
  - Usually rate-limited
- Offline attack
  - Try to guess passwords from the password store / password database
- Phishing attack
- Shoulder surfing

Attacks Against Passwords

- Online attack
  - Try passwords on a live system
  - Usually rate-limited
- Offline attack
  - Try to guess passwords from the password store / password database
- Phishing attack
- Shoulder surfing
- Attack password-protected file / device

Storing Passwords

- **Hash** and **salt** passwords
- Hash function: one-way function
  - Traditionally designed for efficiency (e.g., MD5)
  - Password-specific hash functions (e.g., bcrypt, scrypt, PBKDF2)

Storing Passwords

- Salt: random string assigned per-user
  - Combine the password with the salt, then hash it
  - Stored alongside the hashed
  - Prevents the use of rainbow tables

Data-Driven Statistical Attacks

- (2009) 32 million passwords: rockyou
- (2016) 117 million passwords: Linkedin
- (2017) 3 billion passwords: YAHOO!
- Total: > 5 billions of passwords stolen from > 300 services

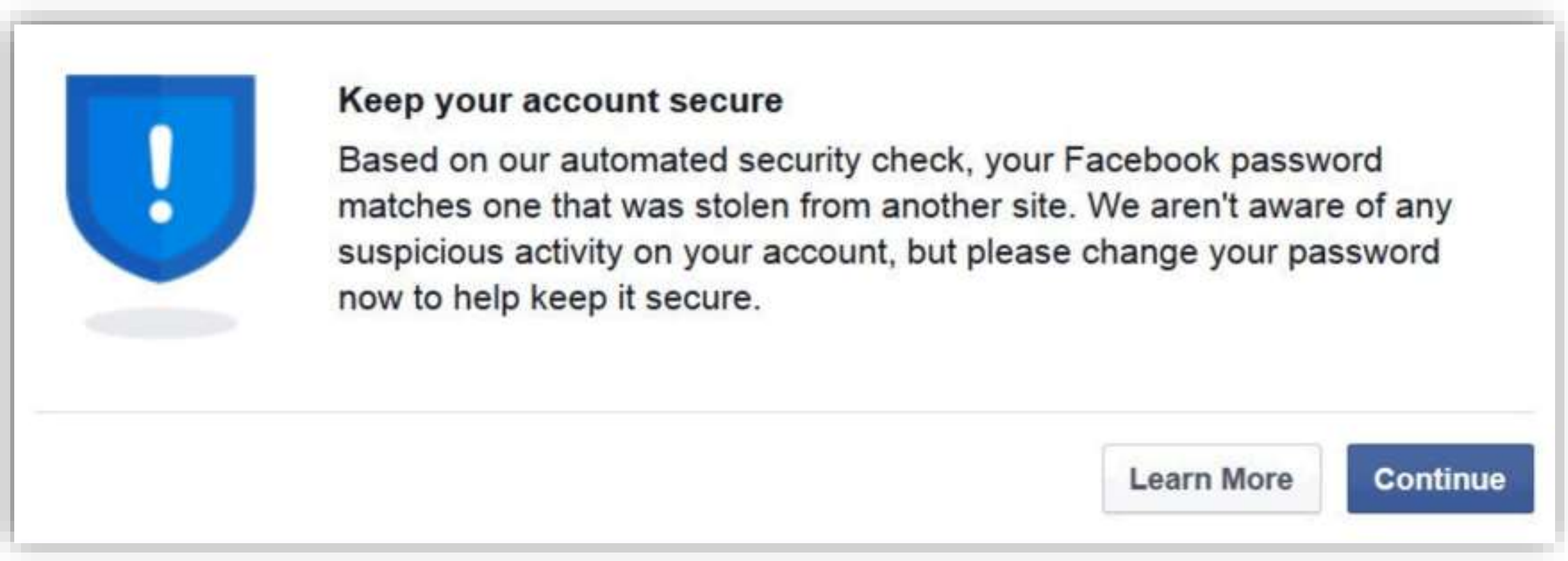
Offline Attack

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

```
$2a$04$iHdEgkI681VdDMc3f7edau9phRwORvhYjqWAIb7hb4B5uFJO1g4zi
```

- Attacker makes and hashes guesses
- Finds match → try on other sites
  - Password **reuse** is a core problem

Password Reuse-Based Attacks



Keep your account secure

Based on our automated security check, your Facebook password matches one that was stolen from another site. We aren't aware of any suspicious activity on your account, but please change your password now to help keep it secure.

Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, Blase Ur. “What was that site doing with my Facebook Password?” Designing Password-Reuse Notifications. In *Proc. CCS*, 2018.

People Reuse Passwords

Booking.com
reddit
淘宝网
Taobao.com
American Airlines
facebook
Adobe
ebay
Microsoft
slack
Baidu 百度
airbnb
YouTube
SONY
PayPal
WELLS FARGO
1&1
Dropbox
twitter
Spotify
Google

R0cky!14

R0cky!17

R0cky!17

123456

Rocky!16

R0ckyStar

R0ckyBox

R0cky!17

R0cky!17

AcmeCo

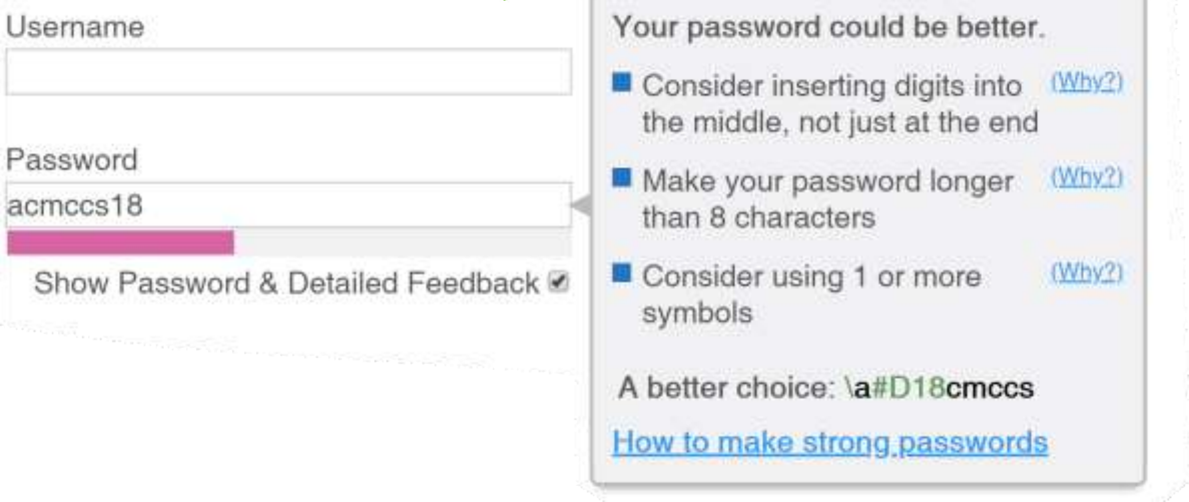
Memory-Hard Hash Function ✓

Email	Argon2i Hash of Password
…	…
jim@mail.com	$argon2i$v=19$m=4096,…
…	…

Rate-Limiting Guessing ✓

□ I'm not a robot

Password Strength Meter ✓


Username

Password
acmccs18

Show Password & Detailed Feedback ☑

Your password could be better.

- Consider inserting digits into the middle, not just at the end (Why?)
- Make your password longer than 8 characters (Why?)
- Consider using 1 or more symbols (Why?)

A better choice: \a#D18cmccs

How to make strong passwords

AcmeCo

Email
…
jim@mail.com
…

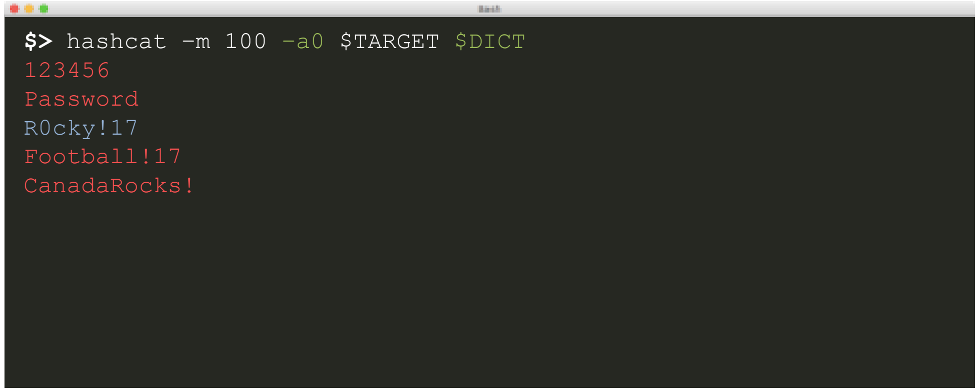
LinkedIn

Email
jane@aol.com
jessey@gmx.net
jenny@gmail.com
jim@mail.com
john@hotmail.com
…

LinkedIn

Email	SHA-1 Hash of Password
jane@aol.com	7c4a8d09ca3762af61e595209
jessey@gmx.net	5baa61e4c9b93f3f0682250b6
jenny@gmail.com	7c222fb2927d828af22f59213
jim@mail.com	ba93664a90285b9ff18a7a081
john@hotmail.com	b1b3773a05c0ed0176787a4f1
...	...

Crack All The Things!



```
$> hashcat -m 100 -a0 $TARGET $DICT
123456
Password
R0cky!17
Football!17
CanadaRocks!
```

LinkedIn

Email	Cracked SHA-1 Hashes
jane@aol.com	123456
jessey@gmx.net	5baa61e4c9b93f3f0682250b6
jenny@gmail.com	Canada4ever
jim@mail.com	R0cky!17
john@hotmail.com	HikingGuy89
…	…

Dead On Arrival

AcmeCo

Email	Argon2i Hash of Password
…	…
jim@mail.com	`$argon2i$v=19$m=4096,…`
…	…

Dead On Arrival

AcmeCo

Email	Argon2i Hash of Password
…	…
jim@mail.com	$argon2i$v=19$m=4096,…
…	…

LinkedIn

Email	Cracked SHA-1 Hashes
jane@aol.com	123456
jessey@gmx.net	5baa61e4c9b93f3f0682250b6
jenny@gmail.com	Canada4ever
jim@mail.com	R0cky!17
john@hotmail.com	HikingGuy89
…	…

Dead On Arrival

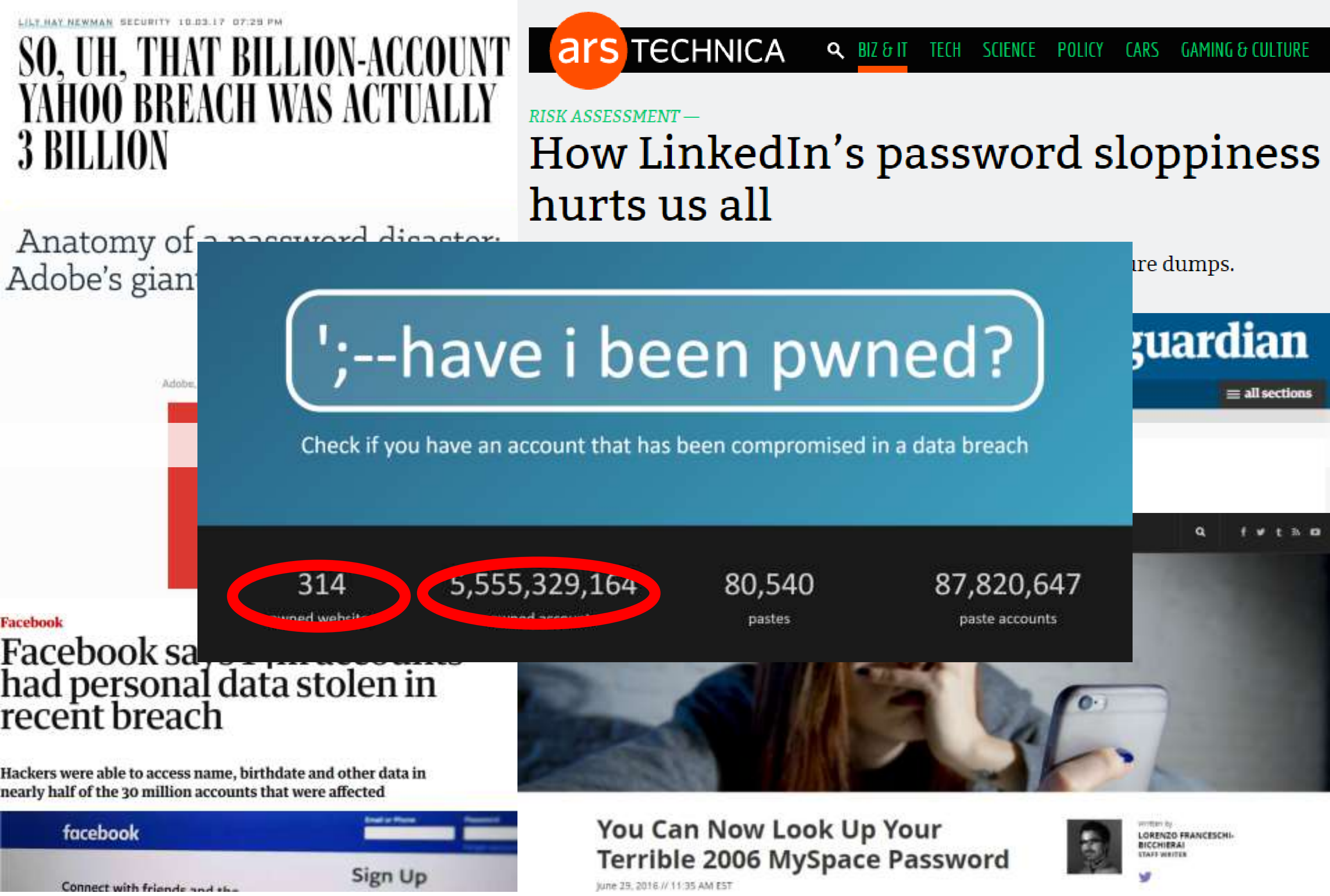
AcmeCo

Email	Cracked
...	...
jim@mail.com	R0cky!17
...	...

LinkedIn

Email	Cracked SHA-1 Hashes
jane@aol.com	123456
jessey@gmx.net	5baa61e4c9b93f3f0682250b6
jenny@gmail.com	Canada4ever
jim@mail.com	R0cky!17
john@hotmail.com	HikingGuy89
...	...

1 guess is enough!



LILY HAY NEWMAN SECURITY 10.03.17 07:29 PM

SO, UH, THAT BILLION-ACCOUNT YAHOO BREACH WAS ACTUALLY 3 BILLION

Anatomy of a password disaster: Adobe's gian

Adobe

ars TECHNICA

RISK ASSESSMENT —

How LinkedIn's password sloppiness hurts us all

ure dumps.

guardian

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

314 pwned websites

5,555,329,164 pwned accounts

80,540 pastes

87,820,647 paste accounts

Facebook

Facebook sa had personal data stolen in recent breach

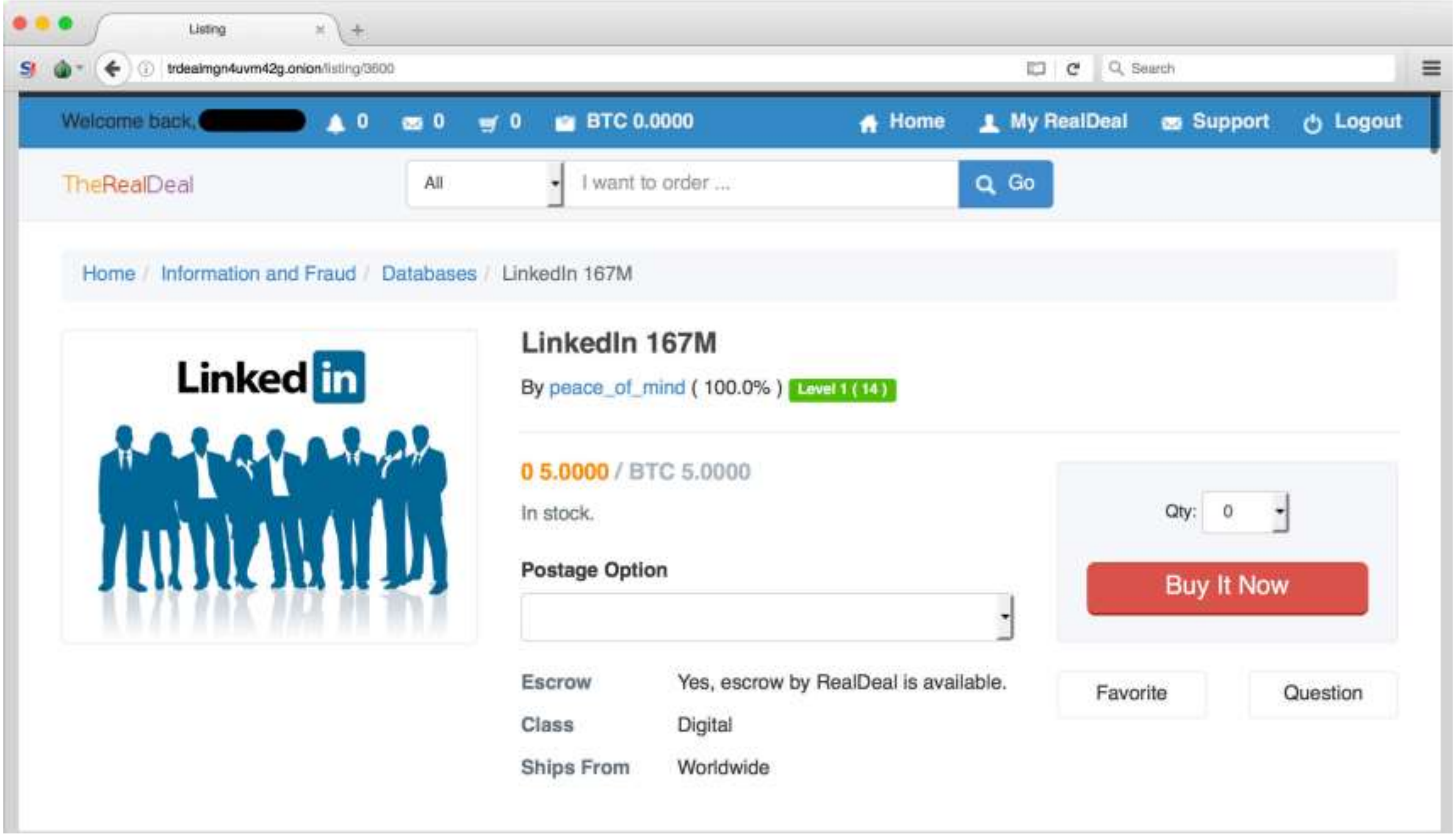
Hackers were able to access name, birthdate and other data in nearly half of the 30 million accounts that were affected

You Can Now Look Up Your Terrible 2006 MySpace Password

June 29, 2016 // 11:35 AM EST

Written by LORENZO FRANCESCHI-BICCHIERAI STAFF WRITER

Monitoring the Black Market



Home / Information and Fraud / Databases / LinkedIn 167M

LinkedIn 167M

By peace_of_mind (100.0%) Level 1 (14)

0 5.0000 / BTC 5.0000

In stock.

Postage Option

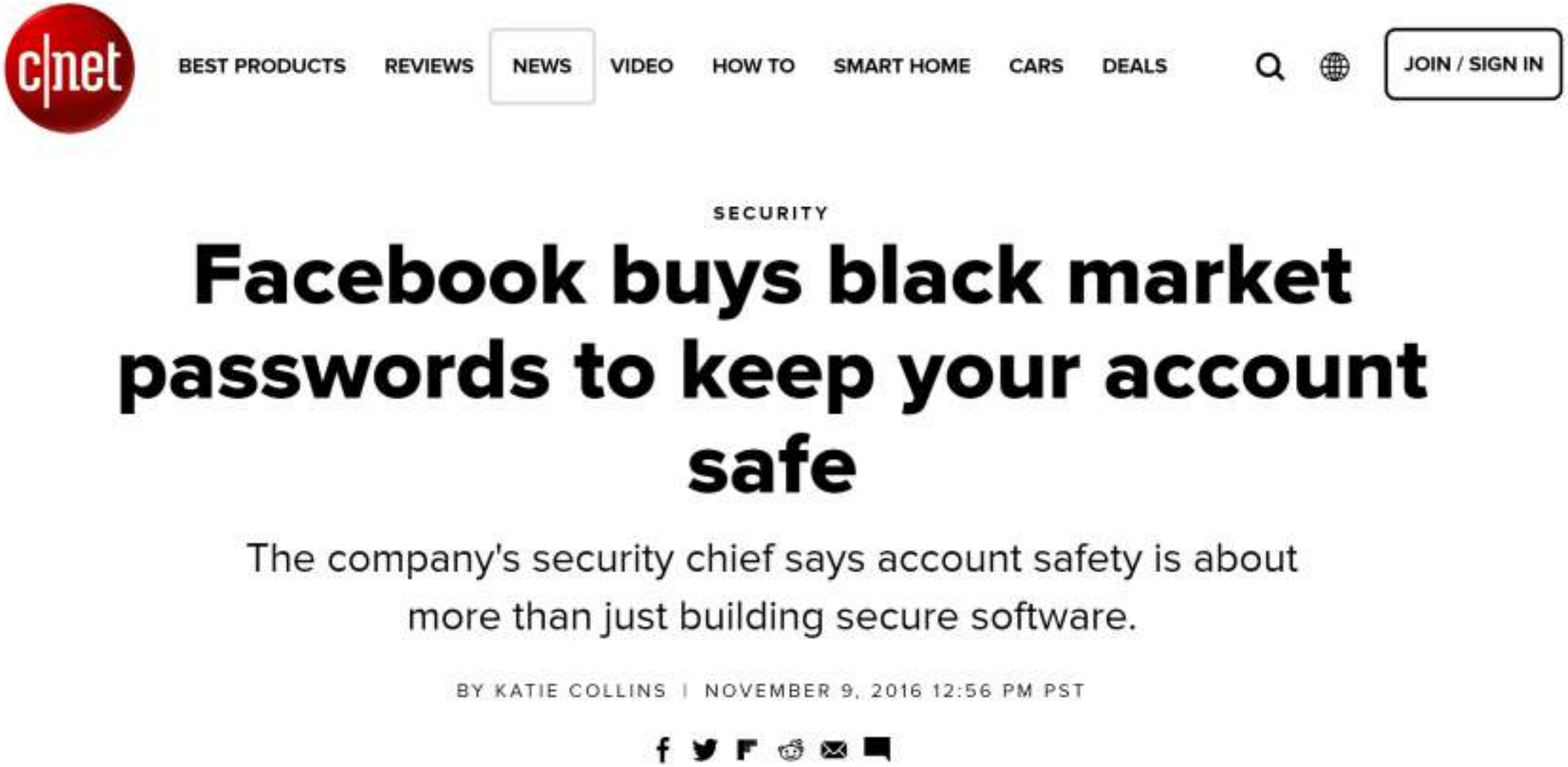
Escrow	Yes, escrow by RealDeal is available.
Class	Digital
Ships From	Worldwide

Qty: 0

Buy It Now

Favorite

Question



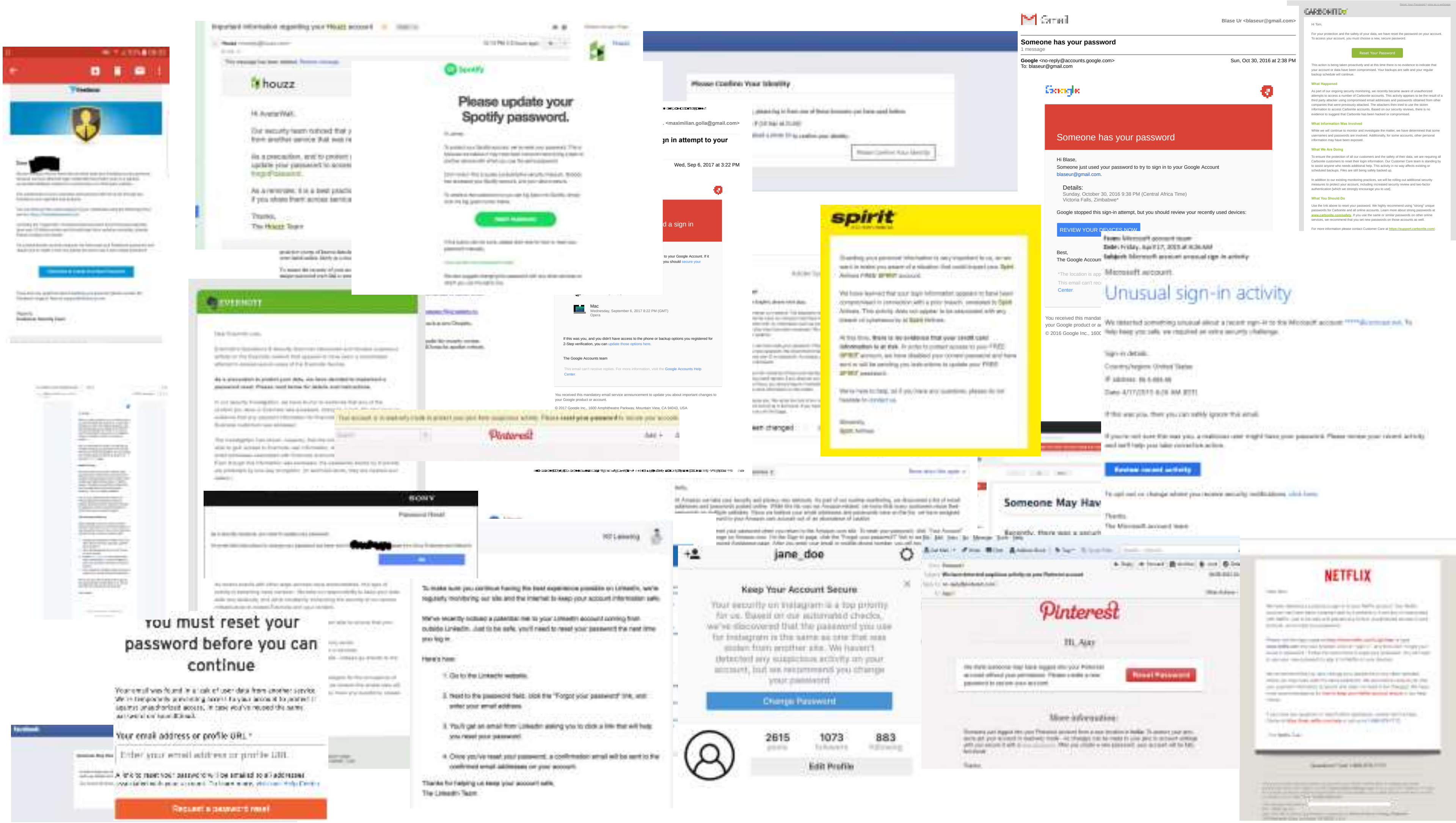
SECURITY

Facebook buys black market passwords to keep your account safe

The company's security chief says account safety is about more than just building secure software.

BY KATIE COLLINS | NOVEMBER 9, 2016 12:56 PM PST

Password-Reuse Notifications



Important information regarding your Houzz account

houzz

Hi AvatarWalt,

Thanks,
The Houzz Team

Spotify

Please update your Spotify password.

Please Confirm Your Identity

Dear [redacted]

Someone has your password
1 message

Google <no-reply@accounts.google.com>
To: blaseur@gmail.com

Sun, Oct 30, 2016 at 2:38 PM

Blase Ur <blaseur@gmail.com>

Someone has your password

Hi Blase,
Someone just used your password to try to sign in to your Google Account blaseur@gmail.com.

Details:
Sunday, October 30, 2016 9:38 PM (Central Africa Time)
Victoria Falls, Zimbabwe*

Google stopped this sign-in attempt, but you should review your recently used devices:

REVIEW YOUR DEVICES NOW

Best,
The Google Account

*The location is app

This email can't rec

Center.

You received this mandat
your Google product or ac
© 2016 Google Inc., 1600

<maximilian.golla@gmail.com>

n attempt to your

Wed, Sep 6, 2017 at 3:22 PM

The Google Accounts team

You received this mandatory email service announcement to update you about important changes to your Google product or account.

© 2017 Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

CARBONITE

Hi Tom,

What Happened

What Information Was Involved

What We Are Doing

In addition to our existing monitoring practices, we will be rolling out additional security measures to protect your account, including increased security review and two-factor authentication [which we strongly encourage you to use].

What You Should Do

Use the link above to reset your password. We highly recommend using "strong" unique passwords for Carbonite and all online accounts. Learn more about strong passwords at www.carbonite.com/safety. If you use the same or similar passwords on other online services, we recommend that you set new passwords on those accounts as well.

For more information please contact Customer Care at https://support.carbonite.com/.

EVERNOTE

spirit

Pinterest

SONY

Password Reset

Microsoft account

Unusual sign-in activity

Review recent activity

Someone May Hav

You must reset your password before you can continue

Your email address or profile URL *

Enter your email address or profile URL

Request a password reset

facebook

To make sure you continue having the best experience possible on LinkedIn, we're regularly monitoring our site and the internet to keep your account information safe.

We've recently noticed a potential risk to your LinkedIn account coming from outside LinkedIn. Just to be safe, you'll need to reset your password the next time you log in.

Here's how:

1. Go to the LinkedIn website.
2. Next to the password field, click the "Forgot your password" link, and enter your email address.
3. You'll get an email from LinkedIn asking you to click a link that will help you reset your password.
4. Once you've reset your password, a confirmation email will be sent to the confirmed email addresses on your account.

Thanks for helping us keep your account safe.
The LinkedIn Team

jane_doe

Keep Your Account Secure

Your security on Instagram is a top priority for us. Based on our automated checks, we've discovered that the password you use for Instagram is the same as one that was stolen from another site. We haven't detected any suspicious activity on your account, but we recommend you change your password.

Change Password

2615 posts | 1073 followers | 883 following

Edit Profile

Pinterest

Hi, Ajay

Reset Password

More information

NETFLIX

Notification Goals

timely

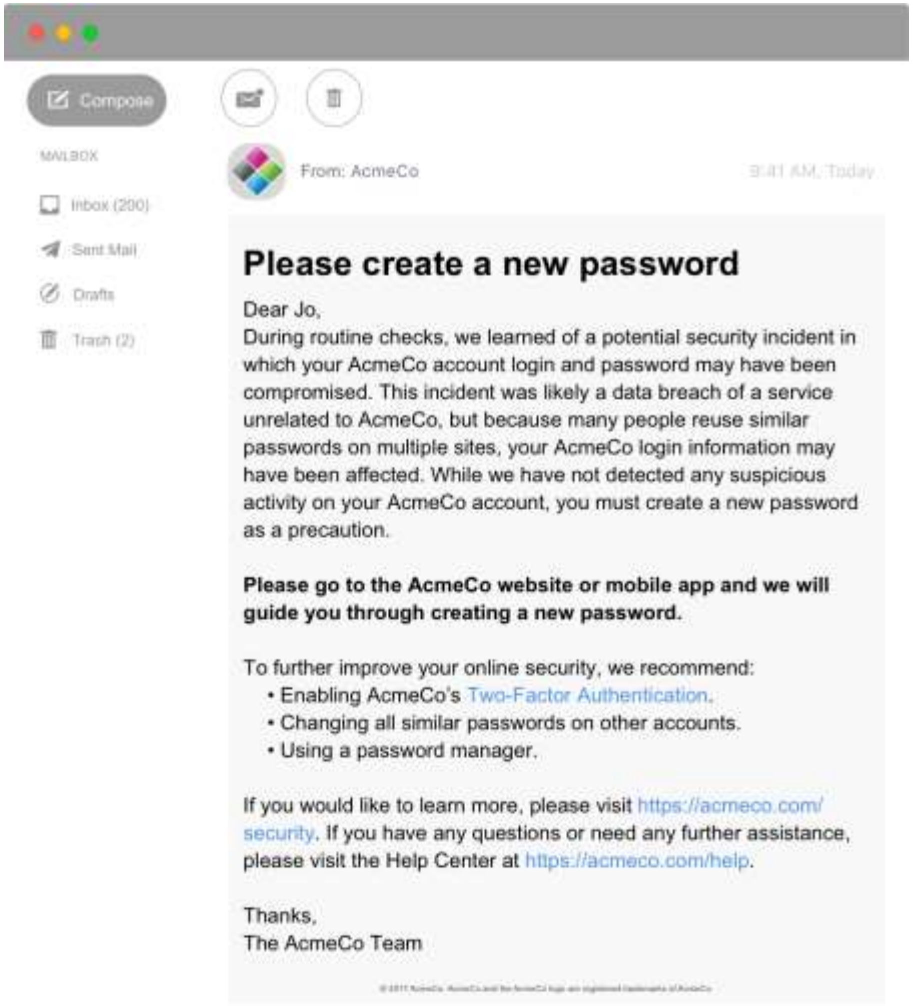
sufficient background

secure actions

legitimate

trust

Our Model Password-Reuse Notification



From: AcmeCo

9:41 AM, Today

Please create a new password

Dear Jo,
During routine checks, we learned of a potential security incident in which your AcmeCo account login and password may have been compromised. This incident was likely a data breach of a service unrelated to AcmeCo, but because many people reuse similar passwords on multiple sites, your AcmeCo login information may have been affected. While we have not detected any suspicious activity on your AcmeCo account, you must create a new password as a precaution.

Please go to the AcmeCo website or mobile app and we will guide you through creating a new password.

To further improve your online security, we recommend:

- Enabling AcmeCo's Two-Factor Authentication.
- Changing all similar passwords on other accounts.
- Using a password manager.

If you would like to learn more, please visit https://acmeco.com/security. If you have any questions or need any further assistance, please visit the Help Center at https://acmeco.com/help.

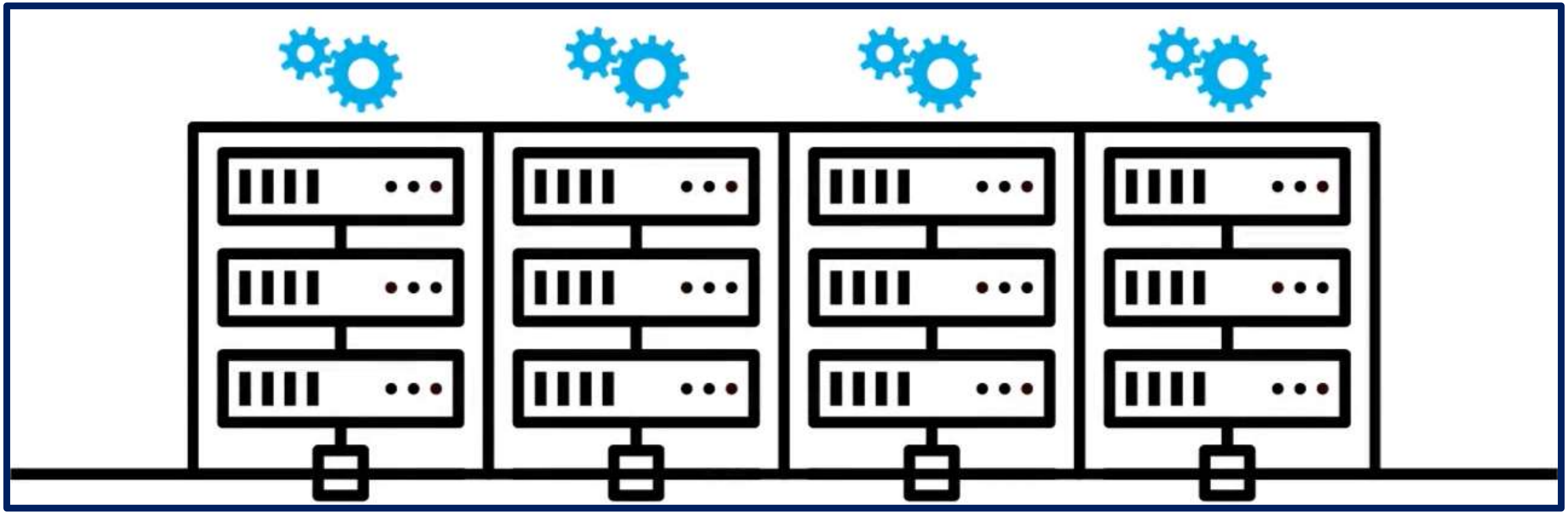
Thanks,
The AcmeCo Team

Understanding Users' Password Behaviors

Some Ways to Understand Users

- Retrospective analysis of user-created passwords rockyou
- Large-scale online studies
- Examine real passwords
- Qualitative studies

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

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

Approach

```
password
iloveyou
teamo123
…
```

```
Pa$$w0rd
iLov3you!
1QaZ2W@x
…
```

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

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

4 password sets

✖

5 password-cracking approaches

Four Password Sets

Four Password Sets

- **Basic** (3,062): 8+ characters

```
password
```

Four Password Sets

- **Basic** (3,062): 8+ characters

`password`

- Complex (3,000): 8+ characters, 4 classes

`Pa$$w0rd`

Four Password Sets

- **Basic** (3,062): 8+ characters

`password`

- Complex (3,000): 8+ characters, 4 classes

`Pa$$w0rd`

- LongBasic (2,054): 16+ characters

`passwordpassword`

Four Password Sets

- **Basic** (3,062): 8+ characters

`password`

- **Complex** (3,000): 8+ characters, 4 classes

`Pa$$w0rd`

- **LongBasic** (2,054): 16+ characters

`passwordpassword`

- **LongComplex** (990): 12+ characters, 3+ classes

`pa$$word1234`

Five Cracking Approaches

- John the Ripper
- Hashcat
- Markov models
- Probabilistic Context-Free Grammar
- Professionals

John the Ripper

- Guesses variants of input wordlist

John the Ripper

- Guesses variants of input wordlist
- Wordlist mode requires:
  - Wordlist (passwords and dictionary entries)
  - Mangling rules

John the Ripper

- Guesses variants of input wordlist
- Wordlist mode requires:
  - Wordlist (passwords and dictionary entries)
  - Mangling rules
- Speed: Fast

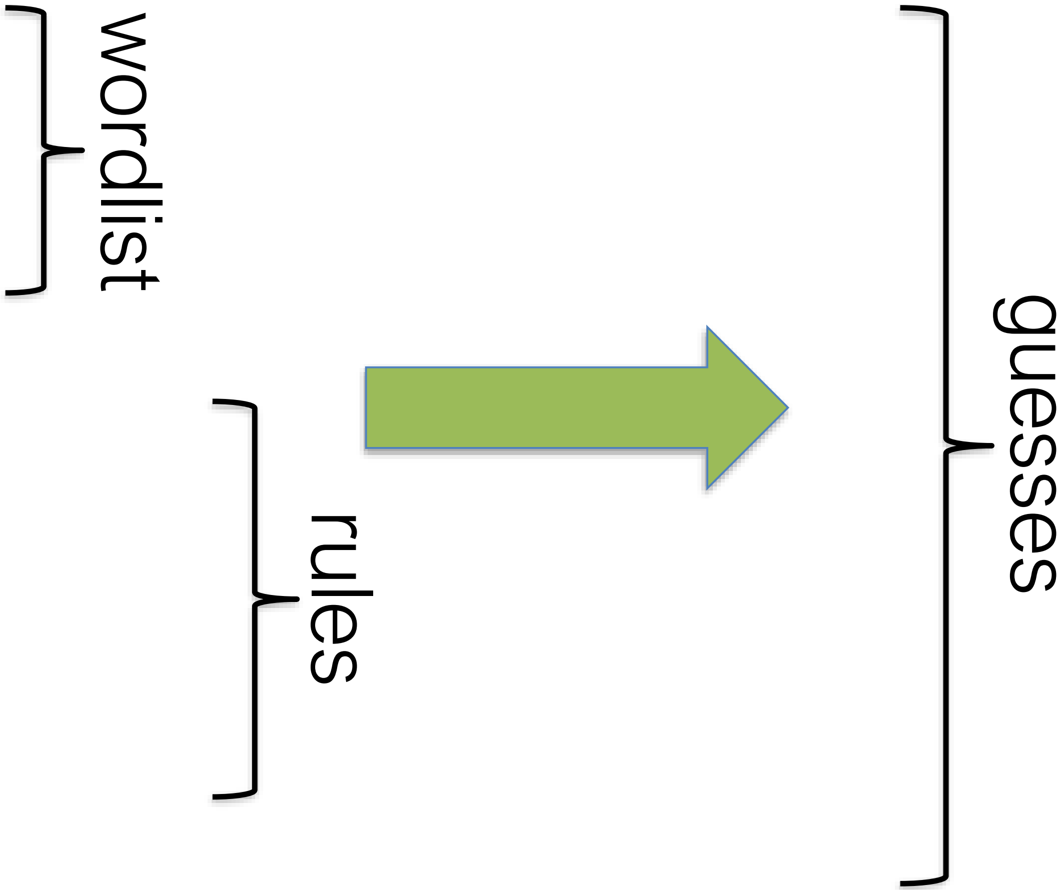
John the Ripper

- Guesses variants of input wordlist
- Wordlist mode requires:
  - Wordlist (passwords and dictionary entries)
  - Mangling rules
- Speed: Fast
  - 10^{13} guesses

John the Ripper

- Guesses variants of input wordlist
- Wordlist mode requires:
  - Wordlist (passwords and dictionary entries)
  - Mangling rules
- Speed: Fast
  - 10^{13} guesses
- “JTR”

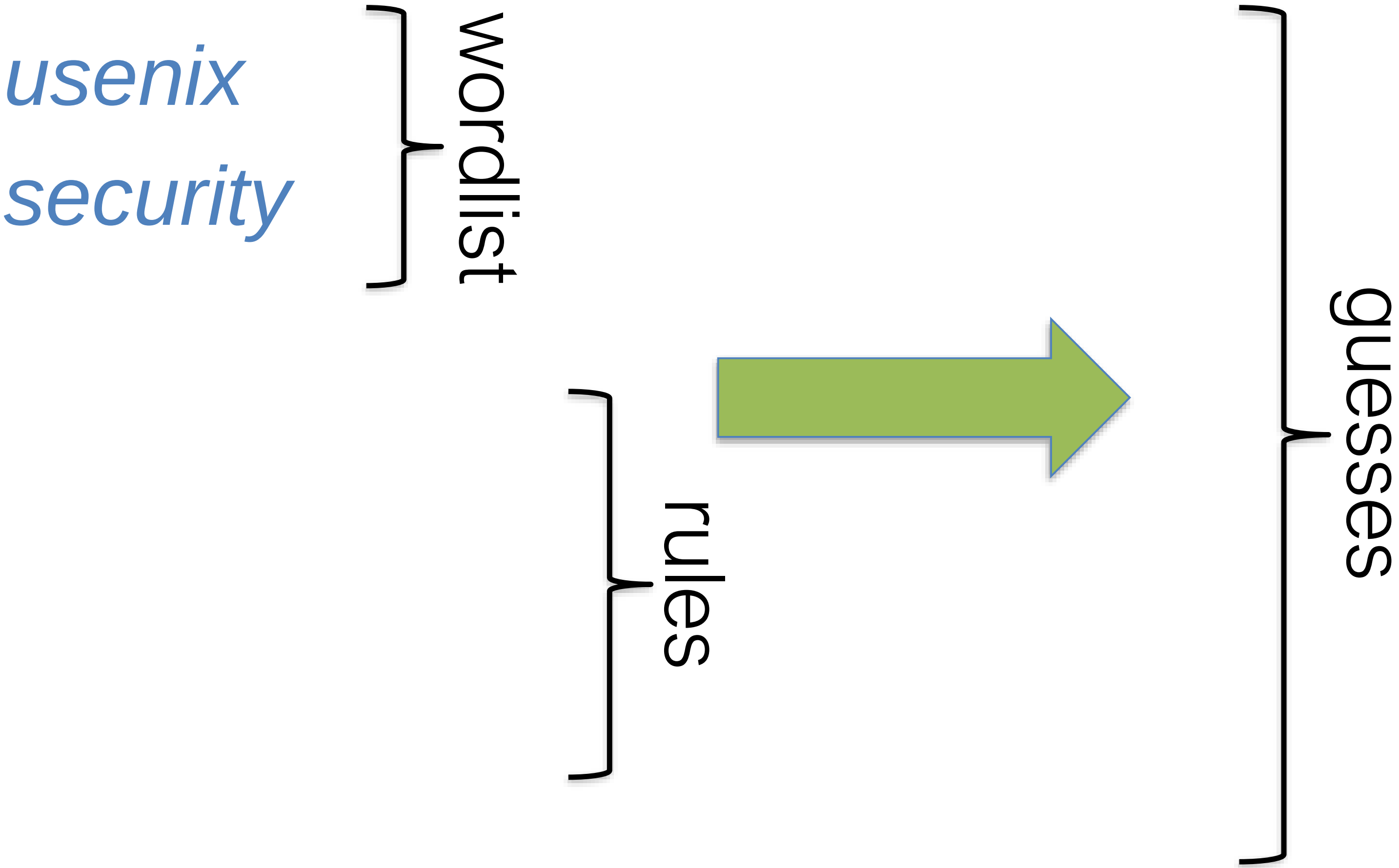
John the Ripper


wordlist

rules

guesses

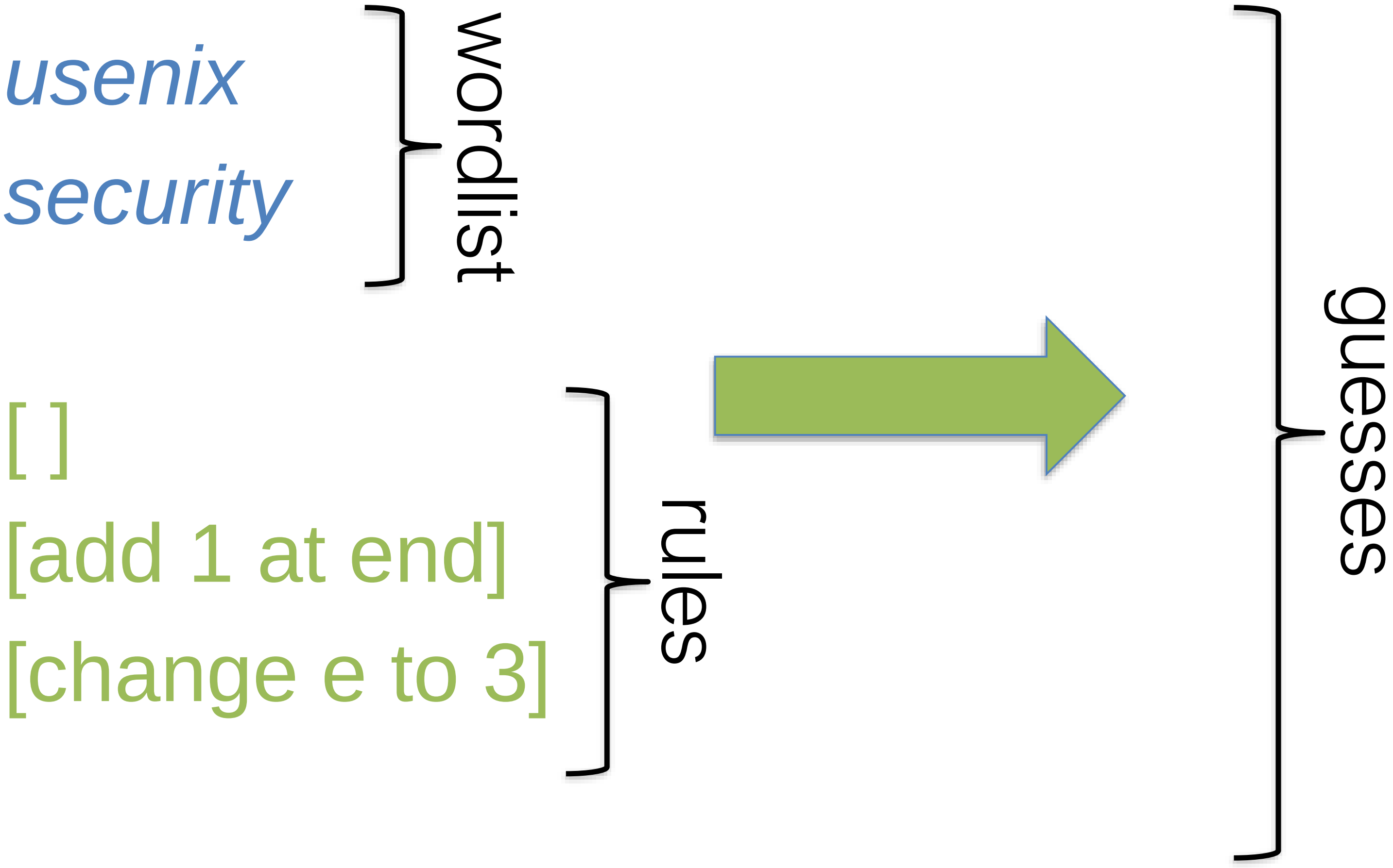
John the Ripper



usenix

security

John the Ripper



usenix

security

[ ]

[add 1 at end]

[change e to 3]

John the Ripper

usenix

security

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

usenix

security

usenix1

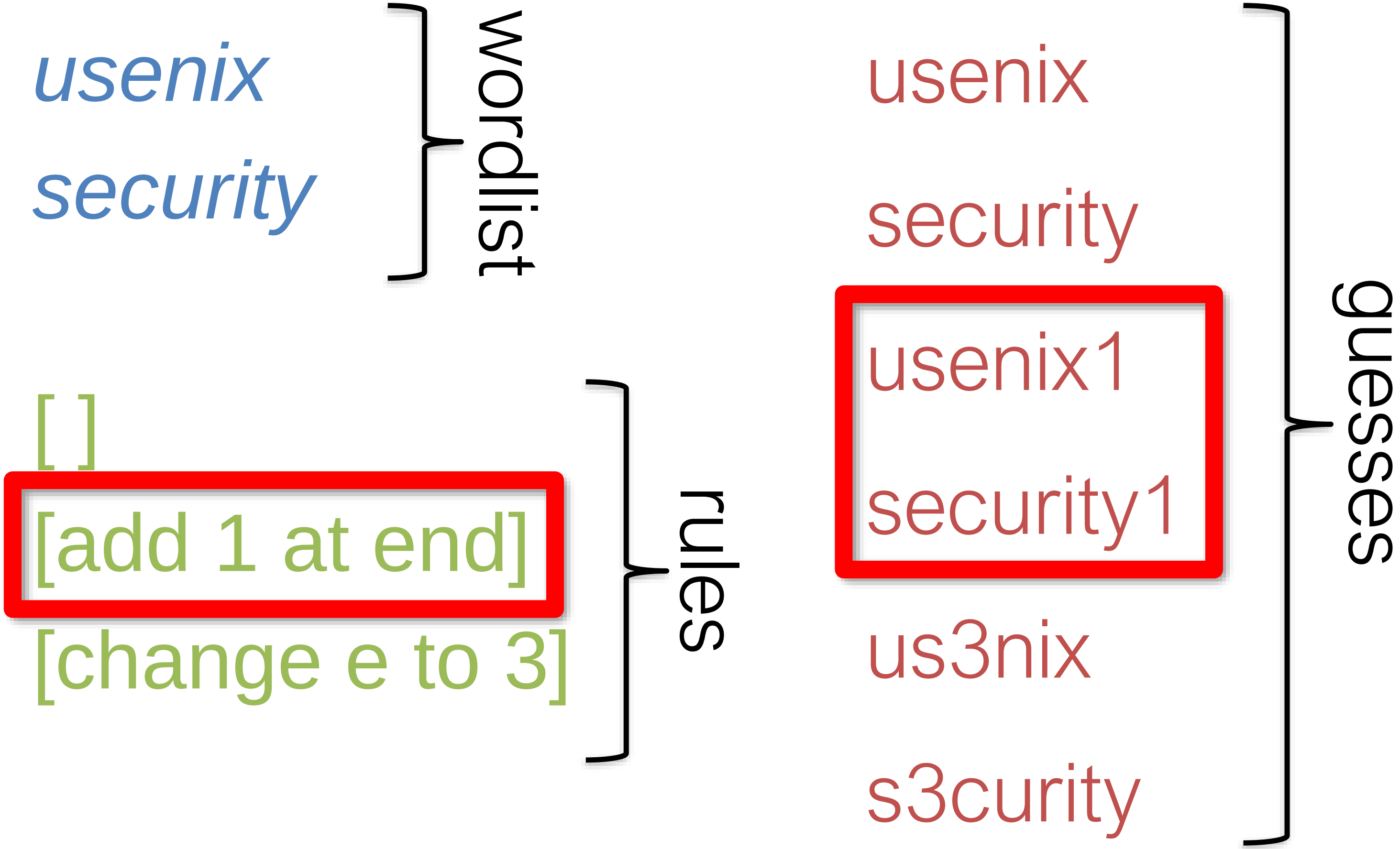
security1

us3nix

s3curity

guesses

John the Ripper



usenix

security

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

usenix

security

usenix1

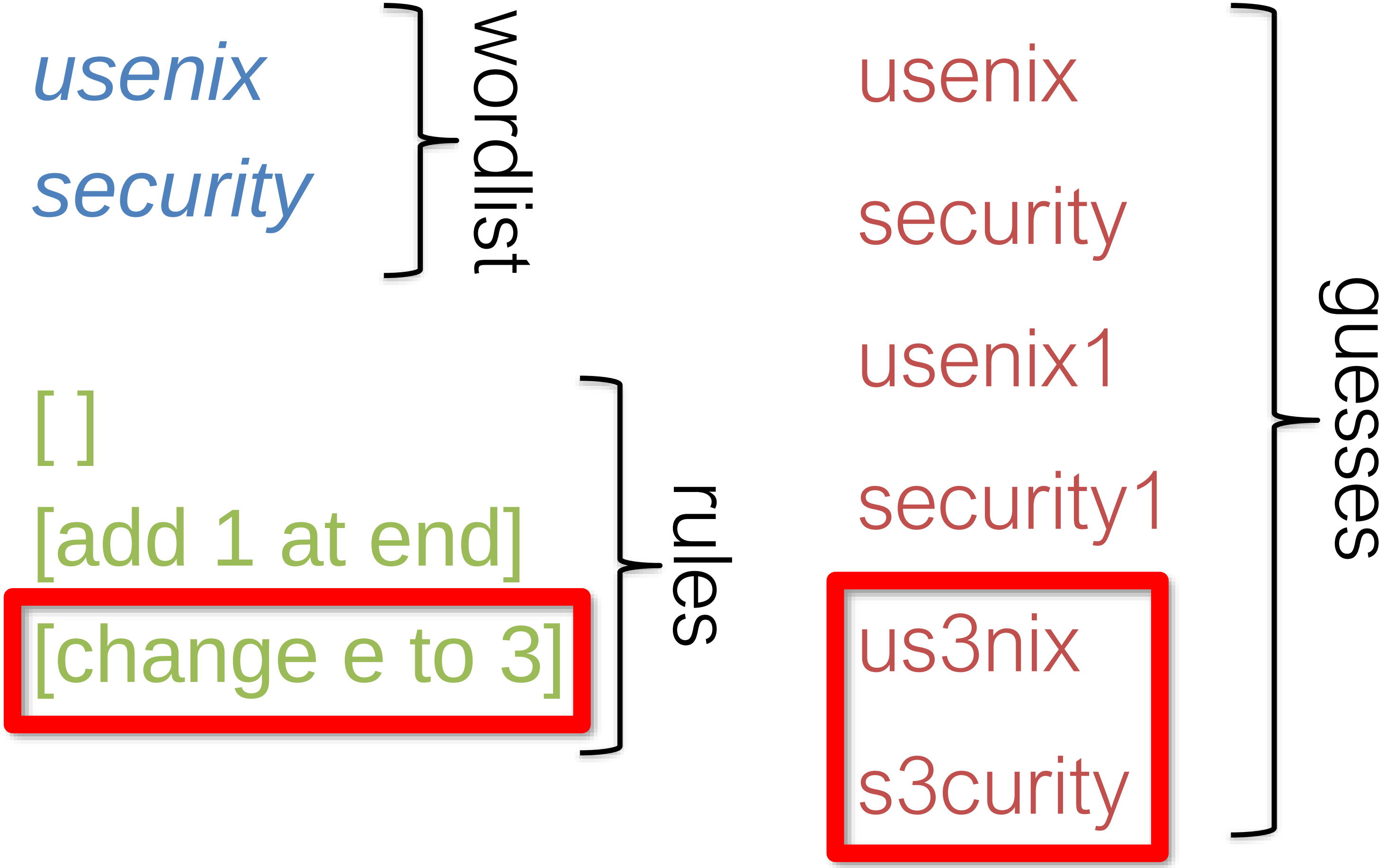
security1

us3nix

s3curity

guesses

John the Ripper



usenix

security

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

usenix

security

usenix1

security1

us3nix

s3curity

guesses

Hashcat

- Guesses variants of input wordlist

Hashcat

- Guesses variants of input wordlist
- Wordlist mode requires:
  - Wordlist (passwords and dictionary entries)
  - Mangling rules

Hashcat

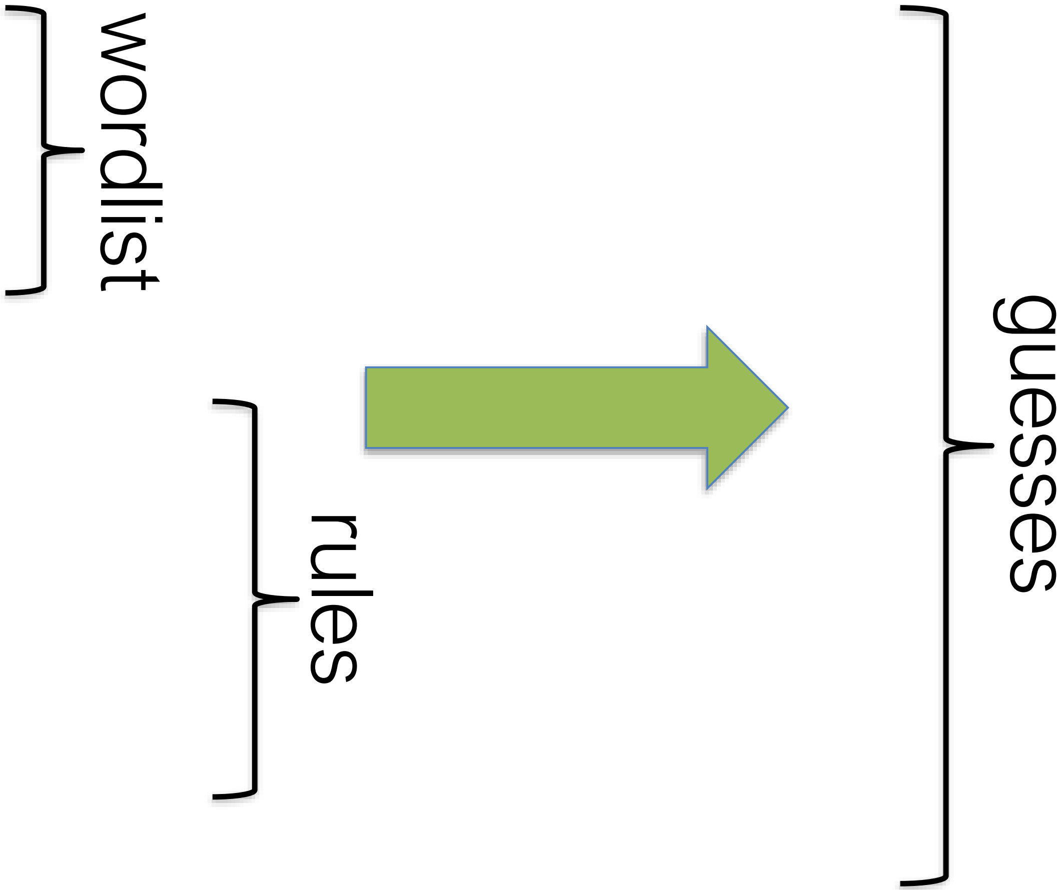
- Guesses variants of input wordlist
- Wordlist mode requires:
  - Wordlist (passwords and dictionary entries)
  - Mangling rules
- Speed: Fast

Hashcat

- Guesses variants of input wordlist
- Wordlist mode requires:
  - Wordlist (passwords and dictionary entries)
  - Mangling rules
- Speed: Fast
  - 10^{13} guesses

Hashcat

hashcat
advanced
password
recovery



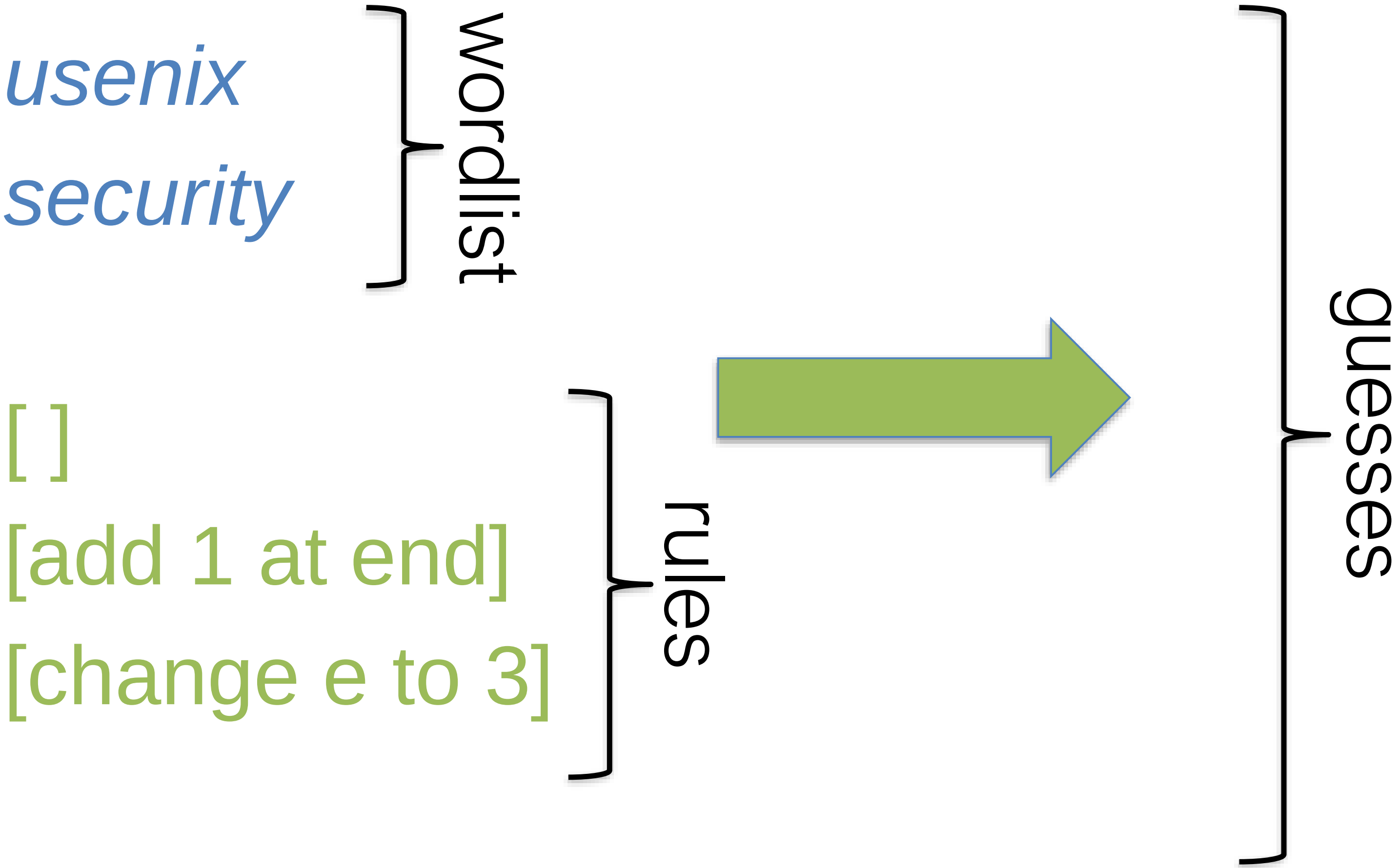
wordlist

rules

guesses

Hashcat

hashcat
advanced
password
recovery



usenix

security

wordlist

[ ]

[add 1 at end]

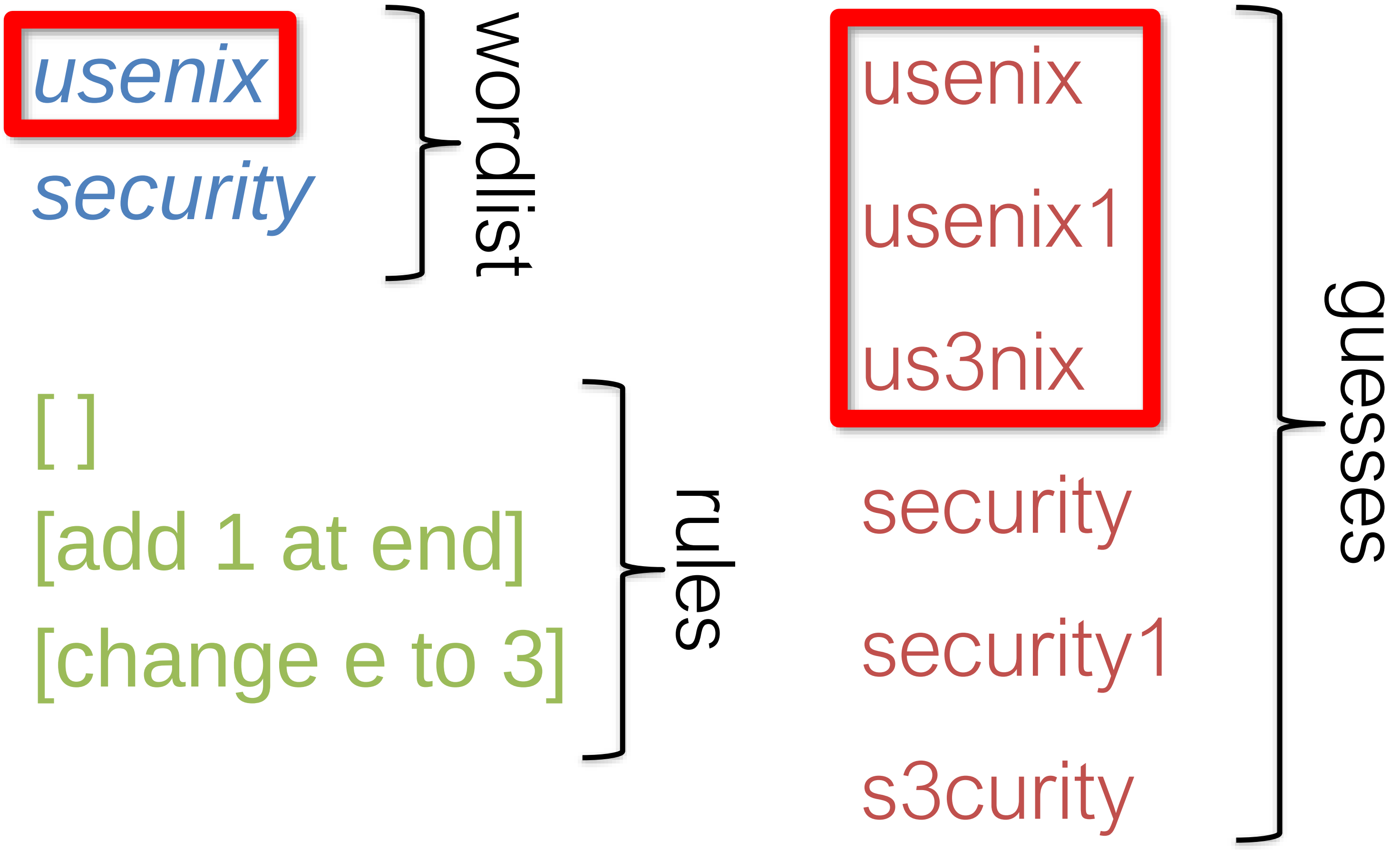
[change e to 3]

rules

guesses

Hashcat

hashcat
advanced
password
recovery



usenix
security

wordlist

[ ]
[add 1 at end]
[change e to 3]

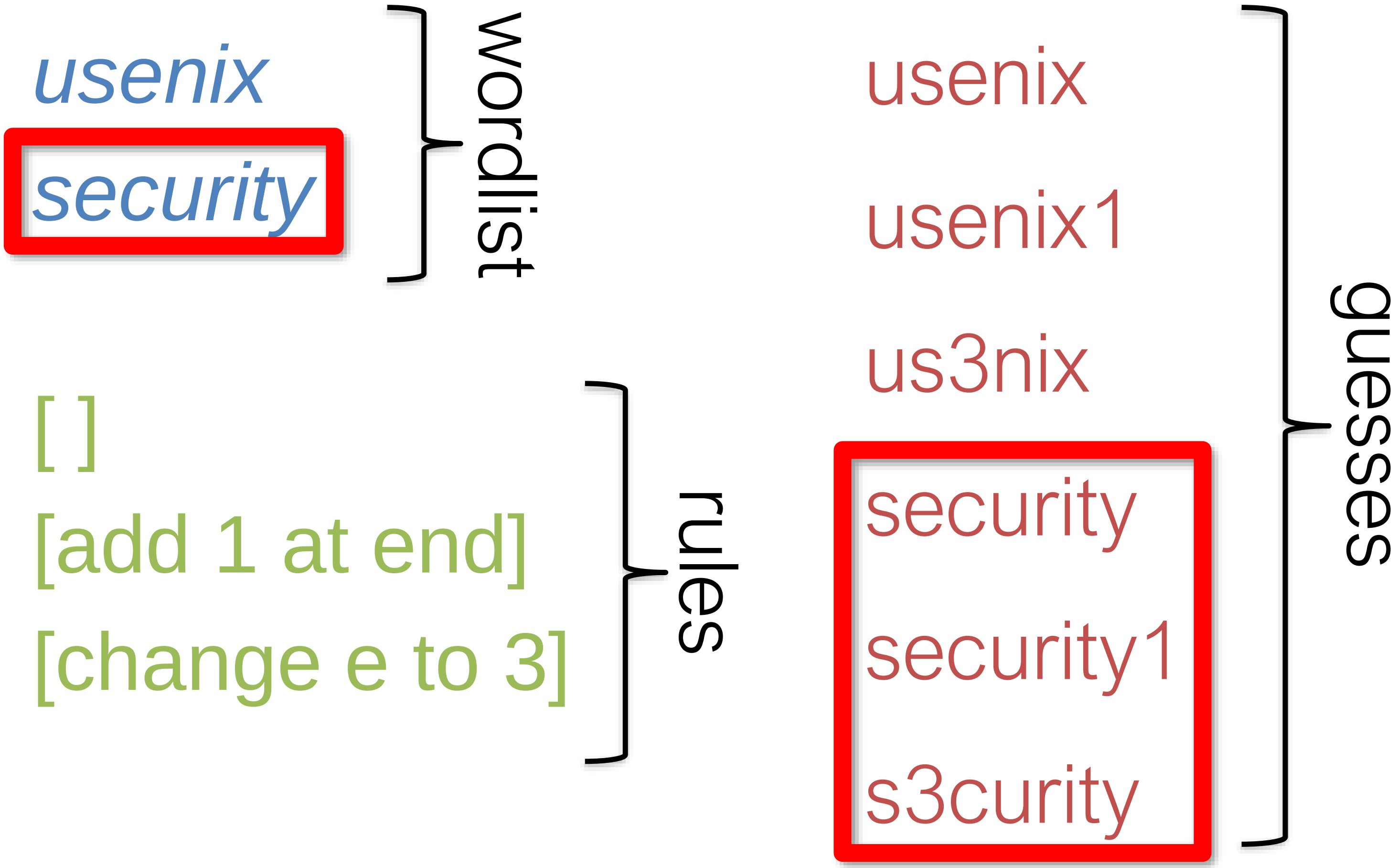
rules

usenix
usenix1
us3nix
security
security1
s3curity

guesses

Hashcat

hashcat
advanced
password
recovery



usenix

security

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

usenix

usenix1

us3nix

security

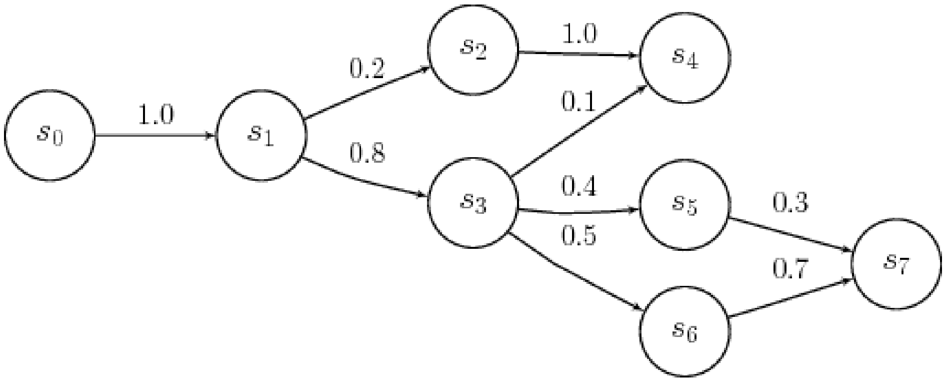
security1

s3curity

guesses

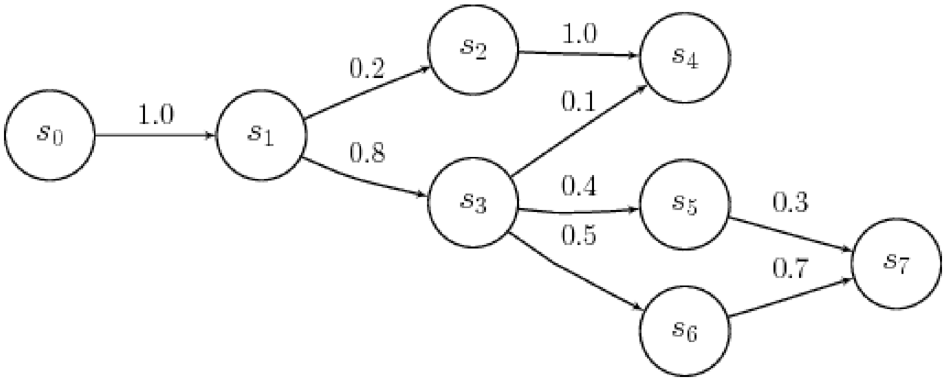
Markov Models

- Predicts future characters from previous



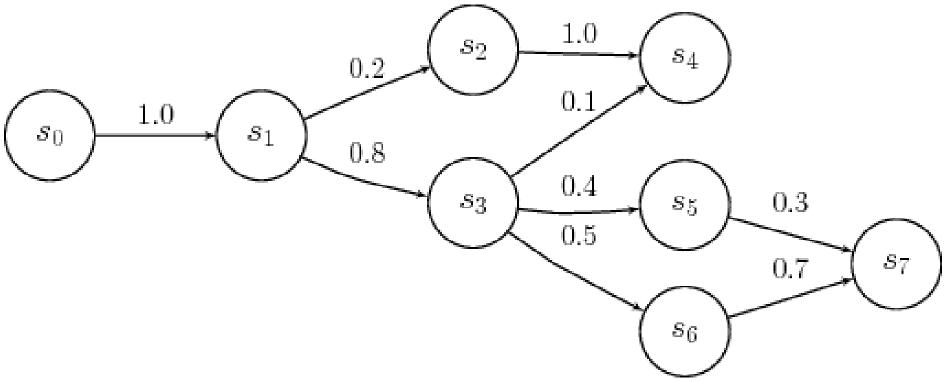
Markov Models

- Predicts future characters from previous
- Approach requires weighted data:
  - Passwords
  - Dictionaries



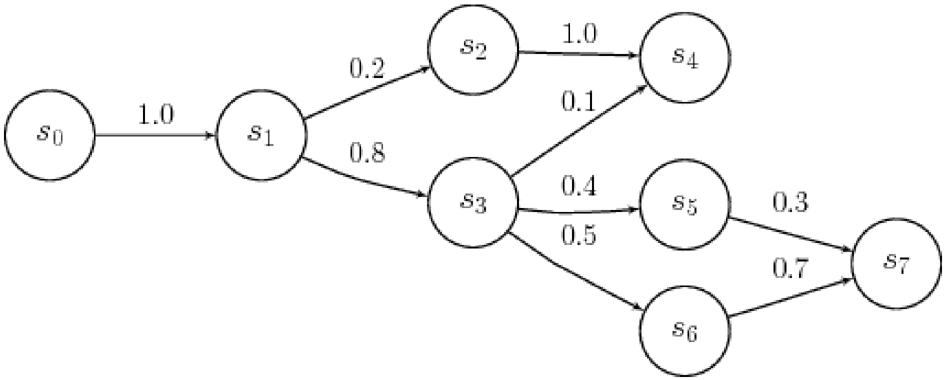
Markov Models

- Predicts future characters from previous
- Approach requires weighted data:
  - Passwords
  - Dictionaries
- Ma et al. IEEE S&P 2014



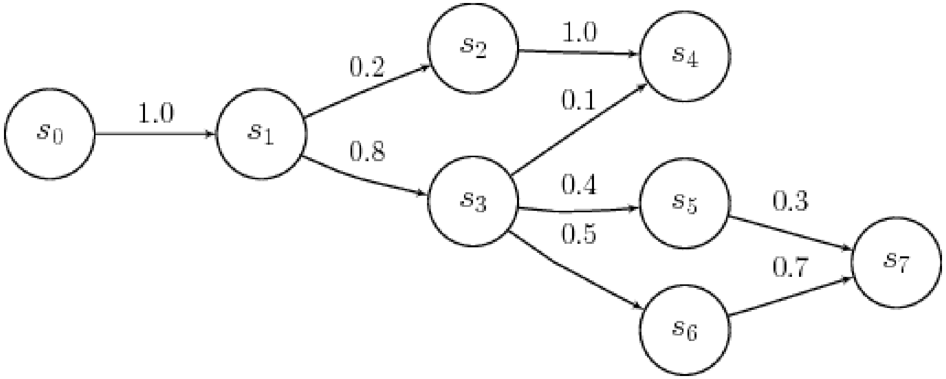
Markov Models

- Predicts future characters from previous
- Approach requires weighted data:
  - Passwords
  - Dictionaries
- Ma et al. IEEE S&P 2014
- Speed: Slow

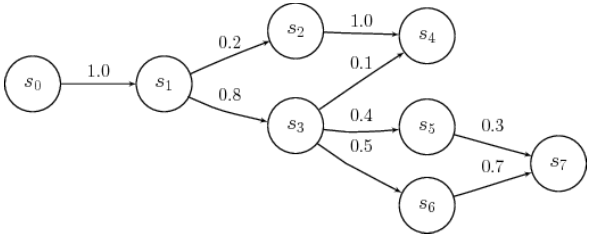


Markov Models

- Predicts future characters from previous
- Approach requires weighted data:
  - Passwords
  - Dictionaries
- Ma et al. IEEE S&P 2014
- Speed: Slow
  - 10^{10} guesses

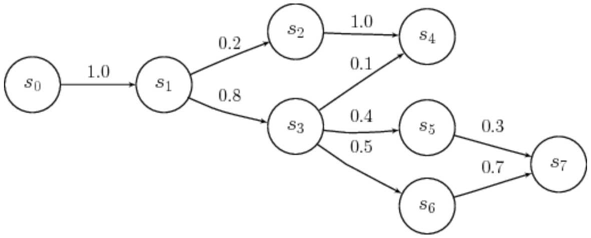


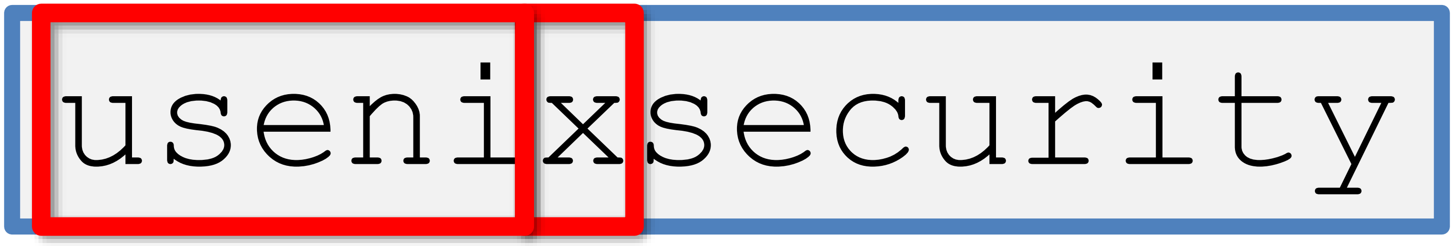
Markov Models



`usenixsecurity`

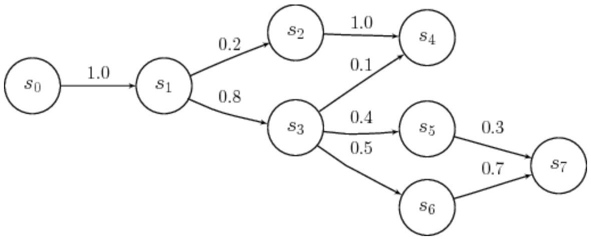
Markov Models

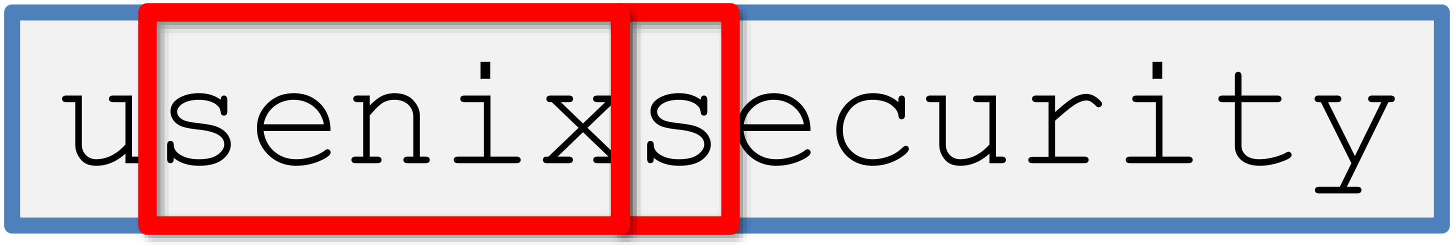




usenixsecurity

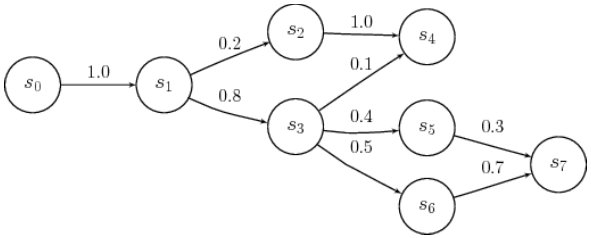
Markov Models

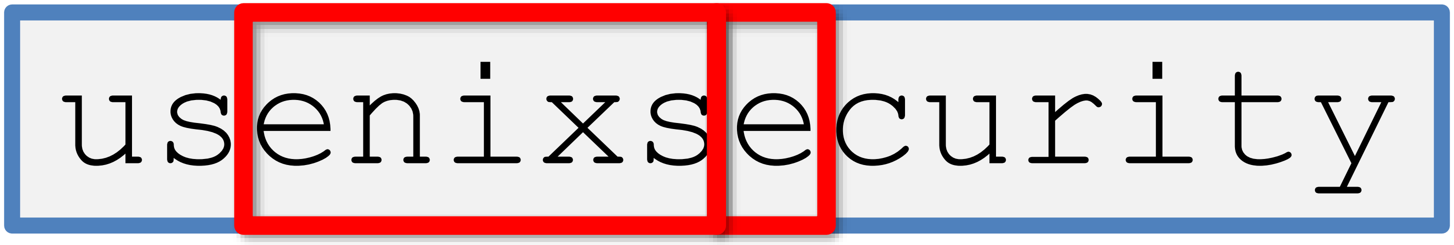




usenixsecurity

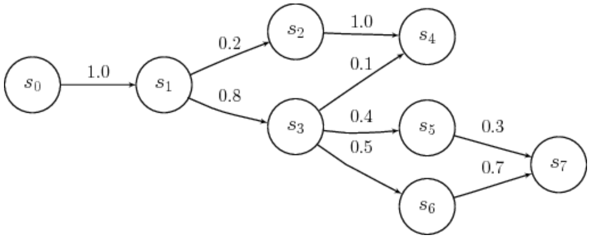
Markov Models

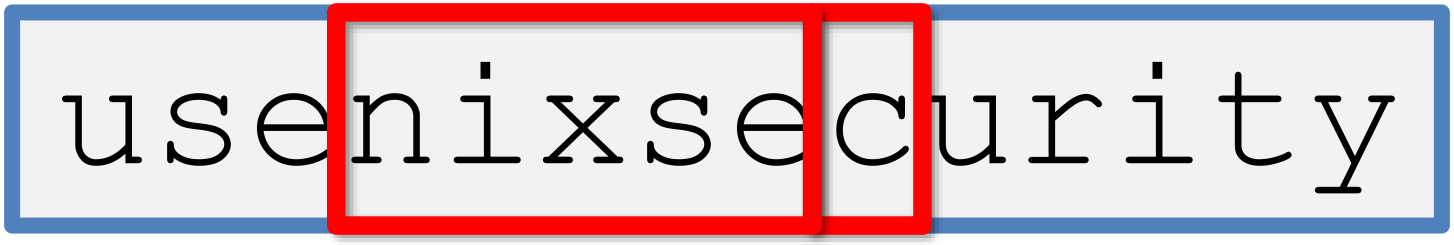




usenixsecurity

Markov Models

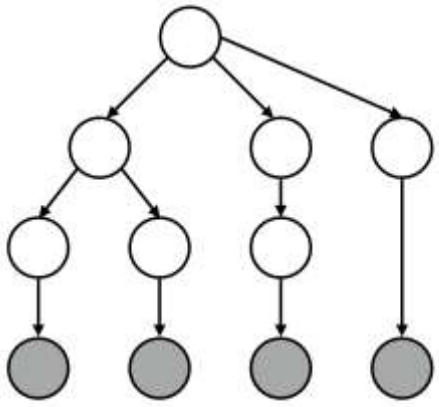




usenixsecurity

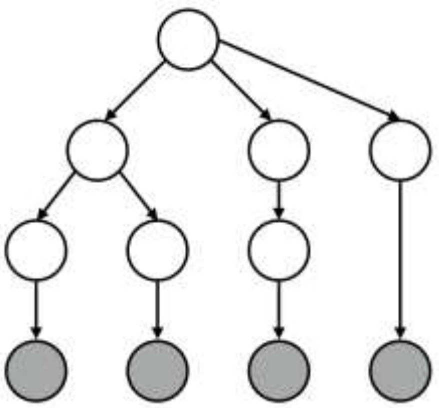
Probabilistic Context-Free Grammar

- Generate password grammar
  - Structures
  - Terminals



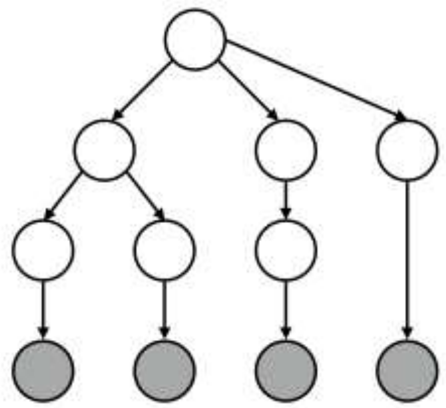
Probabilistic Context-Free Grammar

- Generate password grammar
  - Structures
  - Terminals
- Kelley et al. IEEE S&P 2012
  - Based on Weir et al. IEEE S&P 2009



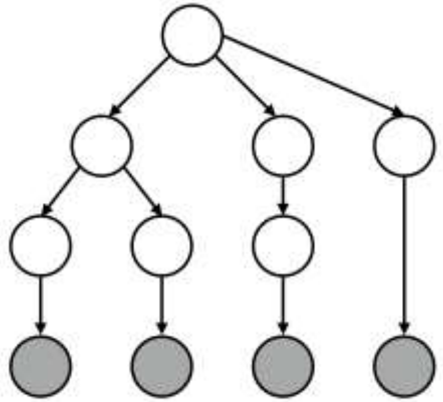
Probabilistic Context-Free Grammar

- Generate password grammar
  - Structures
  - Terminals
- Kelley et al. IEEE S&P 2012
  - Based on Weir et al. IEEE S&P 2009
- Speed: ~~Slow~~ Medium



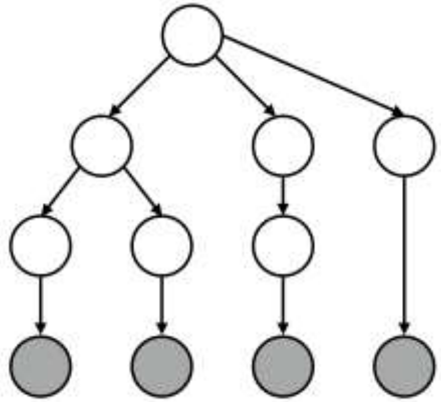
Probabilistic Context-Free Grammar

- Generate password grammar
  - Structures
  - Terminals
- Kelley et al. IEEE S&P 2012
  - Based on Weir et al. IEEE S&P 2009
- Speed: ~~Slow~~ Medium
  - 10^{14} guesses

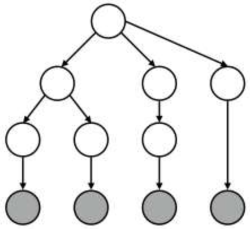


Probabilistic Context-Free Grammar

- Generate password grammar
  - – Structures
  - – Terminals
- Kelley et al. IEEE S&P 2012
  - – Based on Weir et al. IEEE S&P 2009
- Speed: ~~Slow~~ Medium
  - – 10^{14} guesses
- “PCFG”



PCFG



passwordpassword

password123

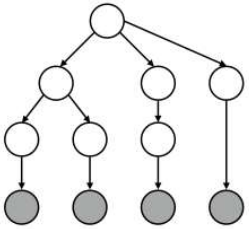
usenix3

5ecurity

iloveyou

nirvana123

PCFG



passwordpassword

password123

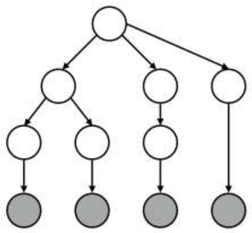
usenix3

5ecurity

iloveyou

nirvana123

PCFG



passwordpassword

password123

usenix3

5ecurity

iloveyou

nirvana123

Professionals (“Pros”)

Professionals (“Pros”)

- Contracted KoreLogic
  - – Password audits for Fortune 500 companies
  - – Run DEF CON “Crack Me If You Can”

Professionals (“Pros”)

- Contracted KoreLogic
  - – Password audits for Fortune 500 companies
  - – Run DEF CON “Crack Me If You Can”
- Proprietary wordlists and configurations

Professionals (“Pros”)

- Contracted KoreLogic
  - Password audits for Fortune 500 companies
  - Run DEF CON “Crack Me If You Can”
- Proprietary wordlists and configurations
  - 10^{14} guesses

Professionals (“Pros”)

- Contracted KoreLogic
  - – Password audits for Fortune 500 companies
  - – Run DEF CON “Crack Me If You Can”
- Proprietary wordlists and configurations
  - – 10^{14} guesses
  - – Manually tuned, updated

Approach

4 password sets ✖ 5 approaches

```
password
iloveyou
teamo123
…
```

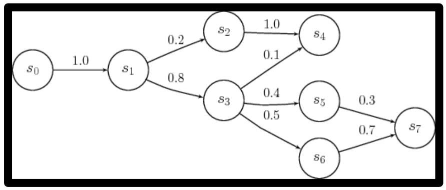
```
passwordpassword
1234567812345678
!1@2#3$4%5^6&7*8
…
```

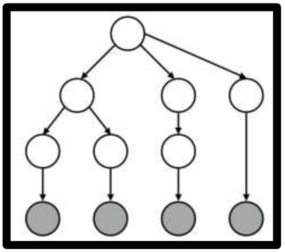
```
Pa$$w0rd
iLov3you!
1QaZ2W@x
…
```

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

John the Ripper

hashcat
advanced
password
recovery



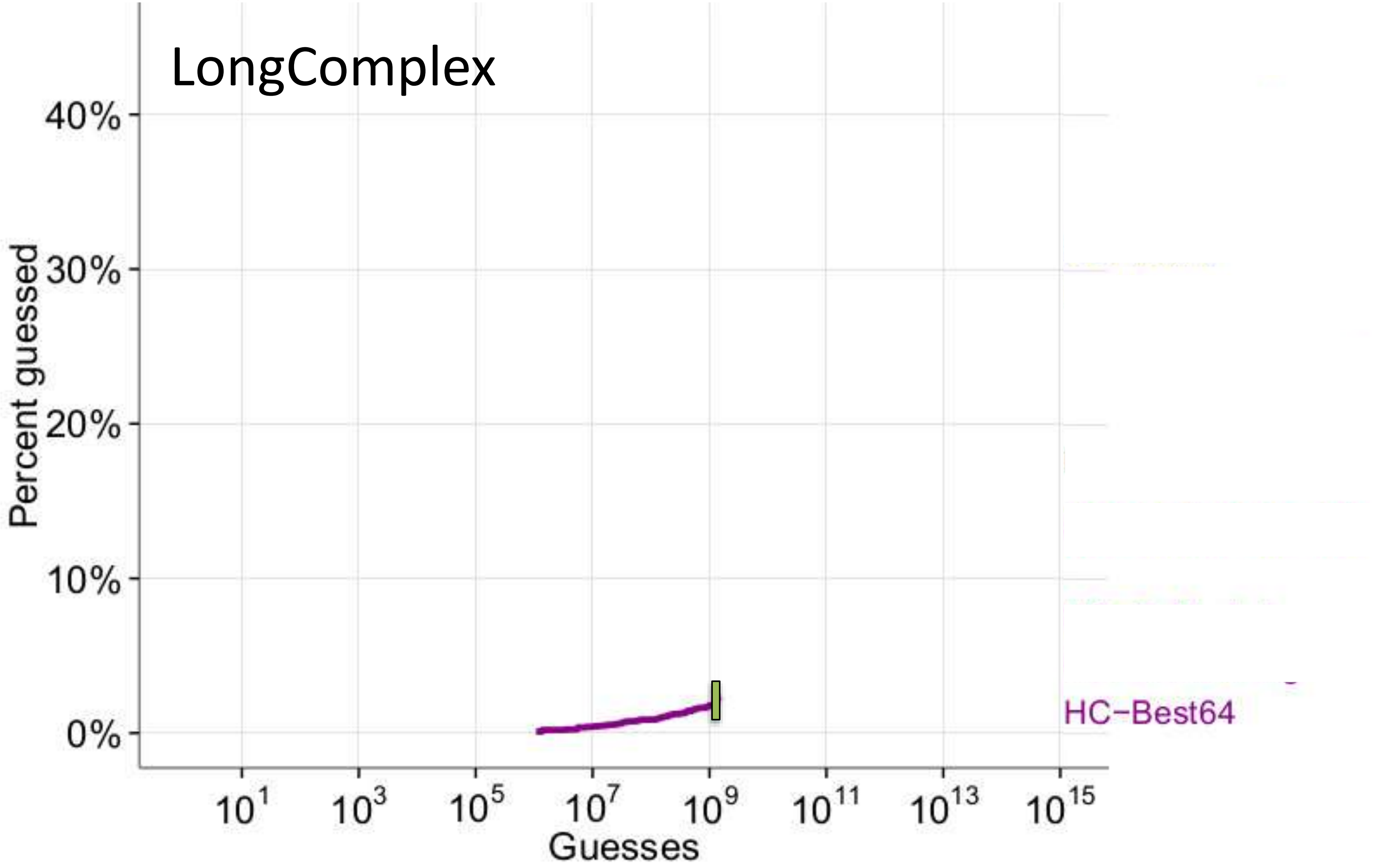


KoreLogic
SECURITY

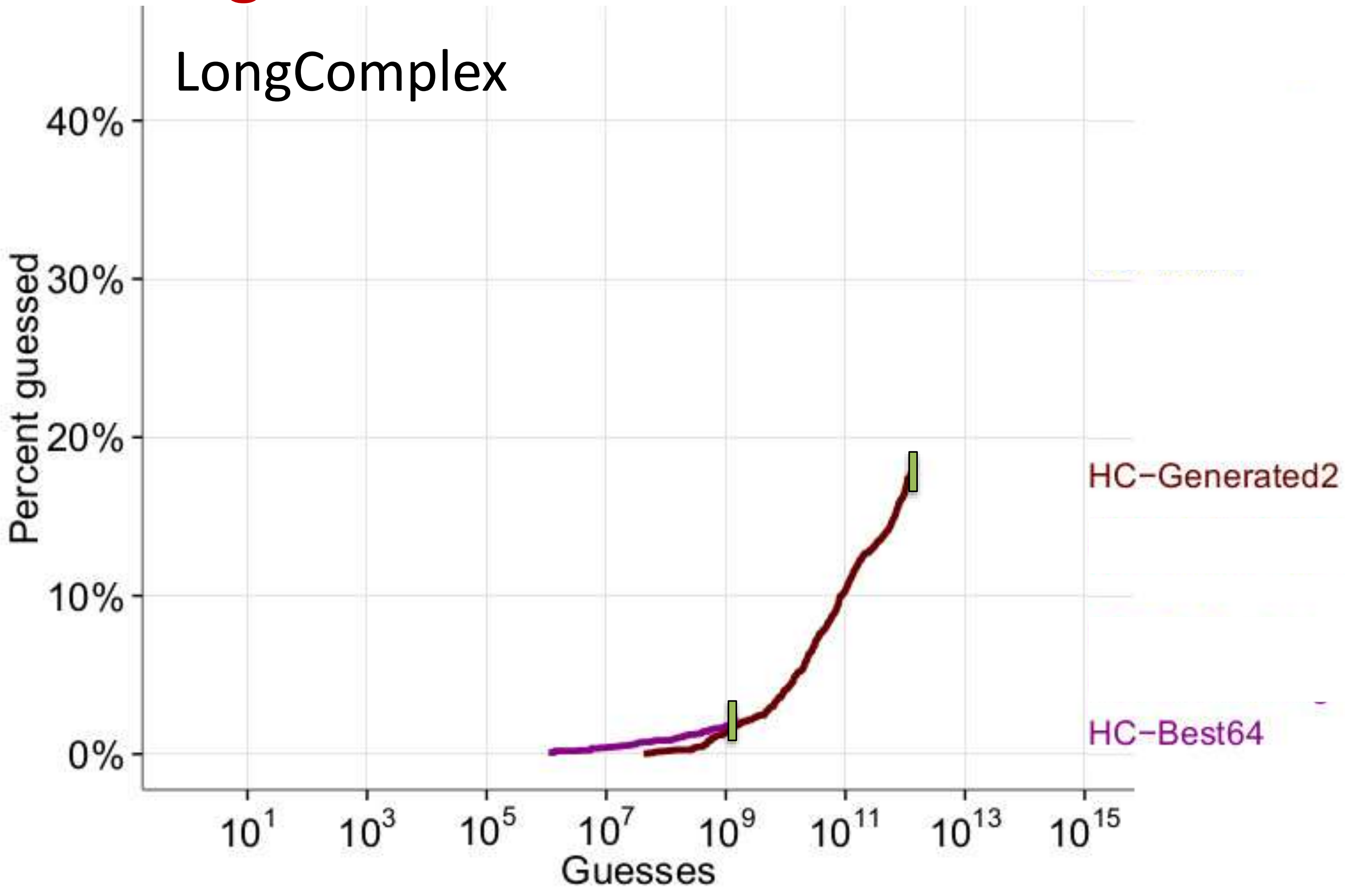
Outline of Results

- Importance of Configuration
- Comparison of Approaches
- Impact on Research Analyses

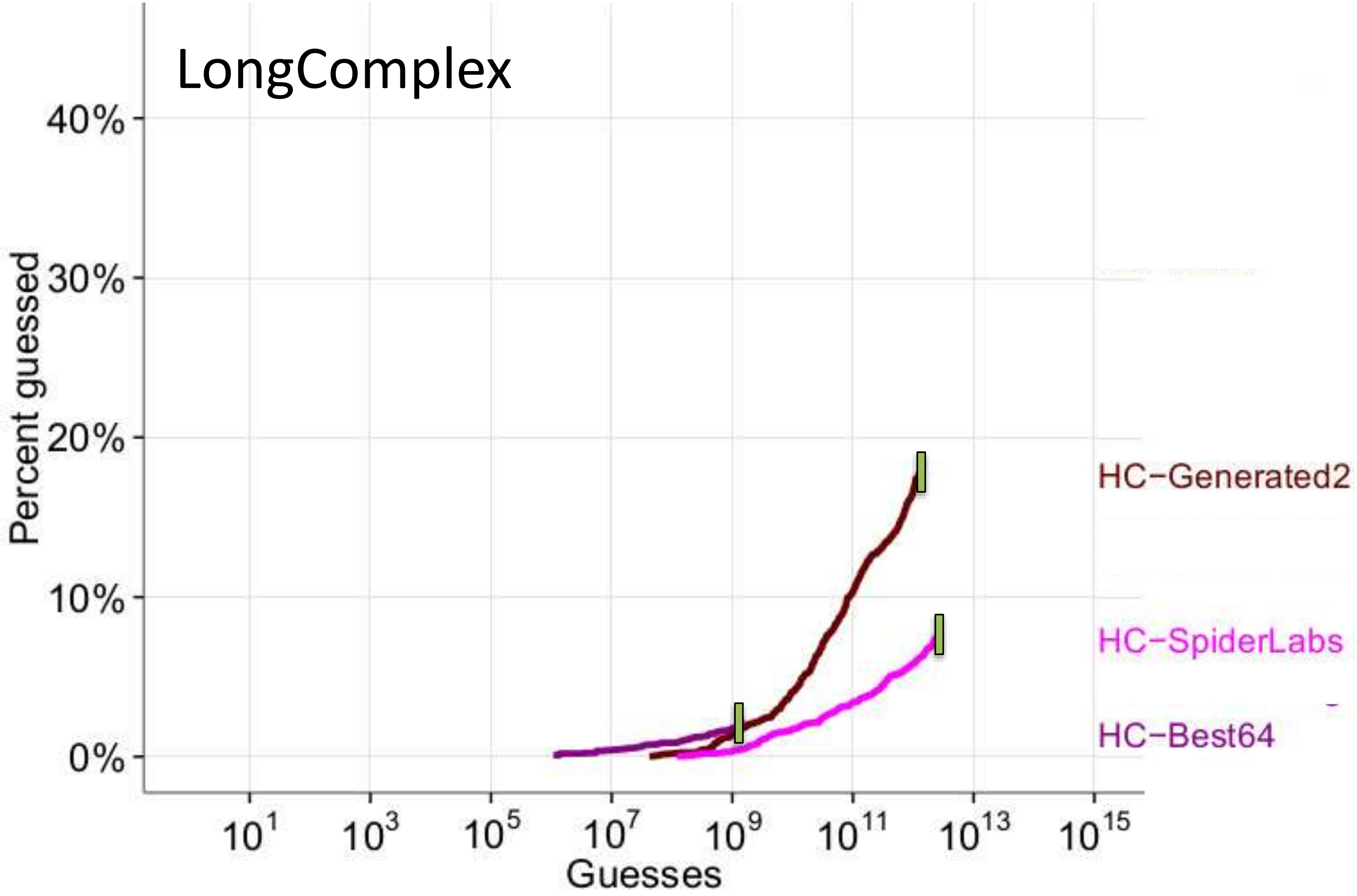
Configuration Is Crucial



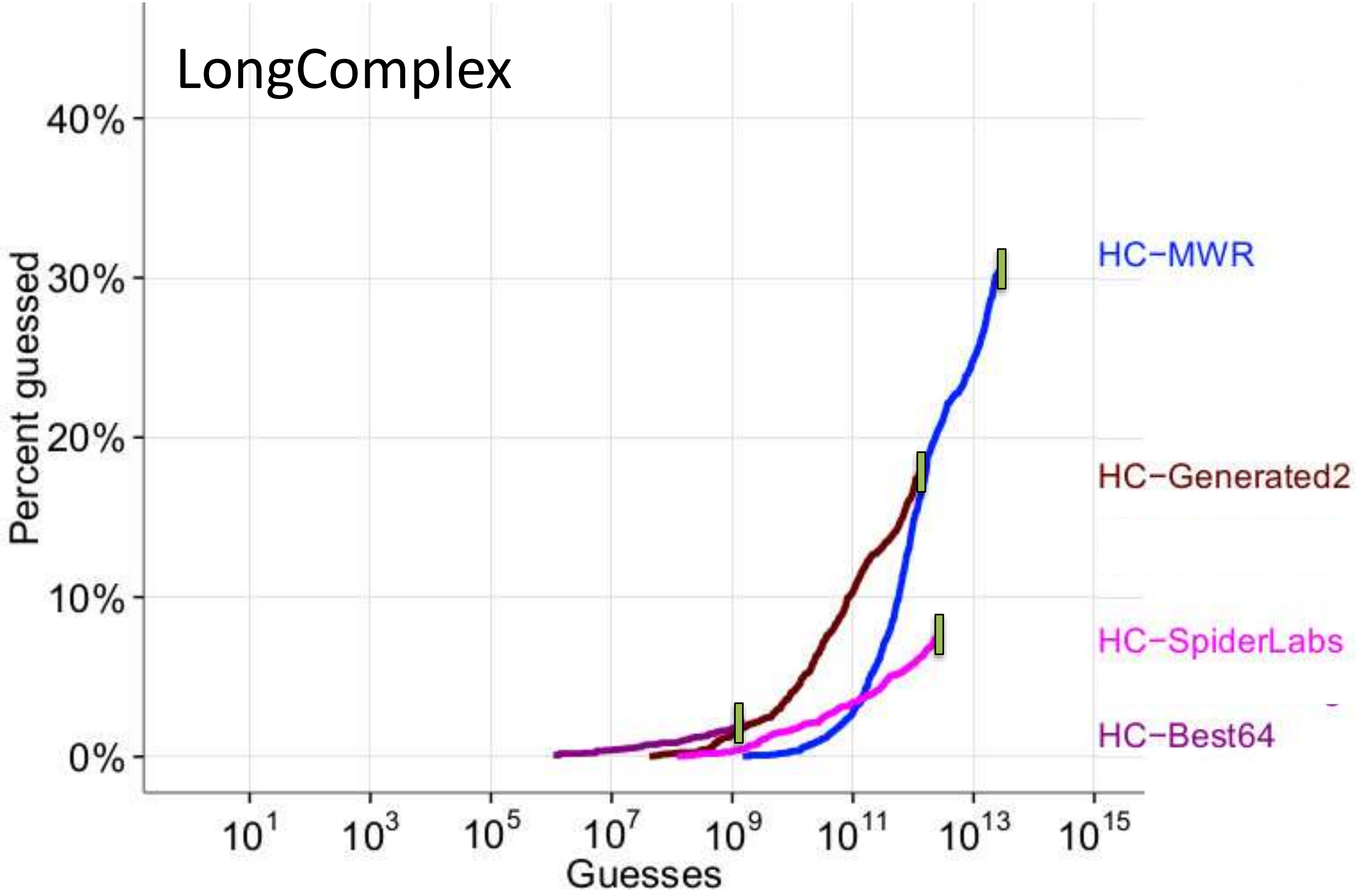
Configuration Is Crucial



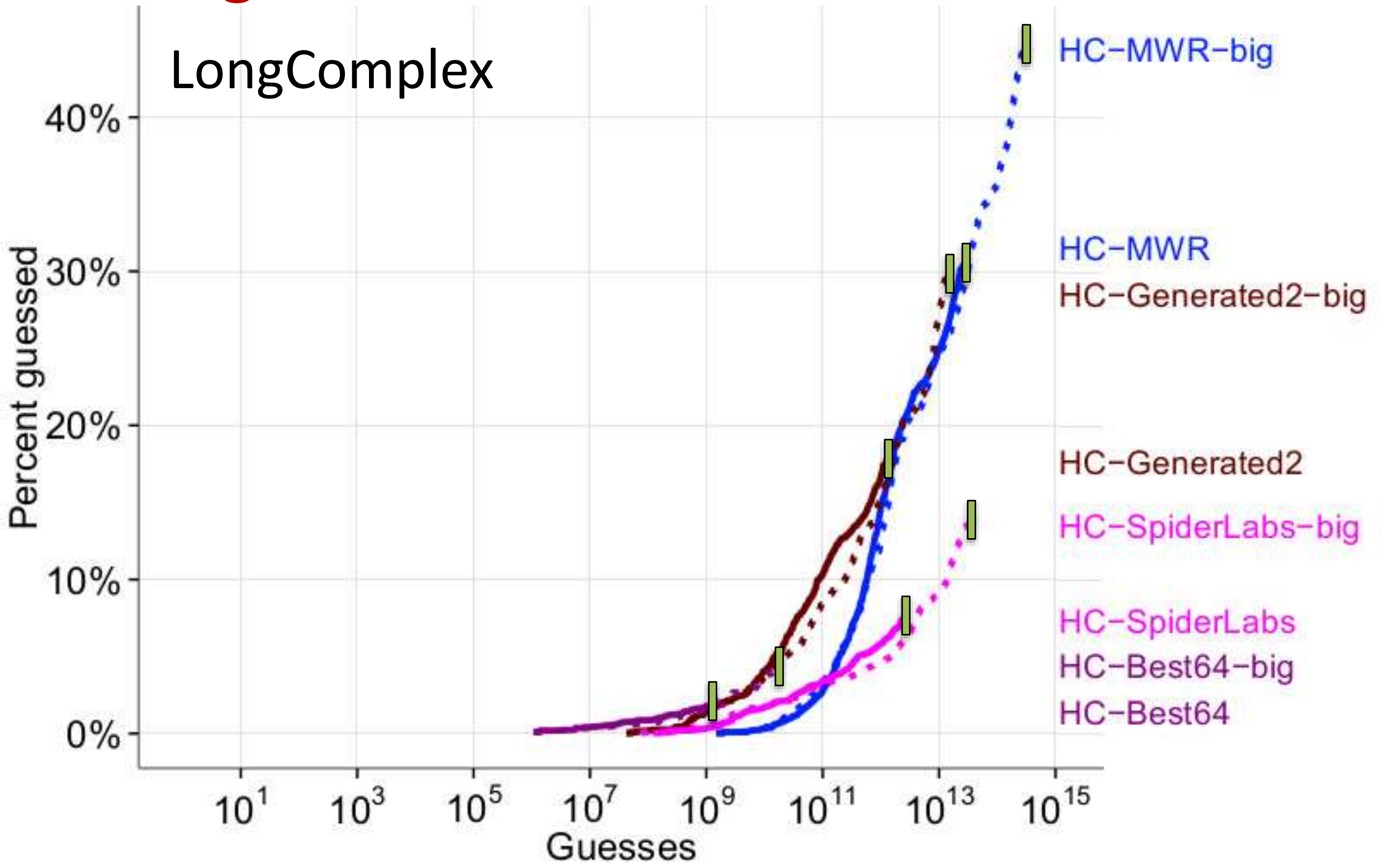
Configuration Is Crucial



Configuration Is Crucial



Configuration Is Crucial

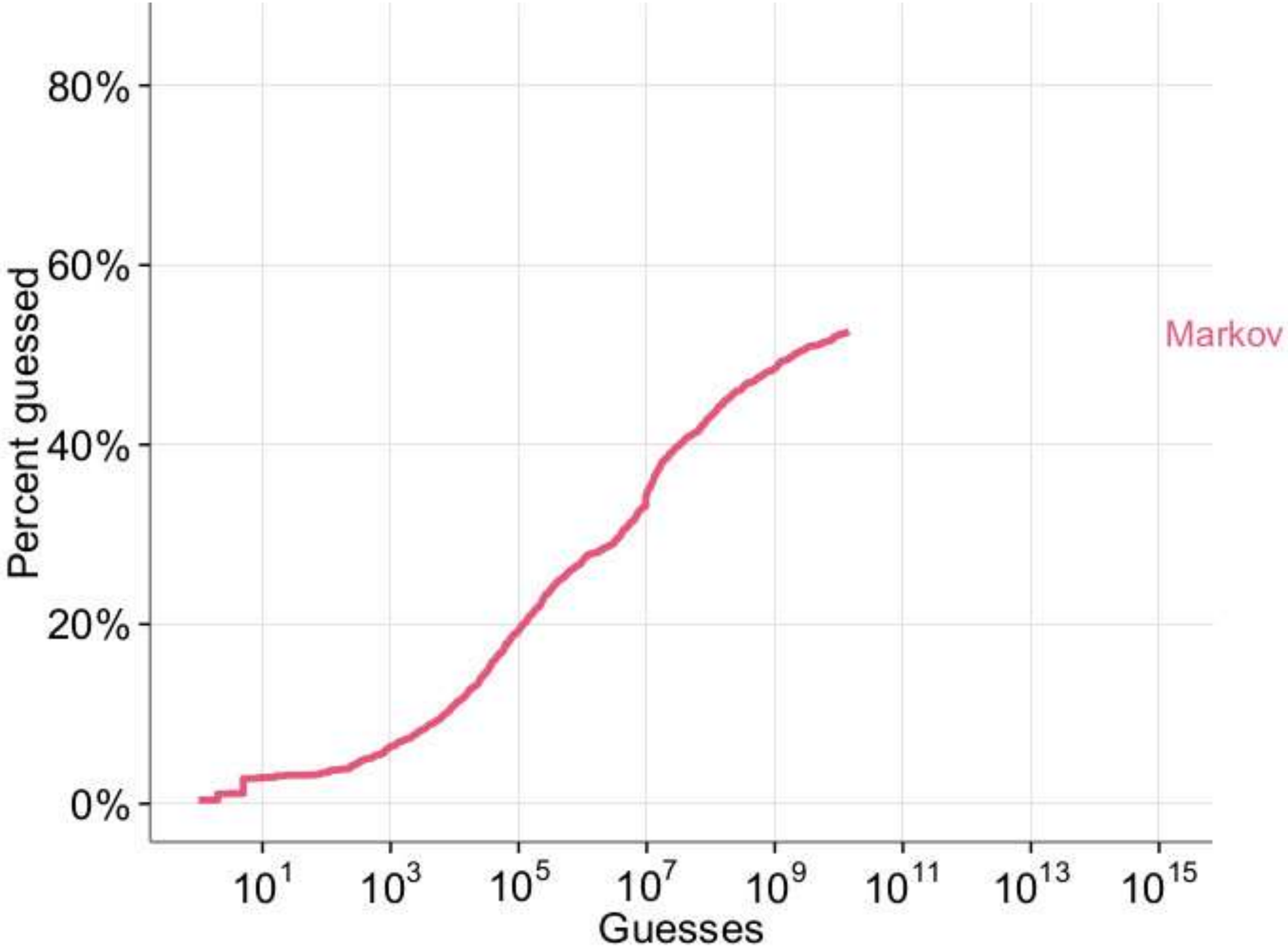


Outline of Results

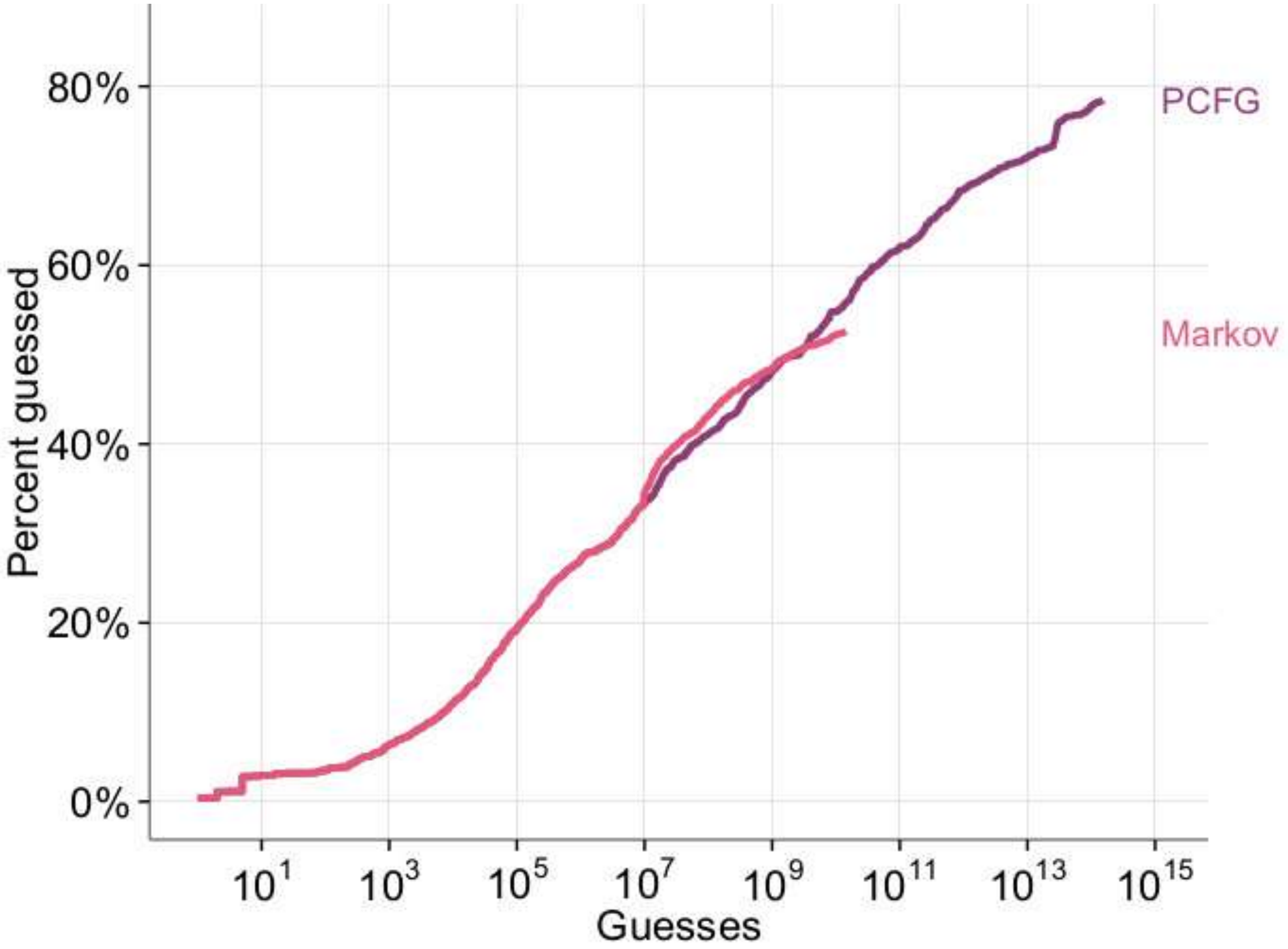
- Importance of Configuration
- Comparison of Approaches
- Impact on Research Analyses

Comparison for Basic Passwords

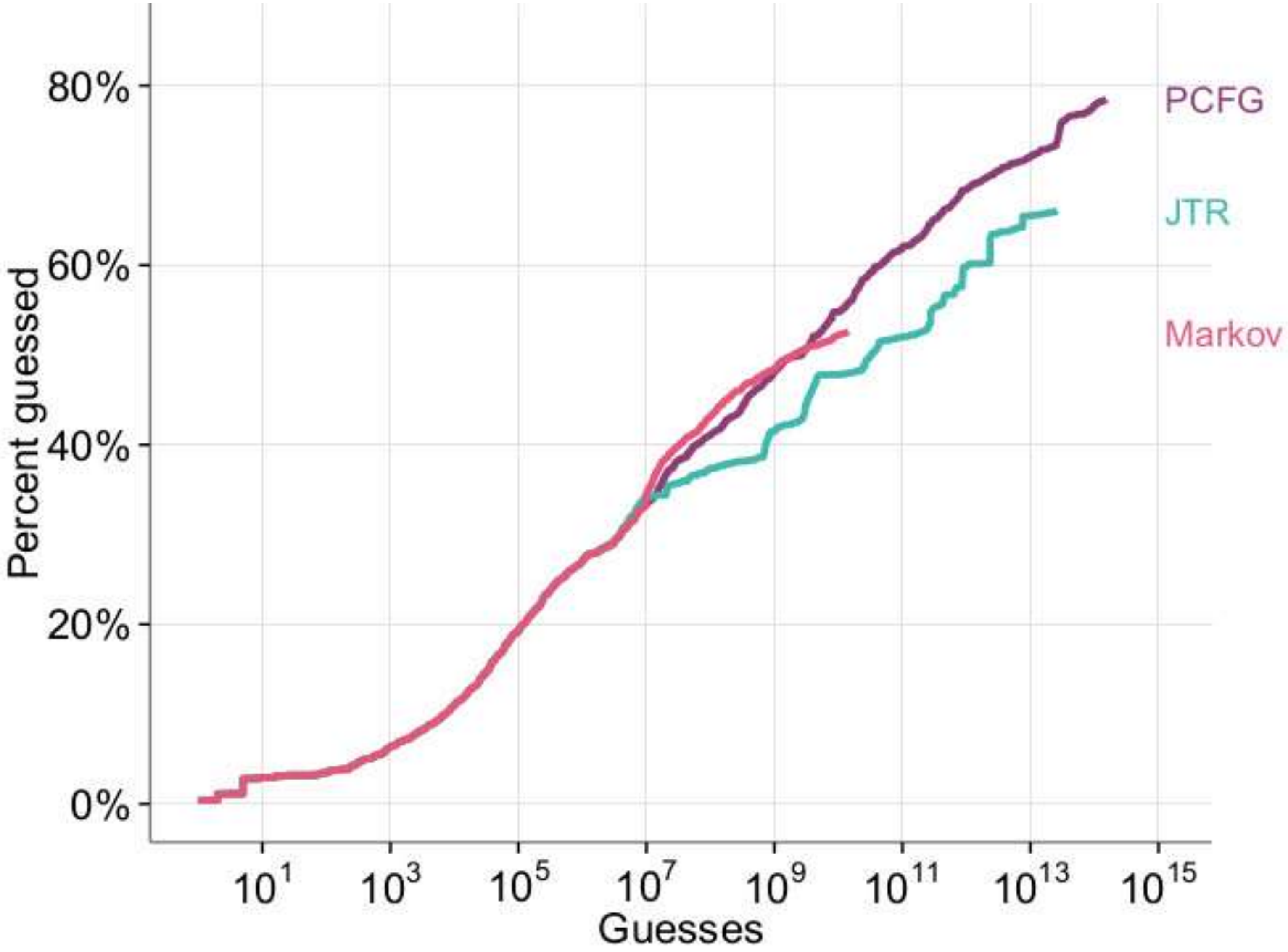
Comparison for Basic Passwords



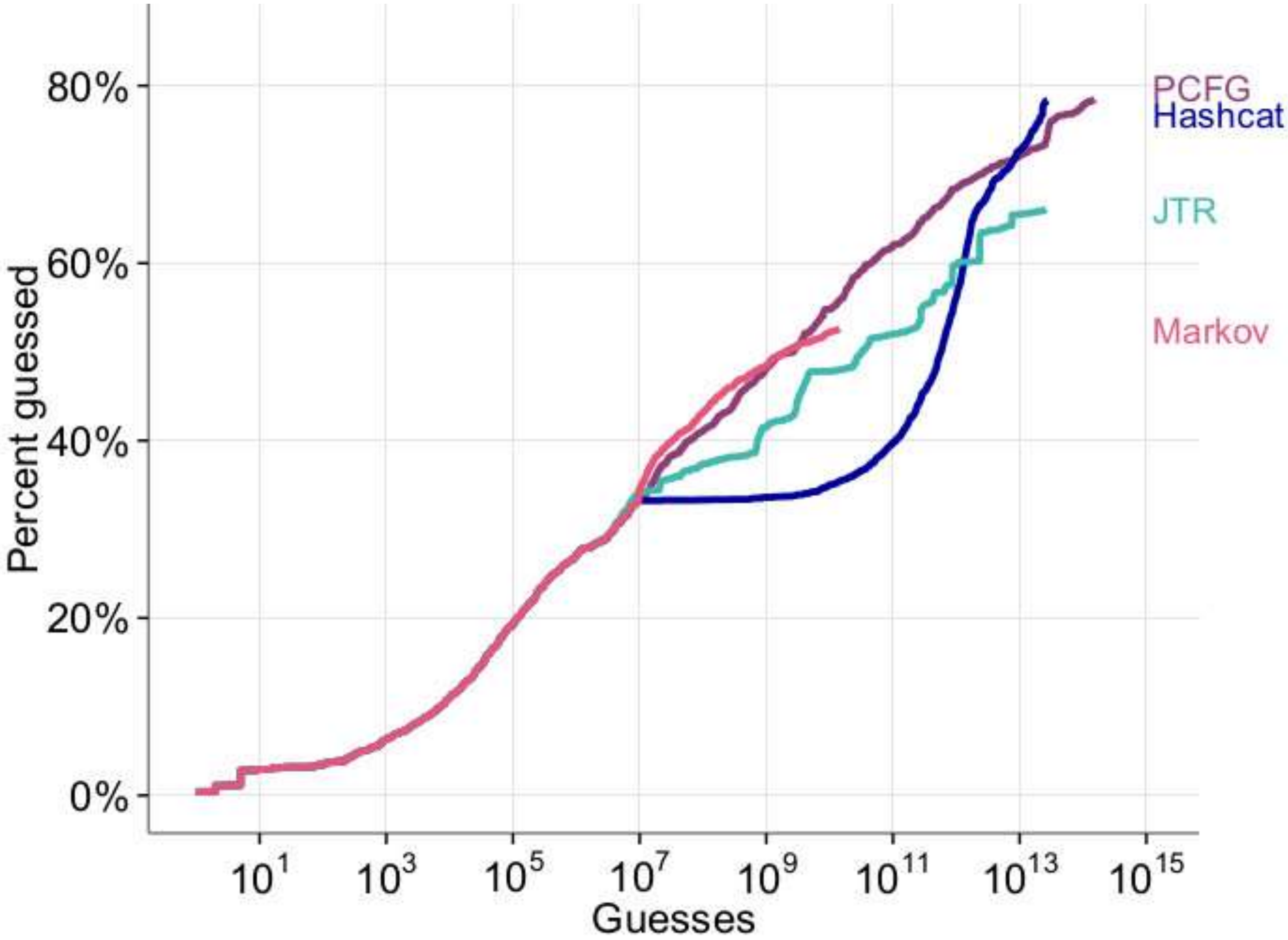
Comparison for Basic Passwords



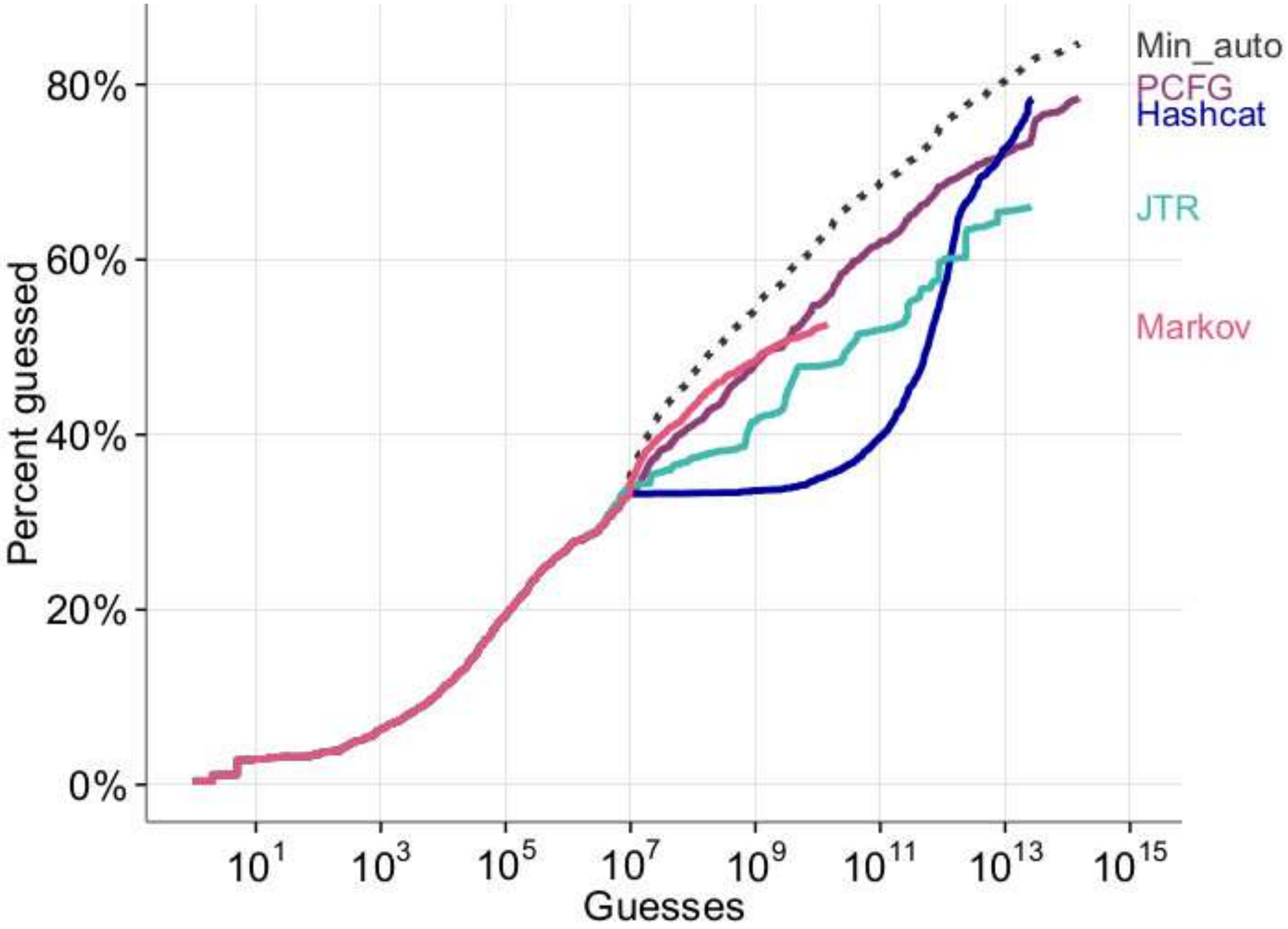
Comparison for Basic Passwords



Comparison for Basic Passwords

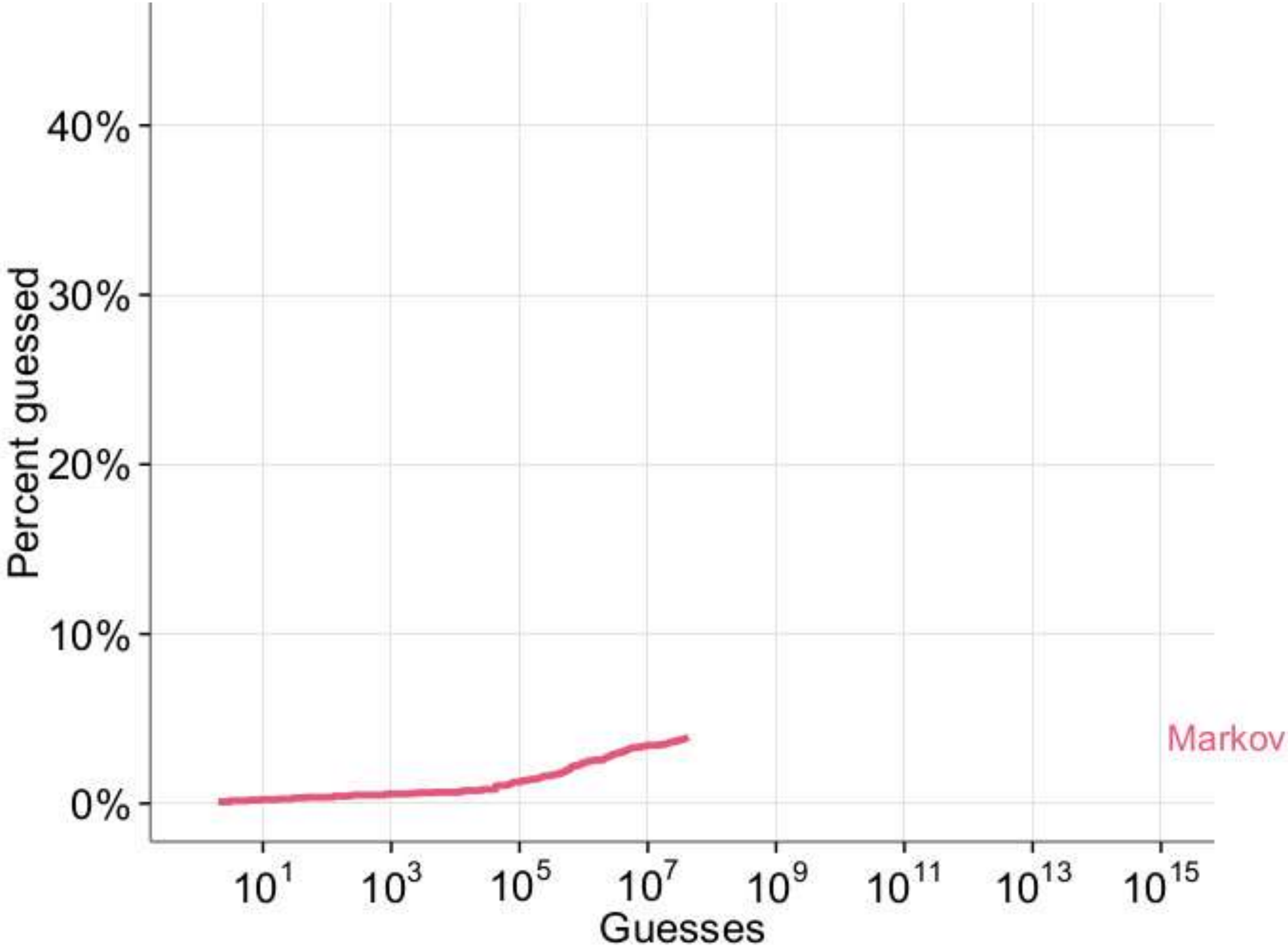


Comparison for Basic Passwords

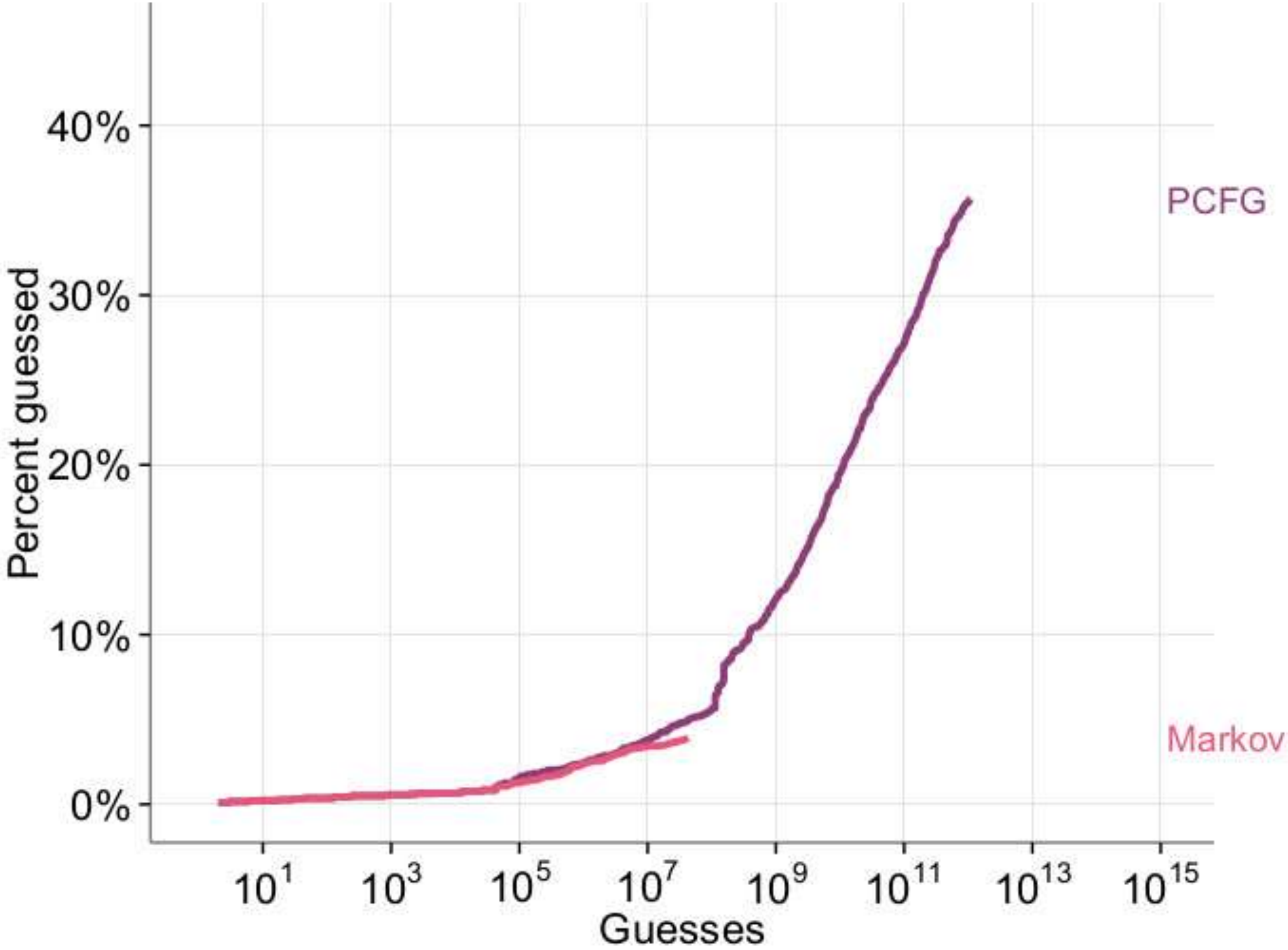


Comparison for Complex Passwords

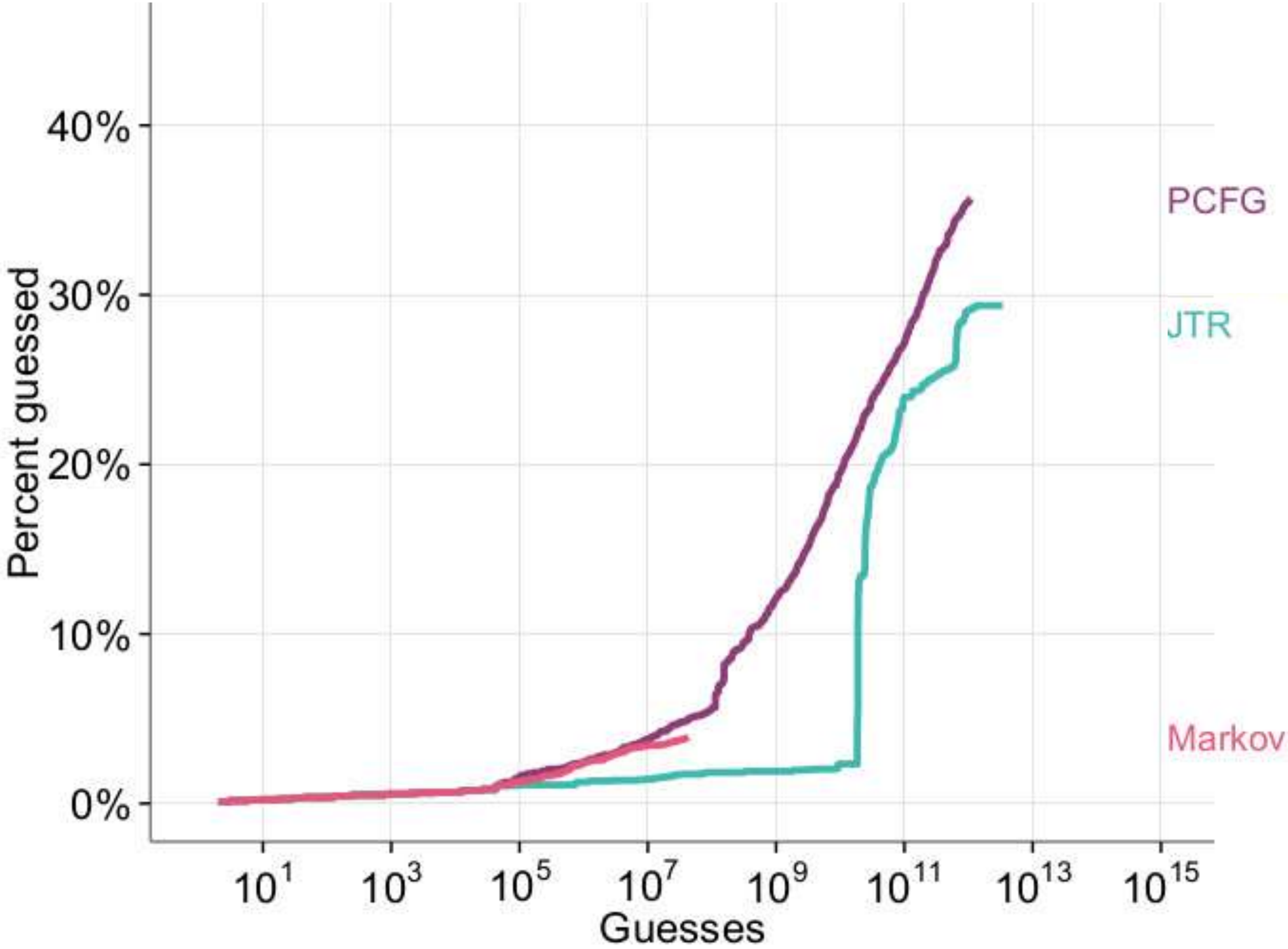
Comparison for Complex Passwords



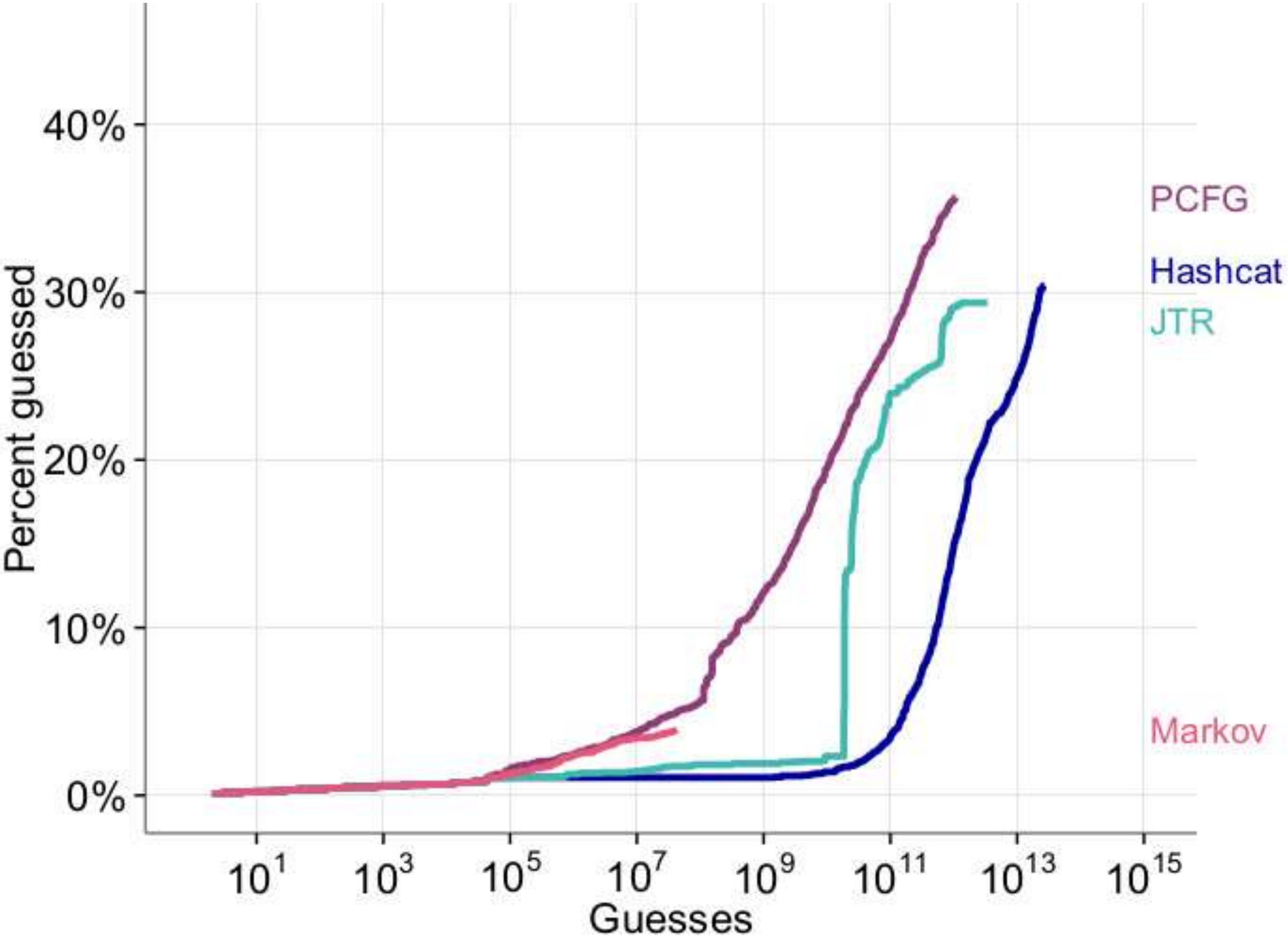
Comparison for Complex Passwords



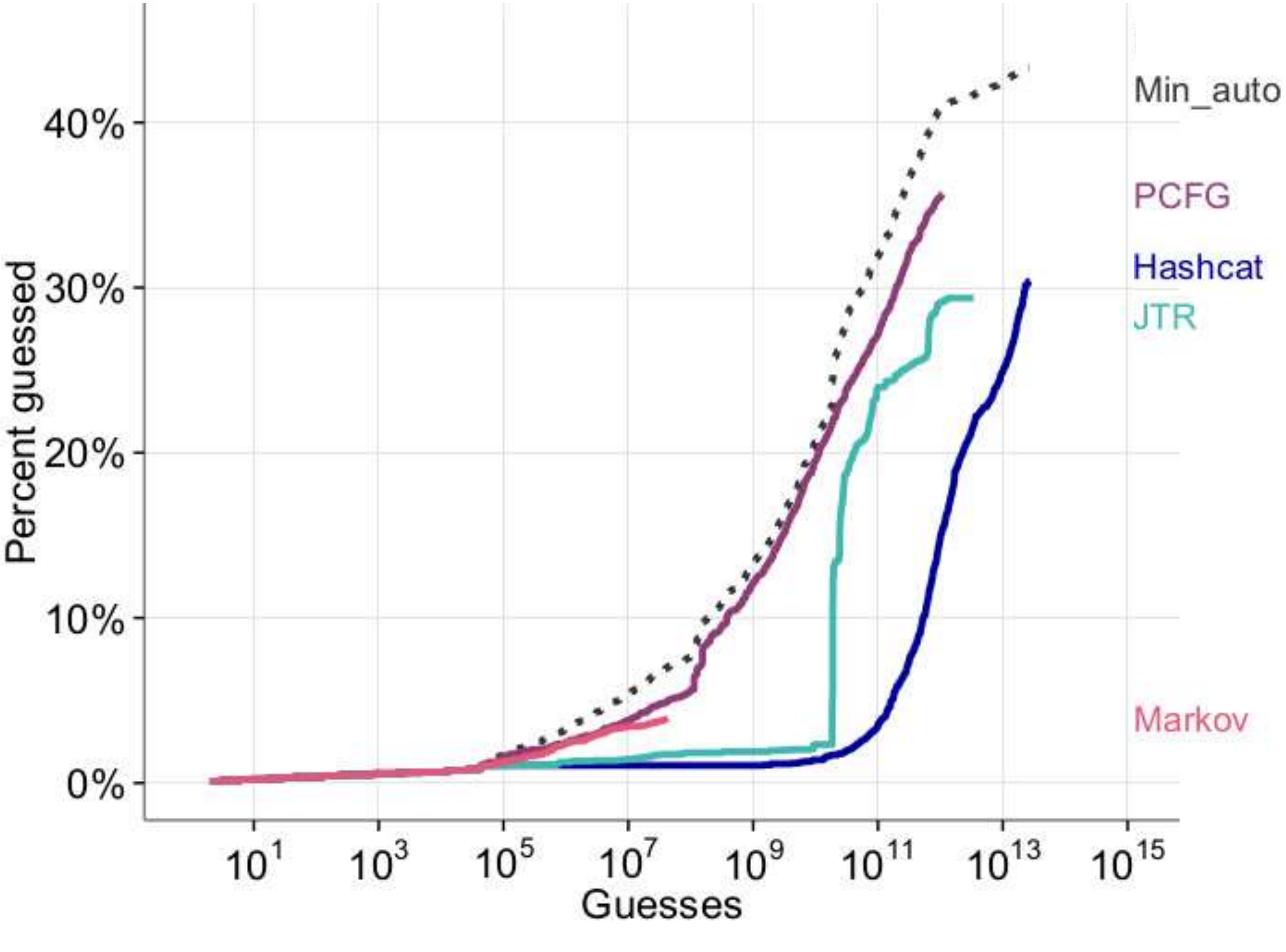
Comparison for Complex Passwords



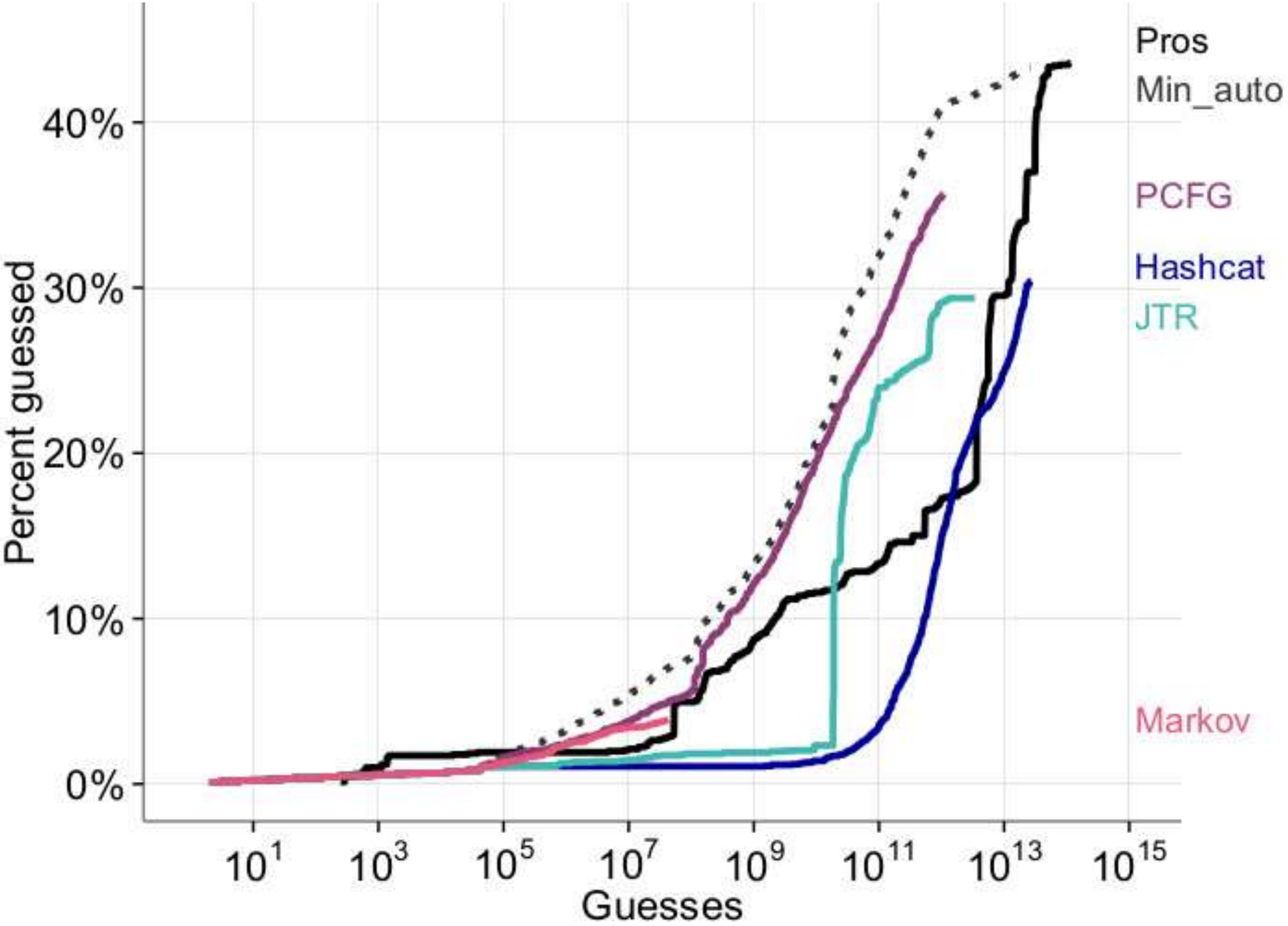
Comparison for Complex Passwords



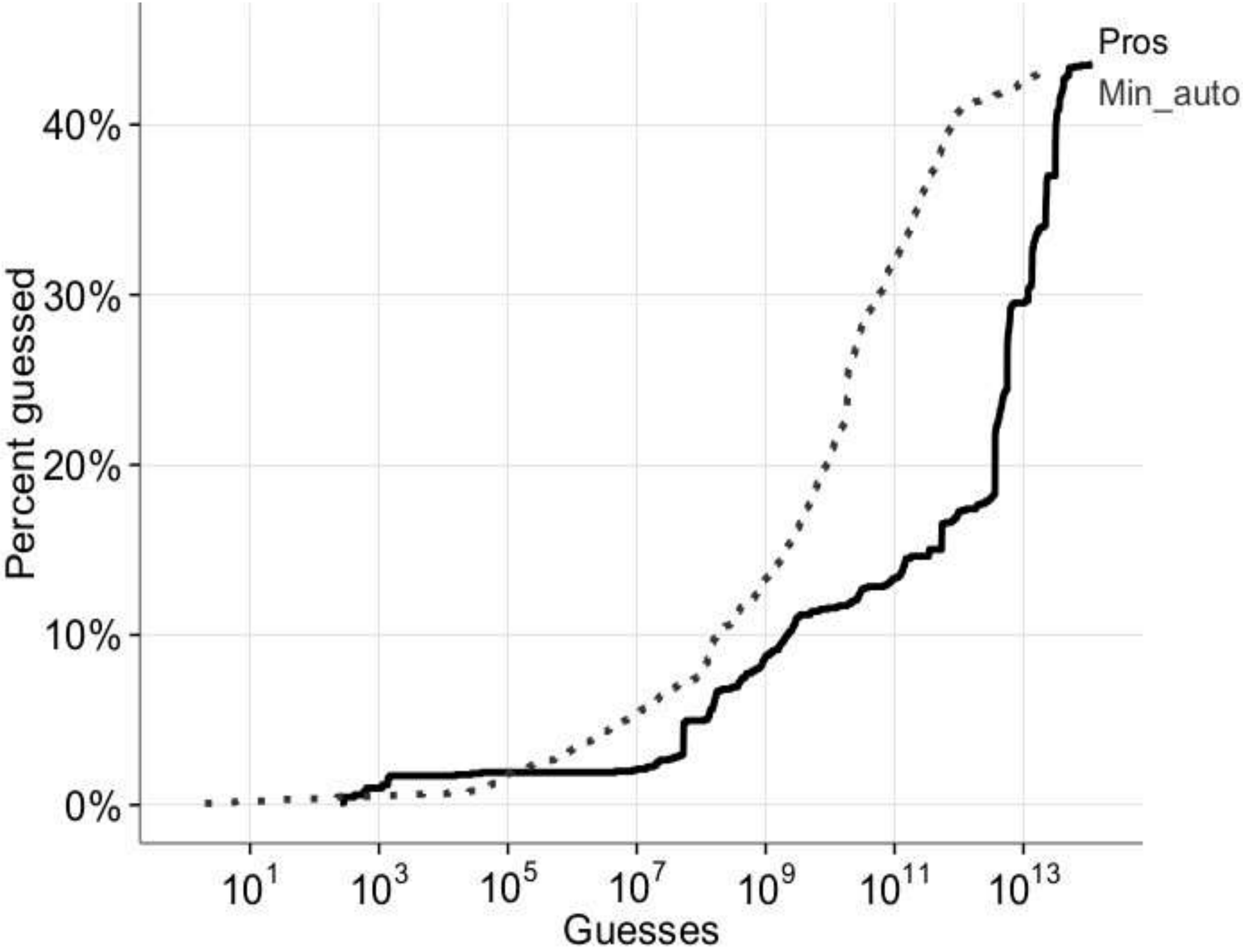
Comparison for Complex Passwords



Comparison for Complex Passwords



Min_auto Conservative Proxy for Pros



Per-Password Highly Impacted

P@ssw0rd!

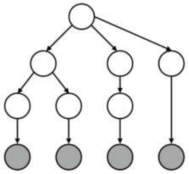
Per-Password Highly Impacted

- JTR guess # 801

P@ssw0rd!

Per-Password Highly Impacted

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

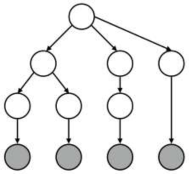


P@ssw0rd!

Per-Password Highly Impacted

- JTR guess # 801

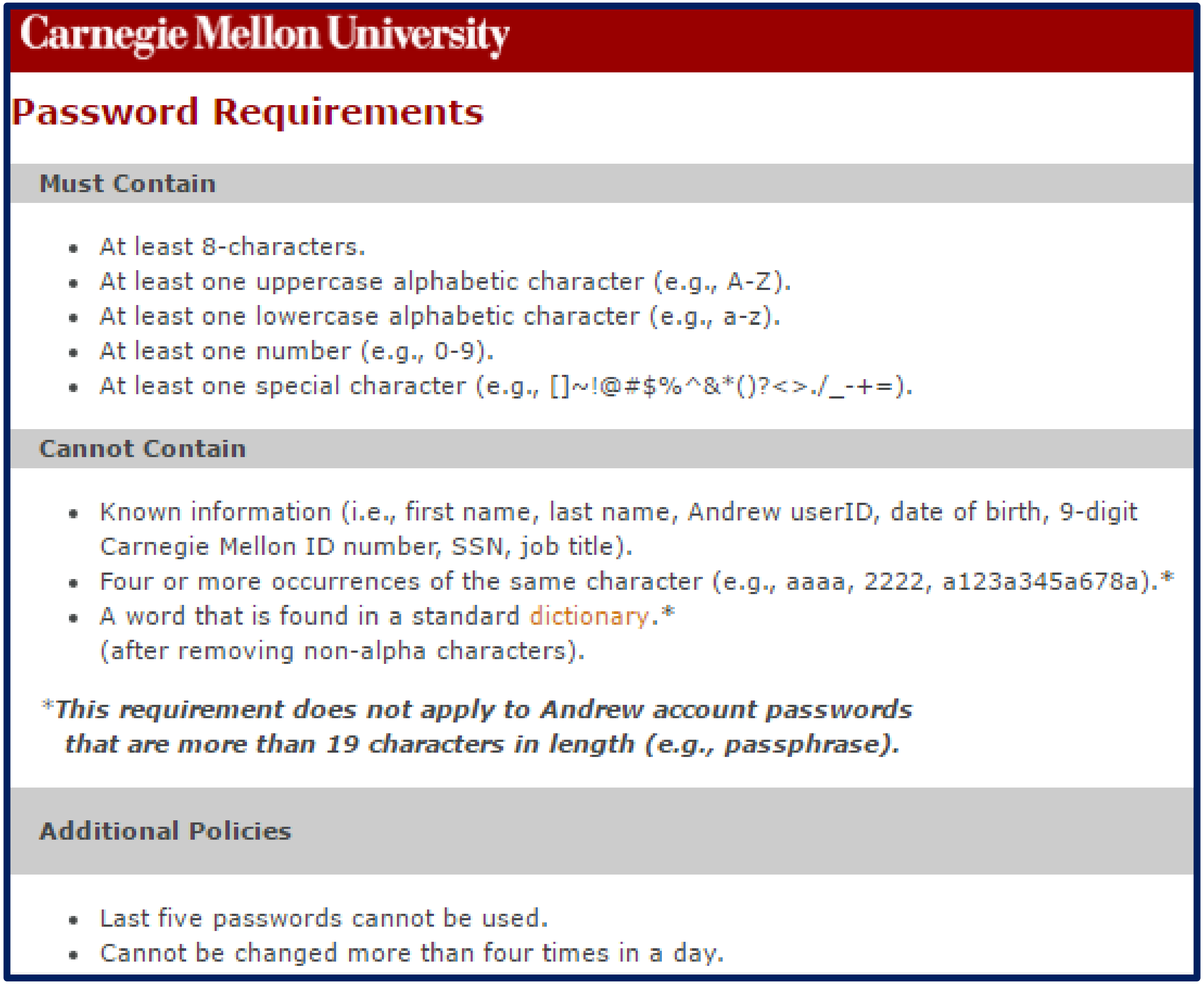
- Not guessed in 10^{14} PCFG guesses



P@ssw0rd!

How Do We Help Users Make Better Passwords?

Problem 1: Bad 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).

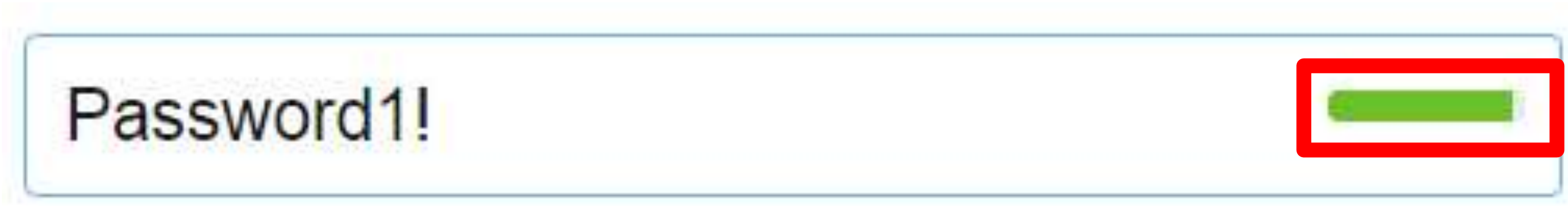
*_**This requirement does not apply to Andrew account passwords
that are more than 19 characters in length (e.g., passphrase).**_

Additional Policies

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

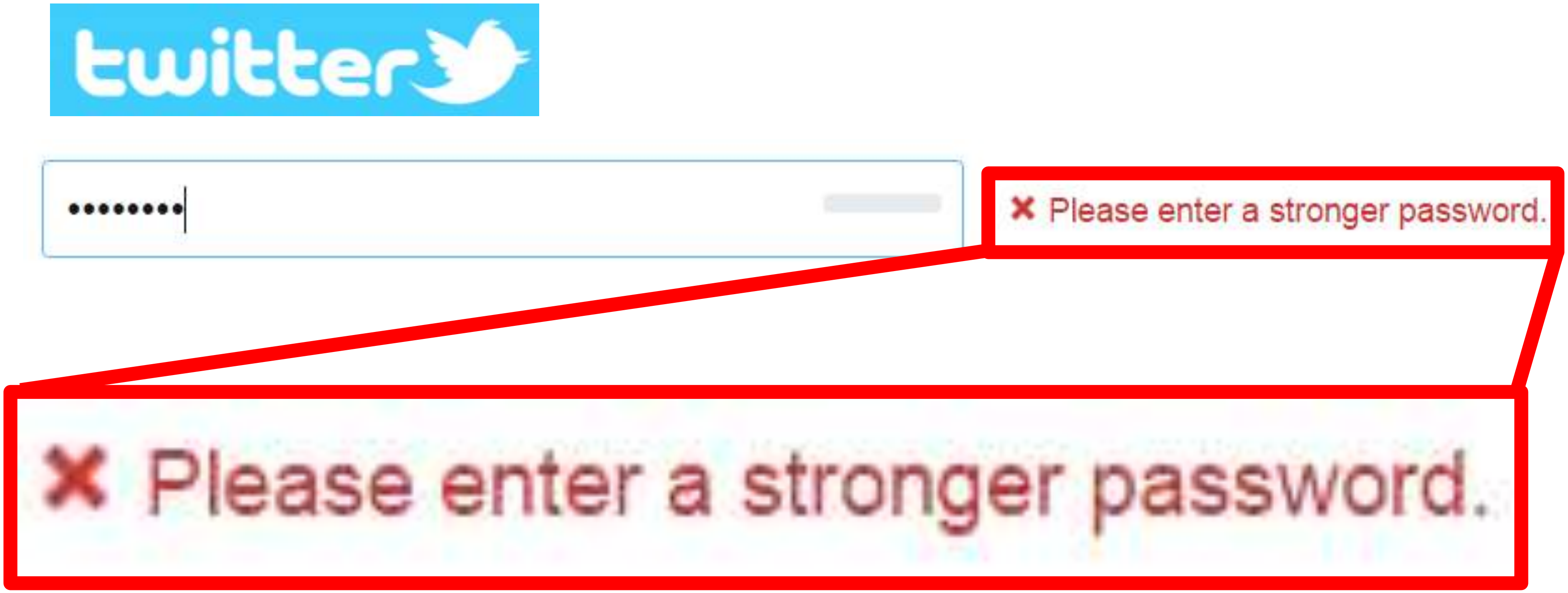
Problem 2: Inaccurate Feedback

twitter



Password1!

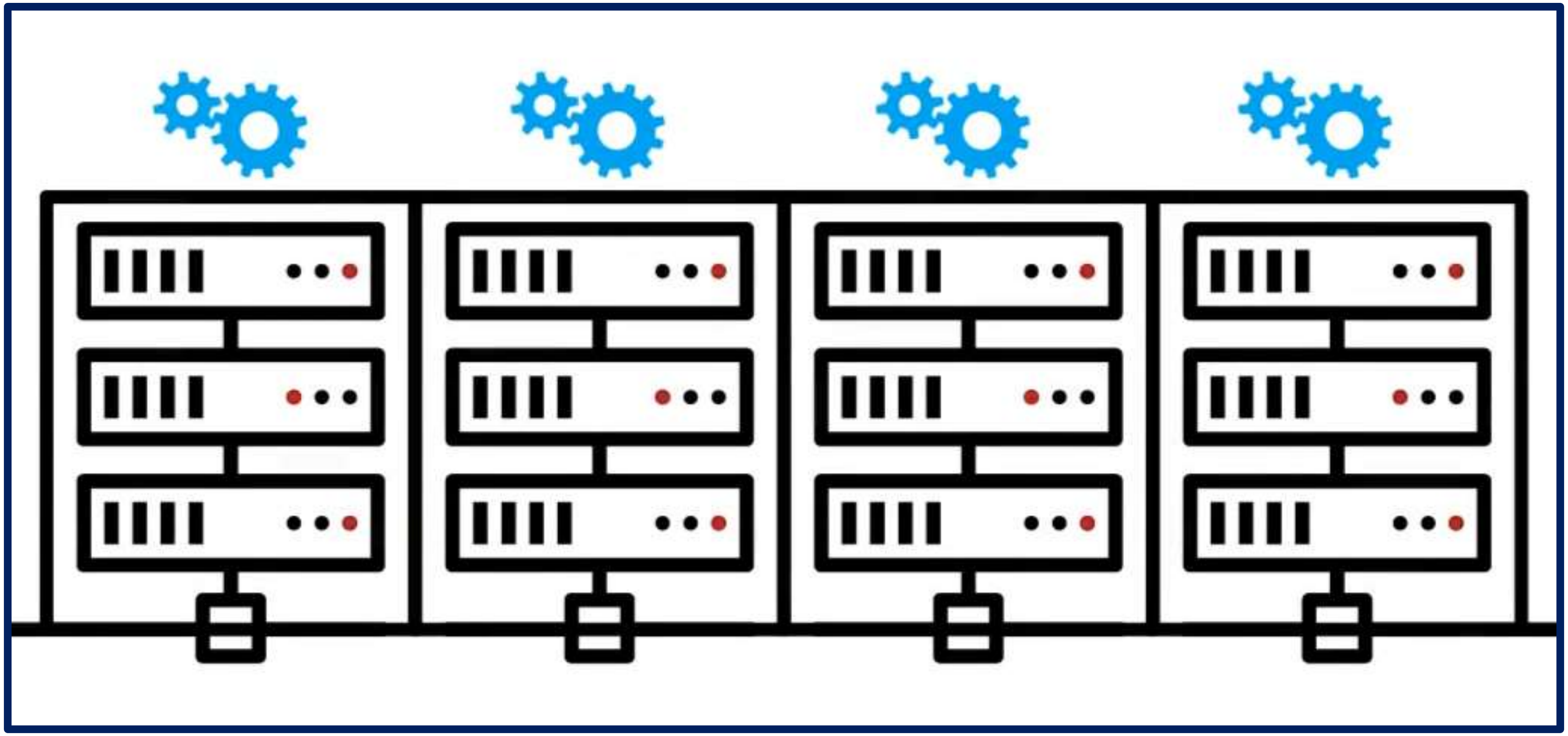
Problem 3: Unhelpful Feedback



✖ Please enter a stronger password.

✖ Please enter a stronger password.

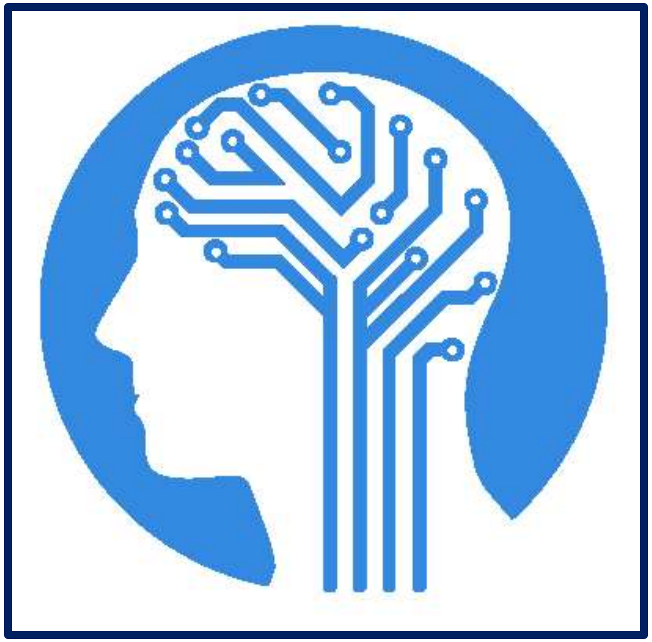
Better Password Scoring



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



Recurrent Neural Networks (RNNs)

LSTM Architecture

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

“”

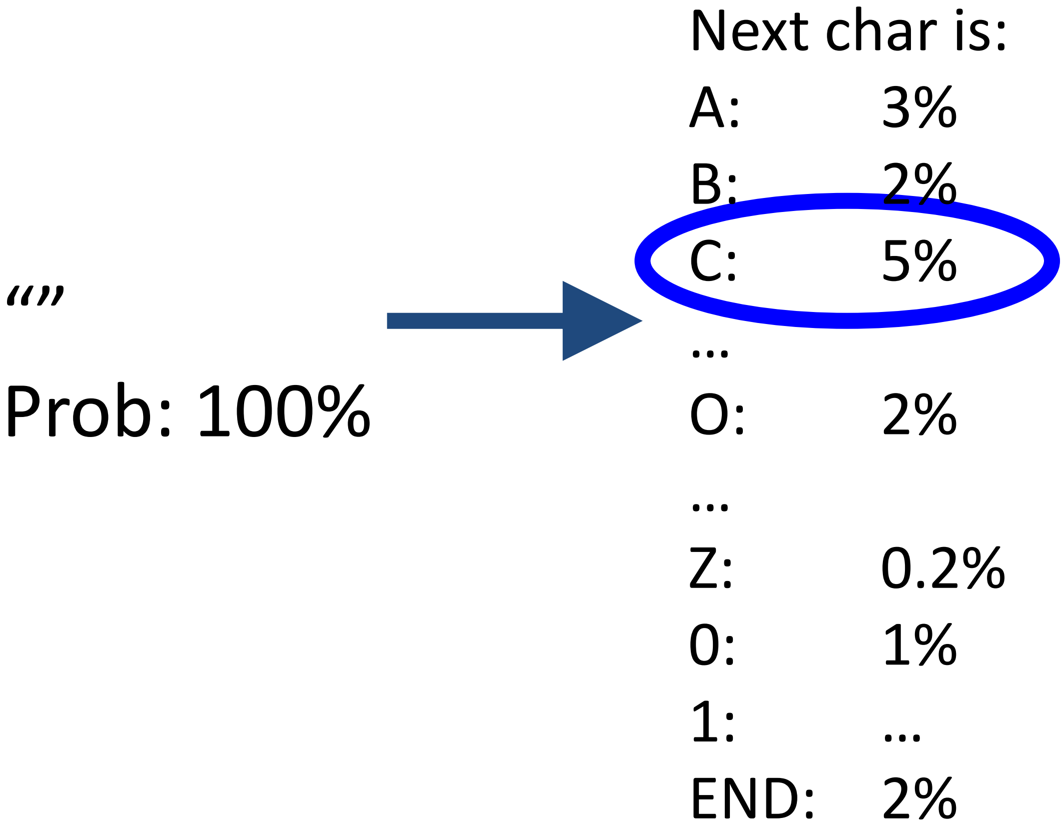
Prob: 100%

→

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"

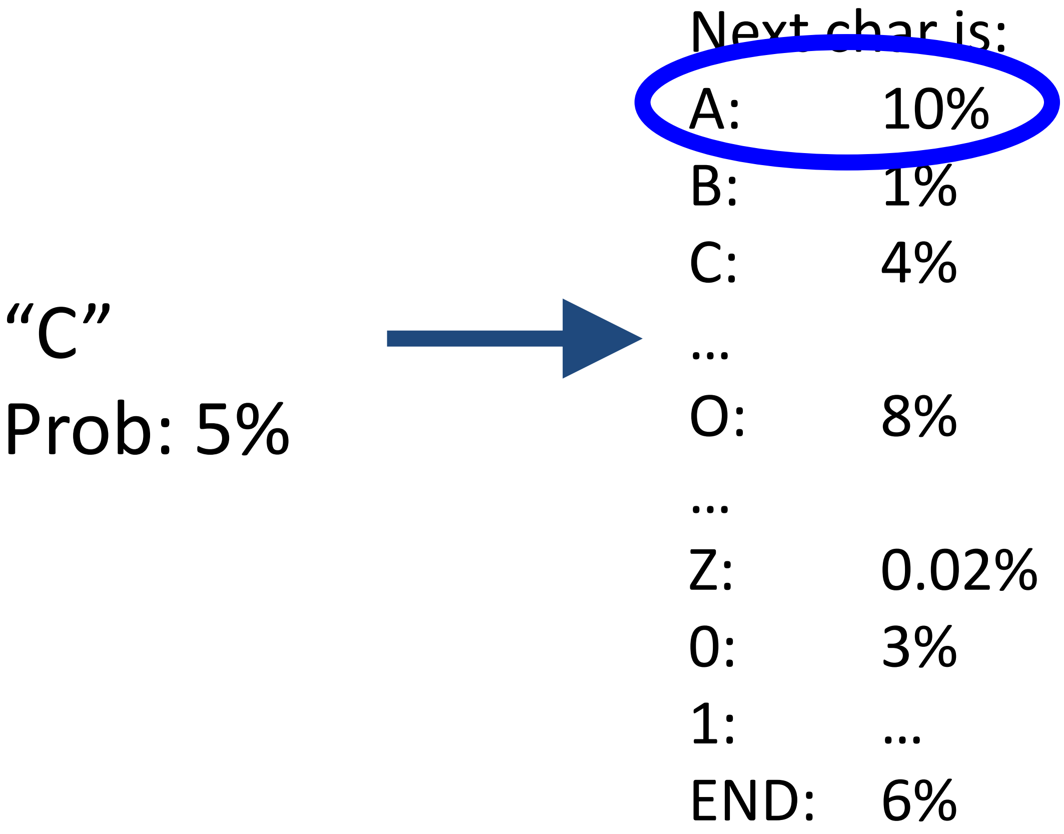
Prob: 5%

→

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”

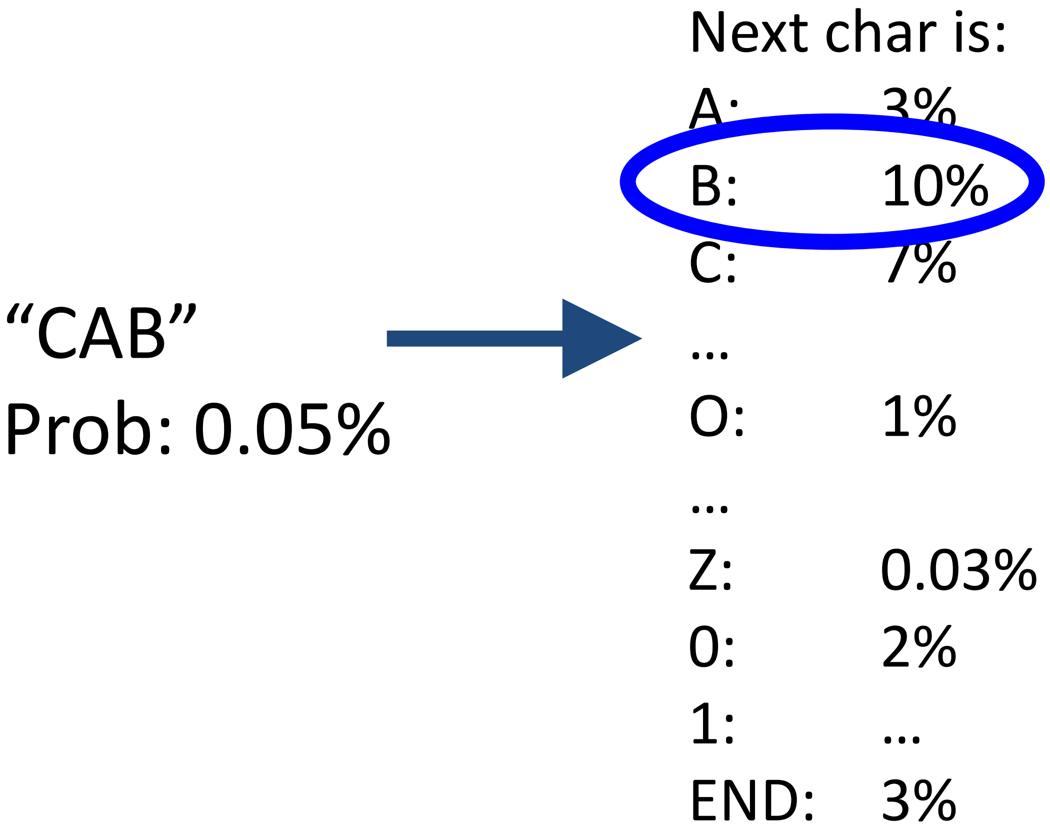
Prob: 0.5%

→

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”

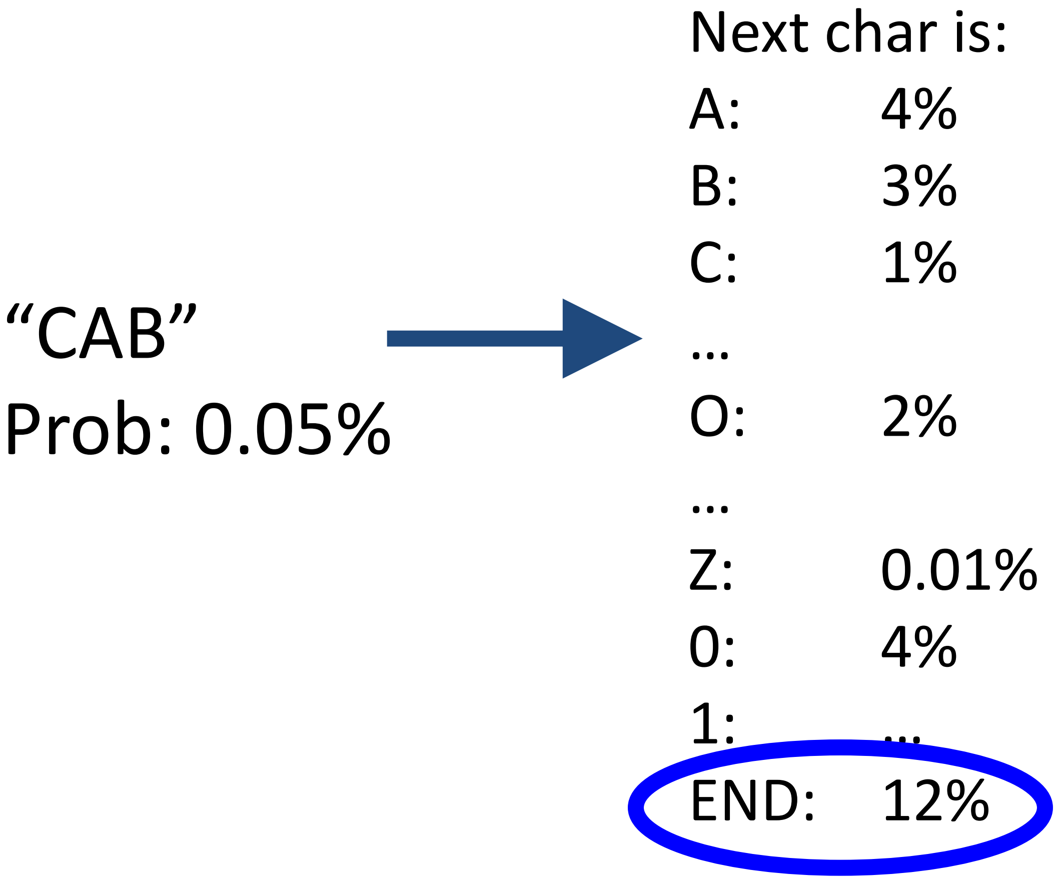
Prob: 0.05%

→

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%

Descending Probability Order

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

…

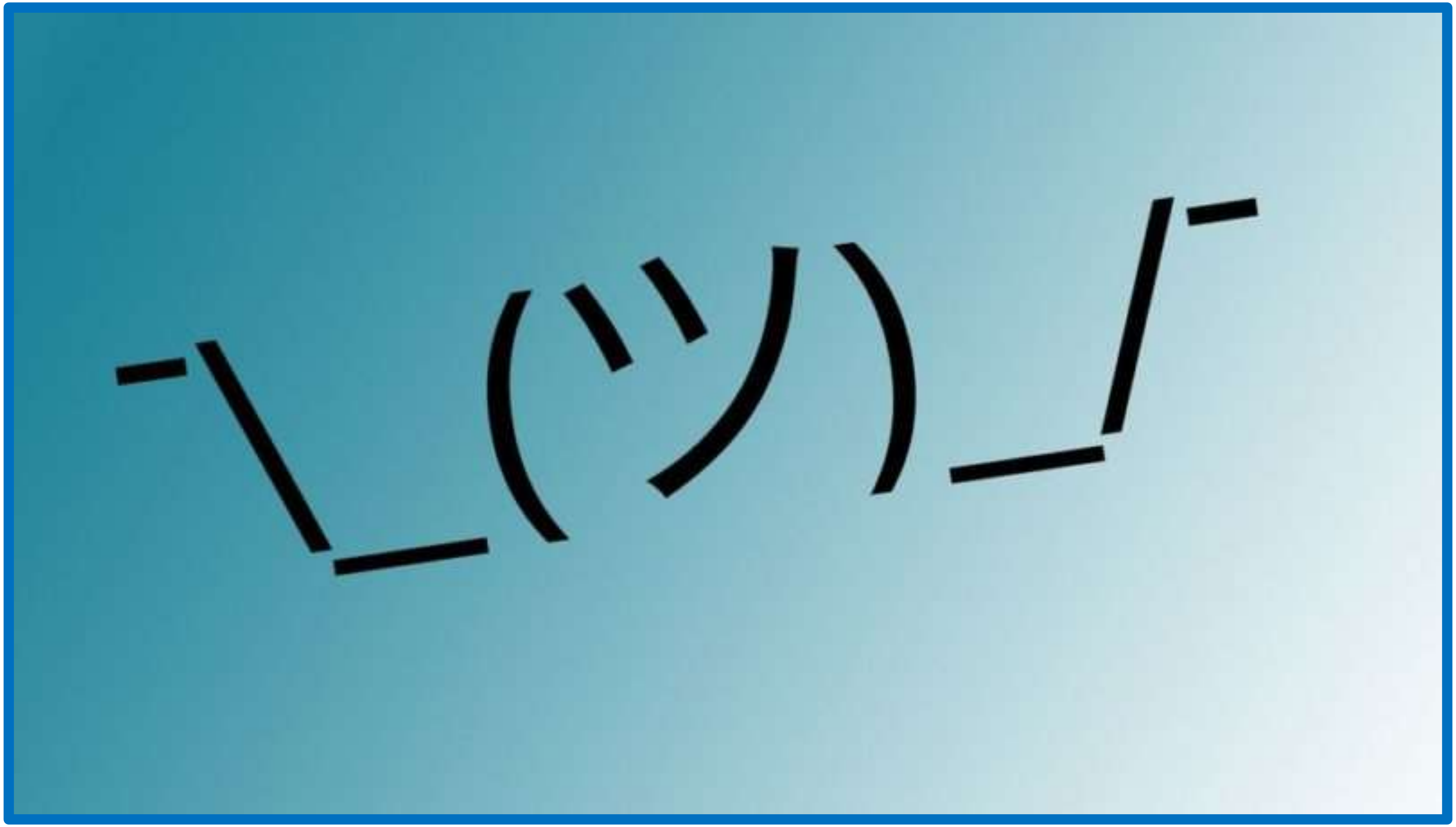
Design Space

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

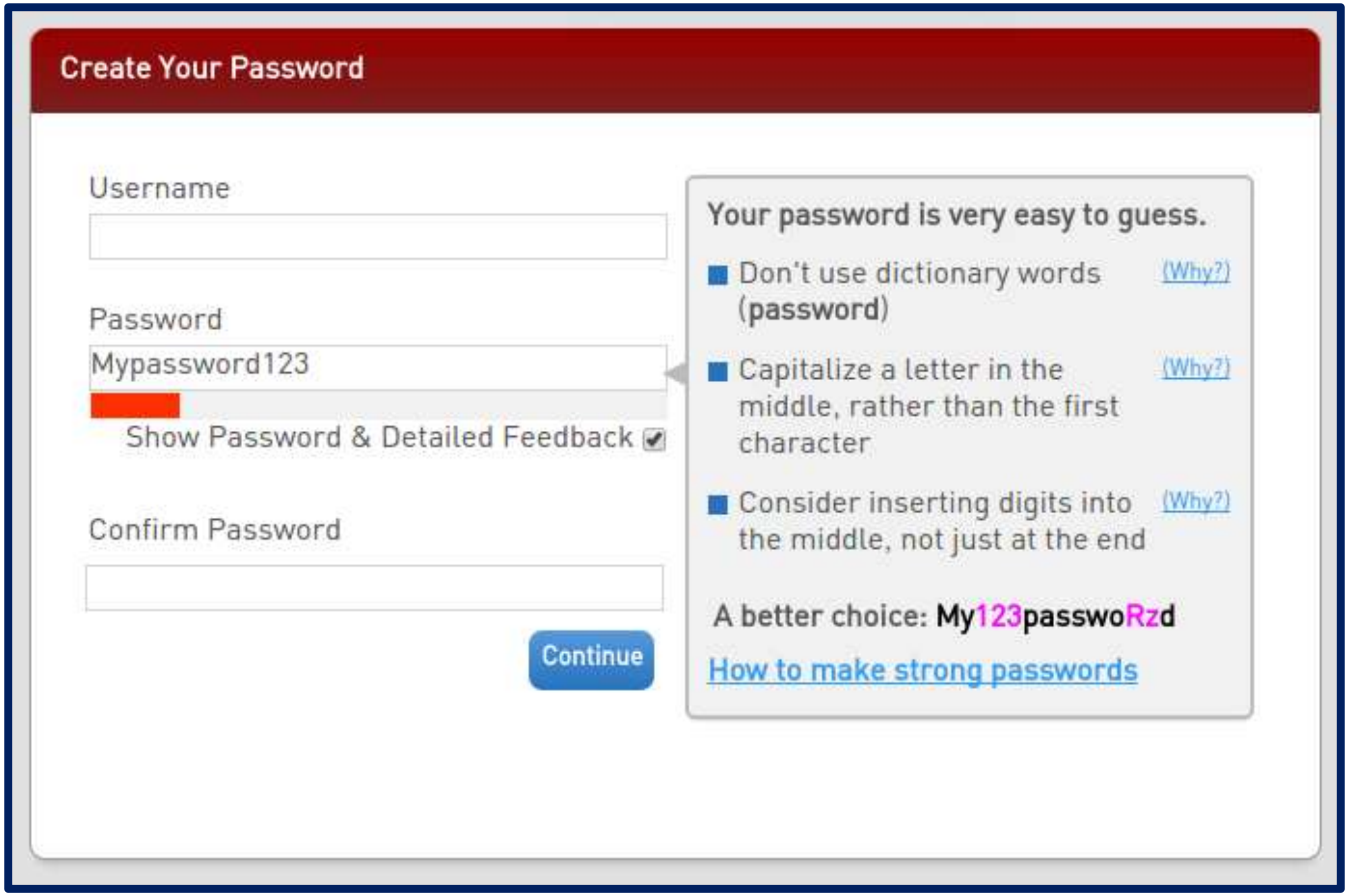
Key Results

- Neural networks produce better guesses than previous methods
- Larger model not a major advantage
- Browser implementation in Javascript

Intelligibility (Explanations)



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 (RNN)

2) Data-driven feedback to users

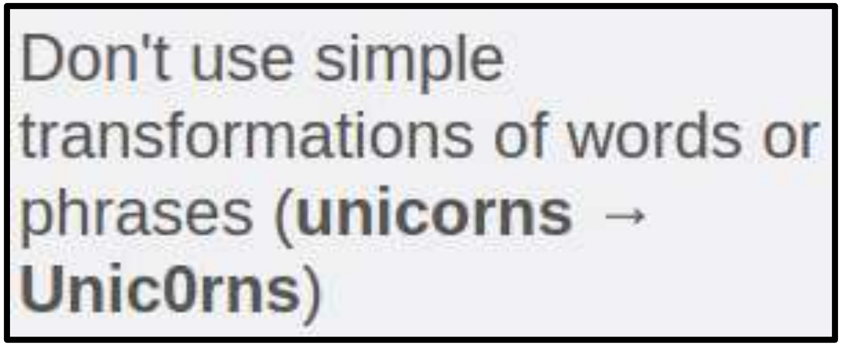
We designed & tested a meter with:

1) Principled strength estimates

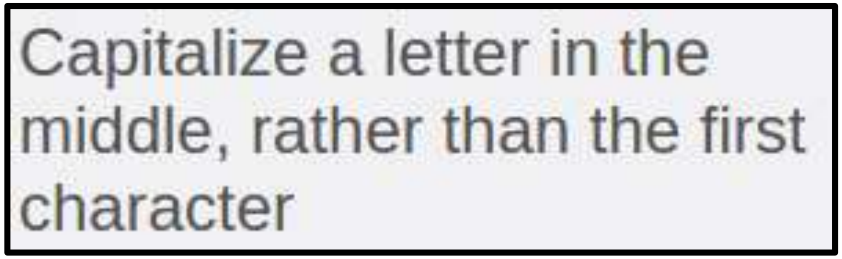
2) Data-driven feedback to users

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

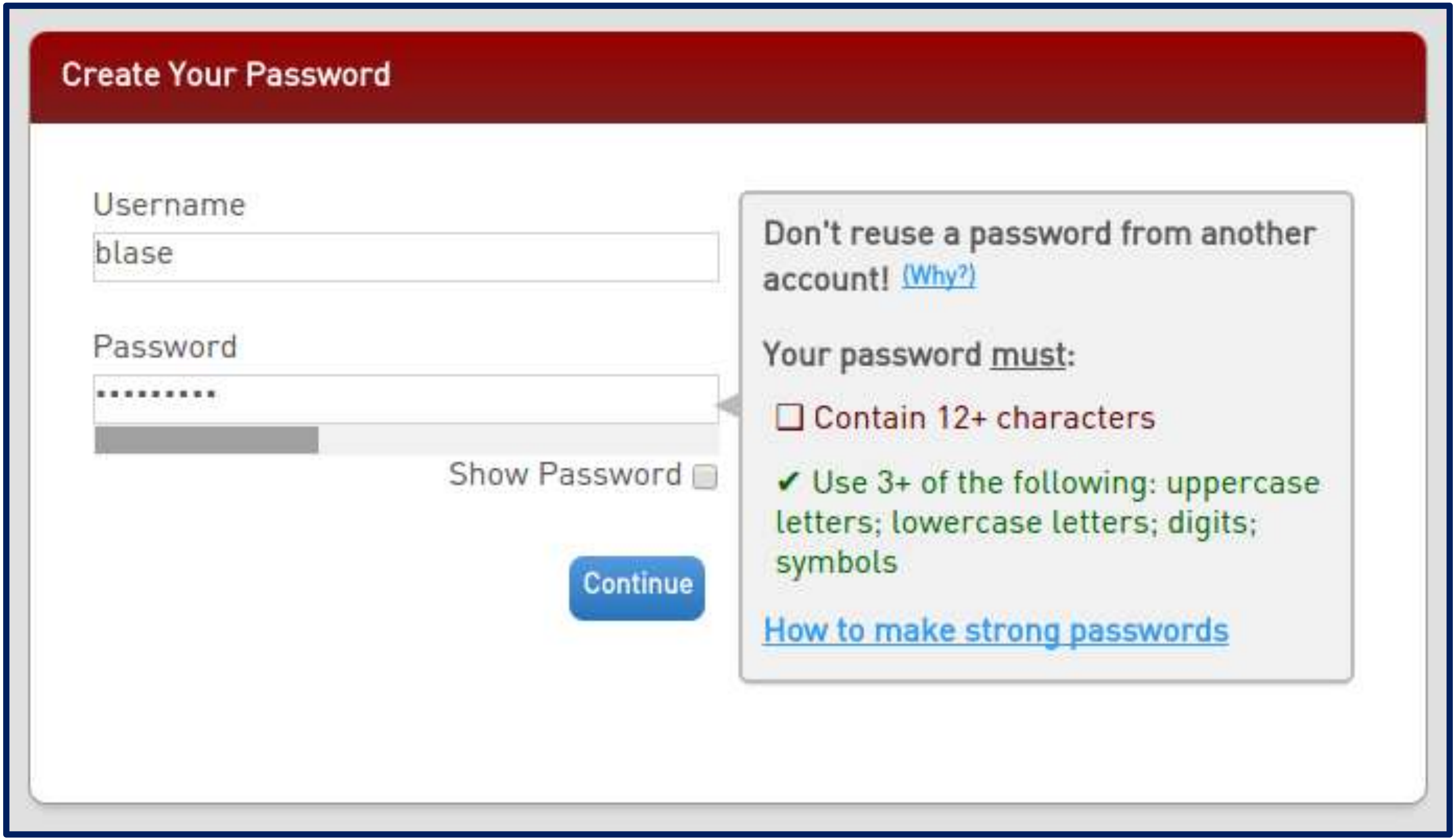
- 21 characteristics
- Weightings determined with regression

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 □

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

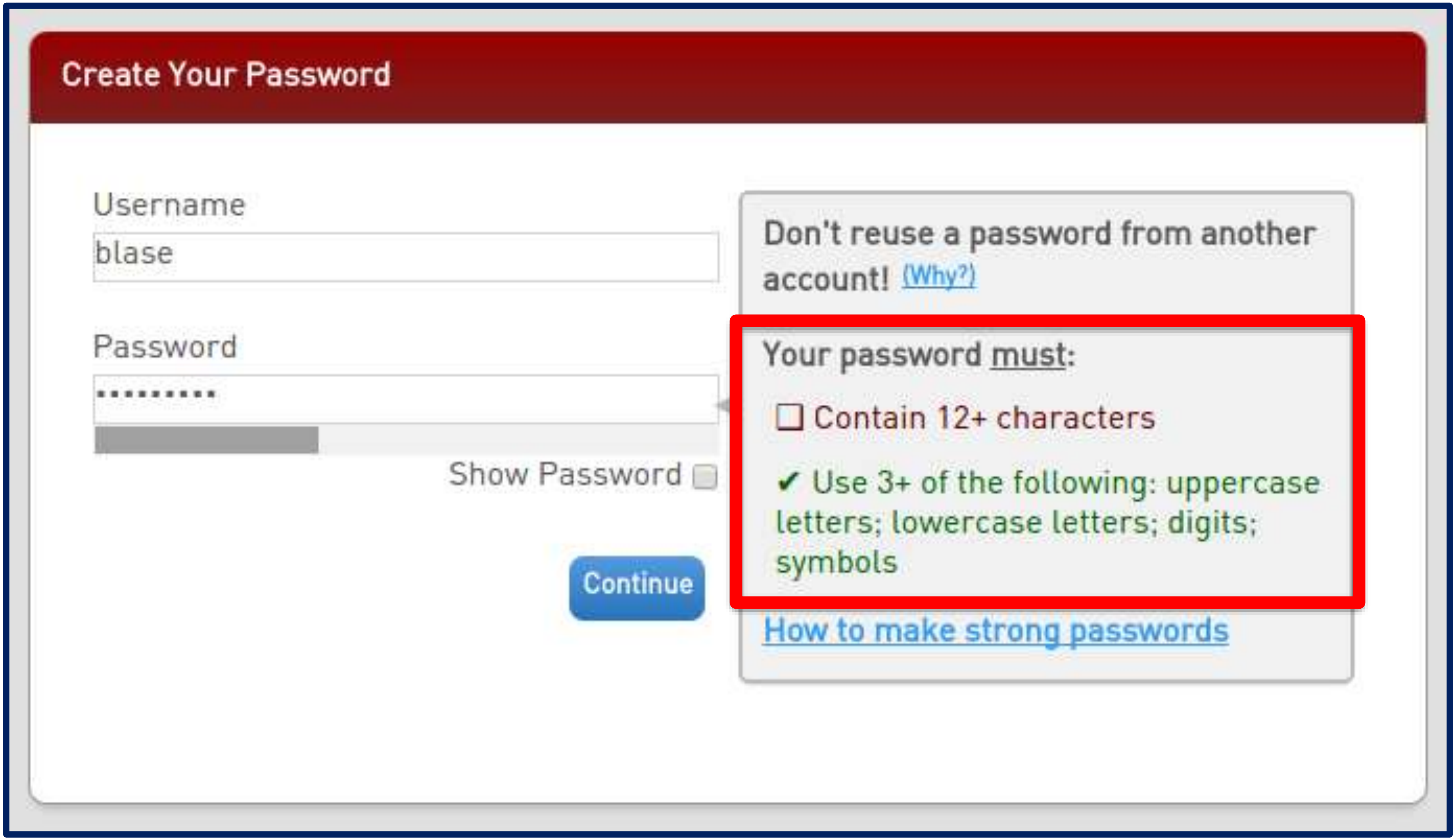
Your password must:

□ 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?)

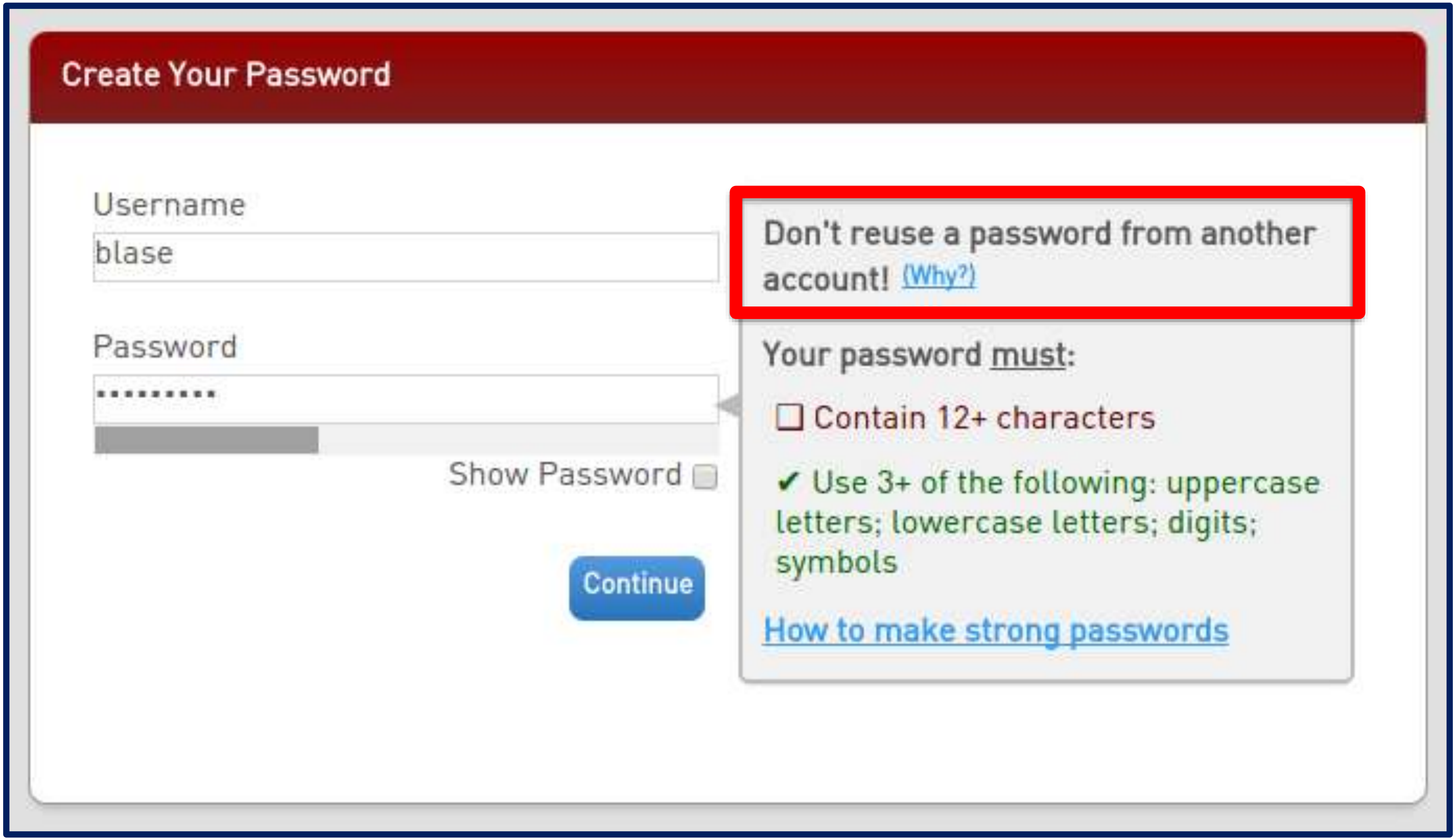
Your password must:

□ 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

••••••••••

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

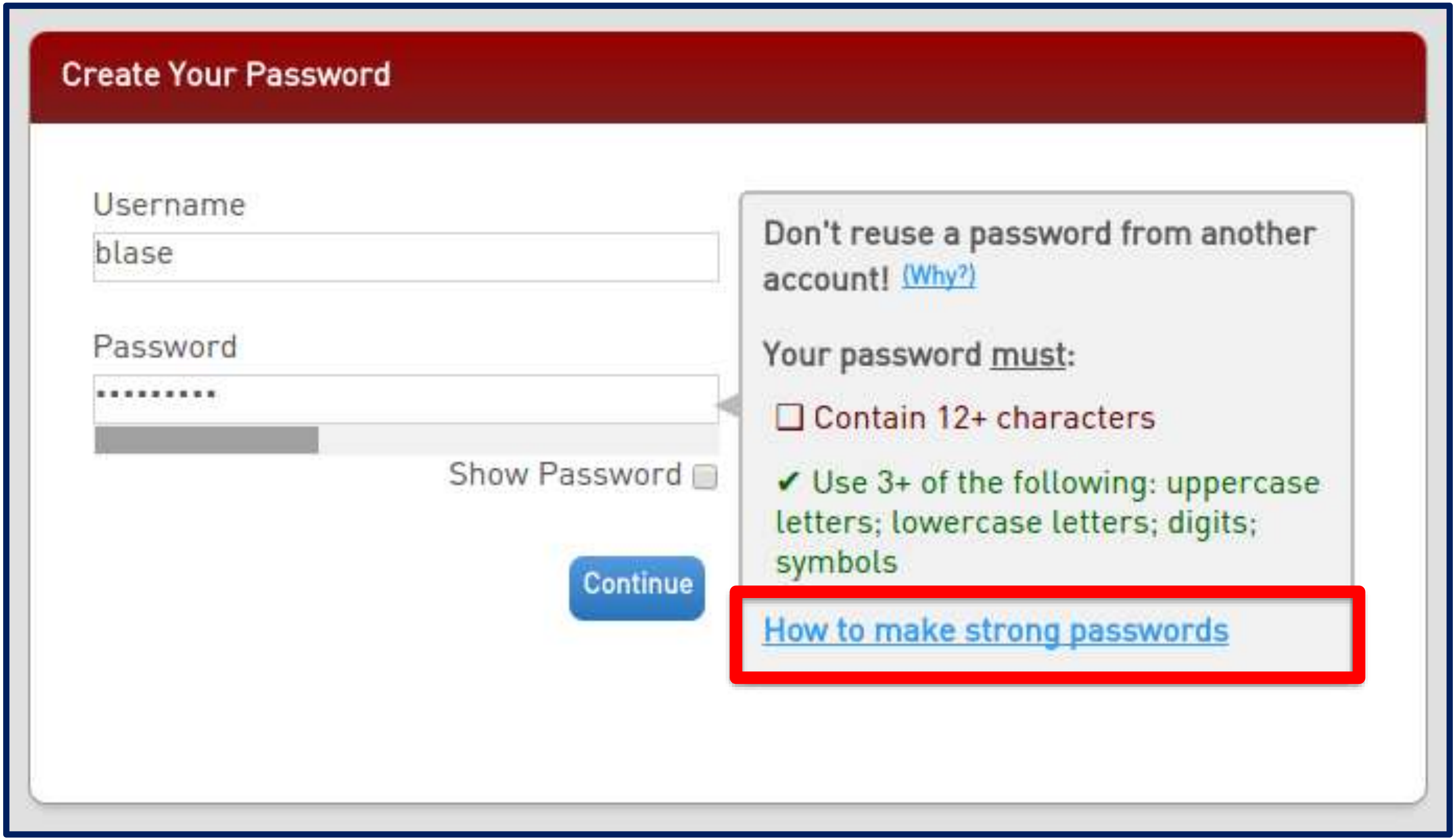
Your password must:

☐ 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

••••••••••

Show Password □

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

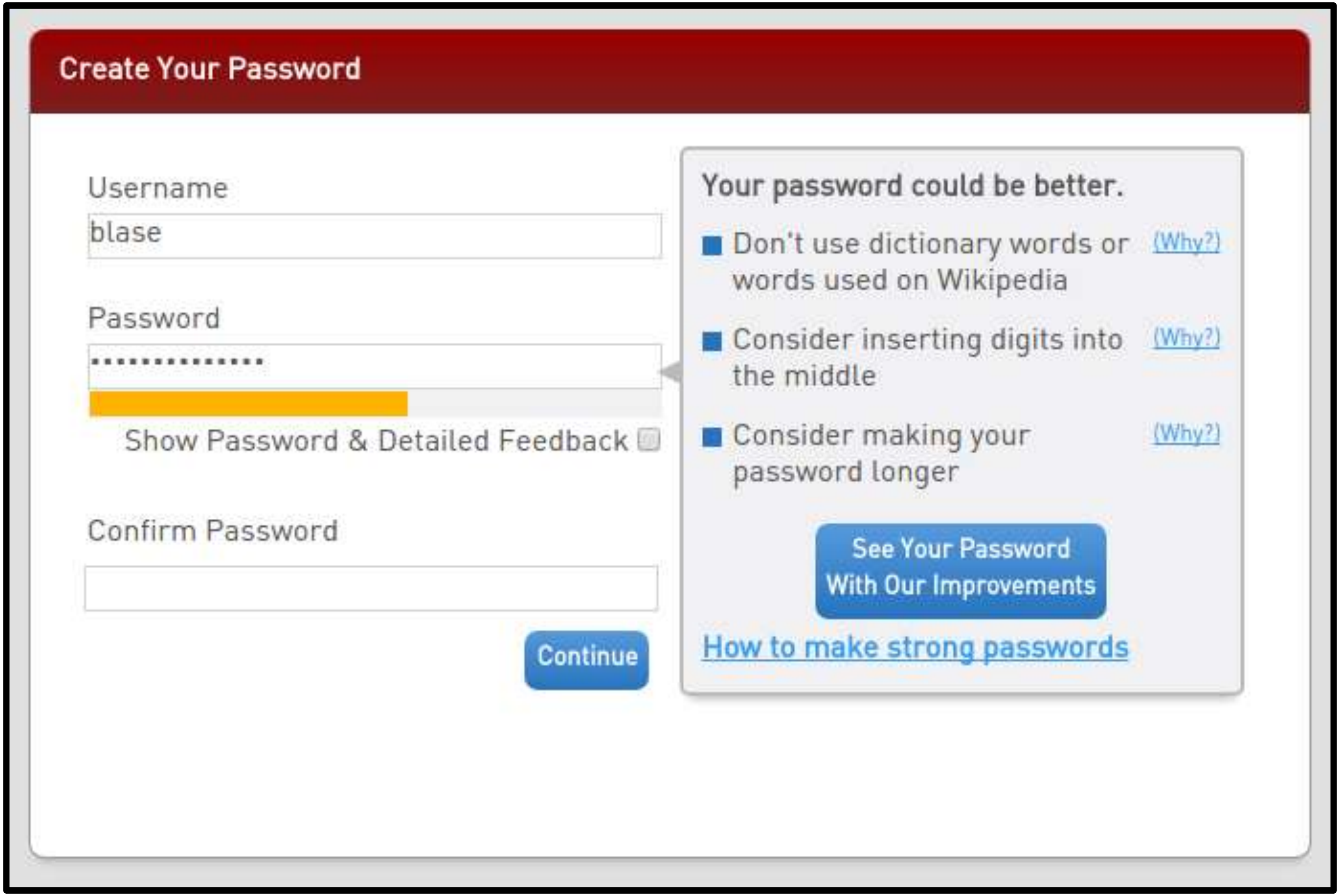
Your password must:

□ Contain 12+ characters

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

How to make strong passwords

After Requirements Are Met…



Create Your Password

Username

blase

Password

••••••••••••••

Show Password & Detailed Feedback □

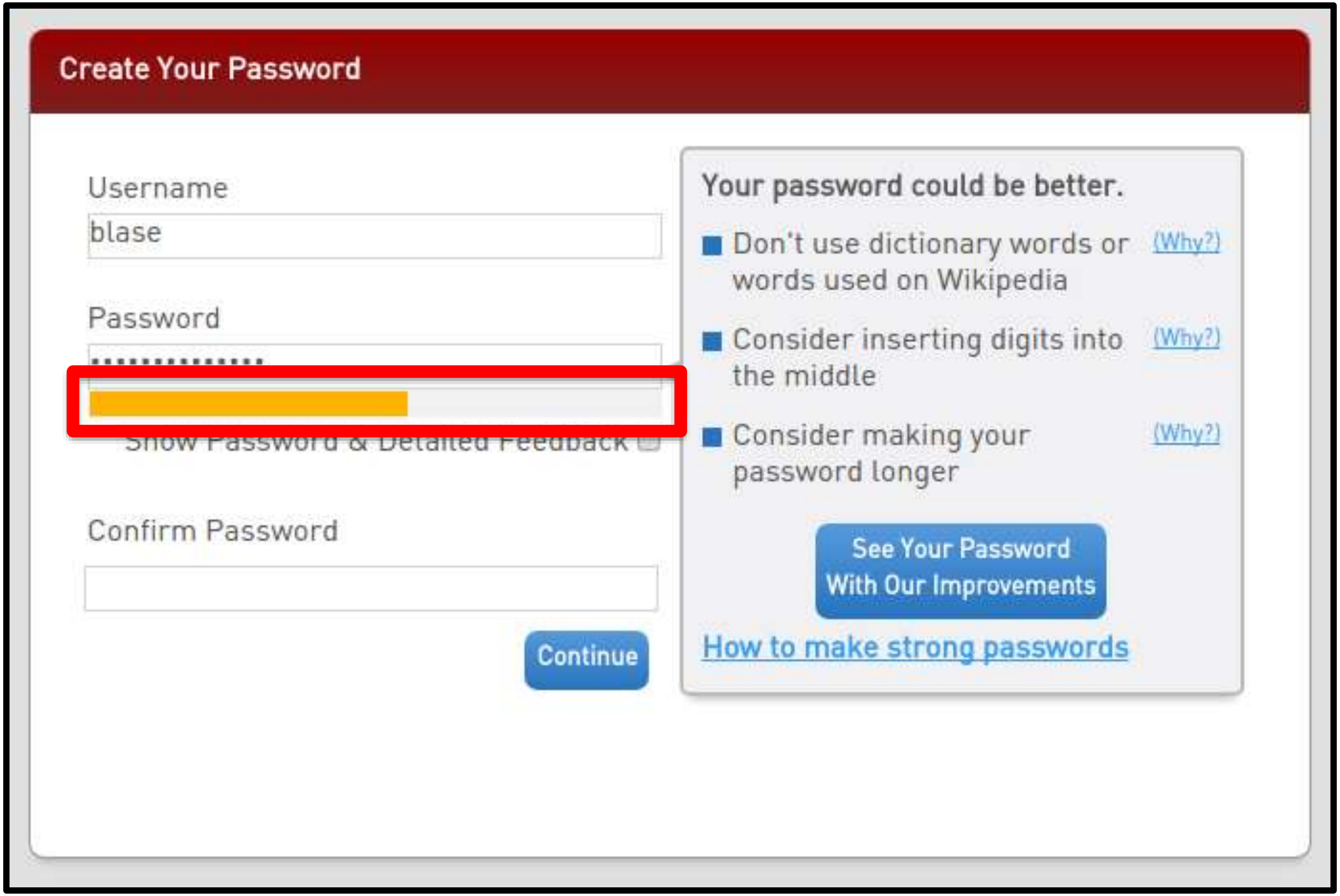
Confirm Password

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

…Displays Score Visually



Create Your Password

Username

blase

Password

•••••••••••••••

Show Password & Detailed Feedback □

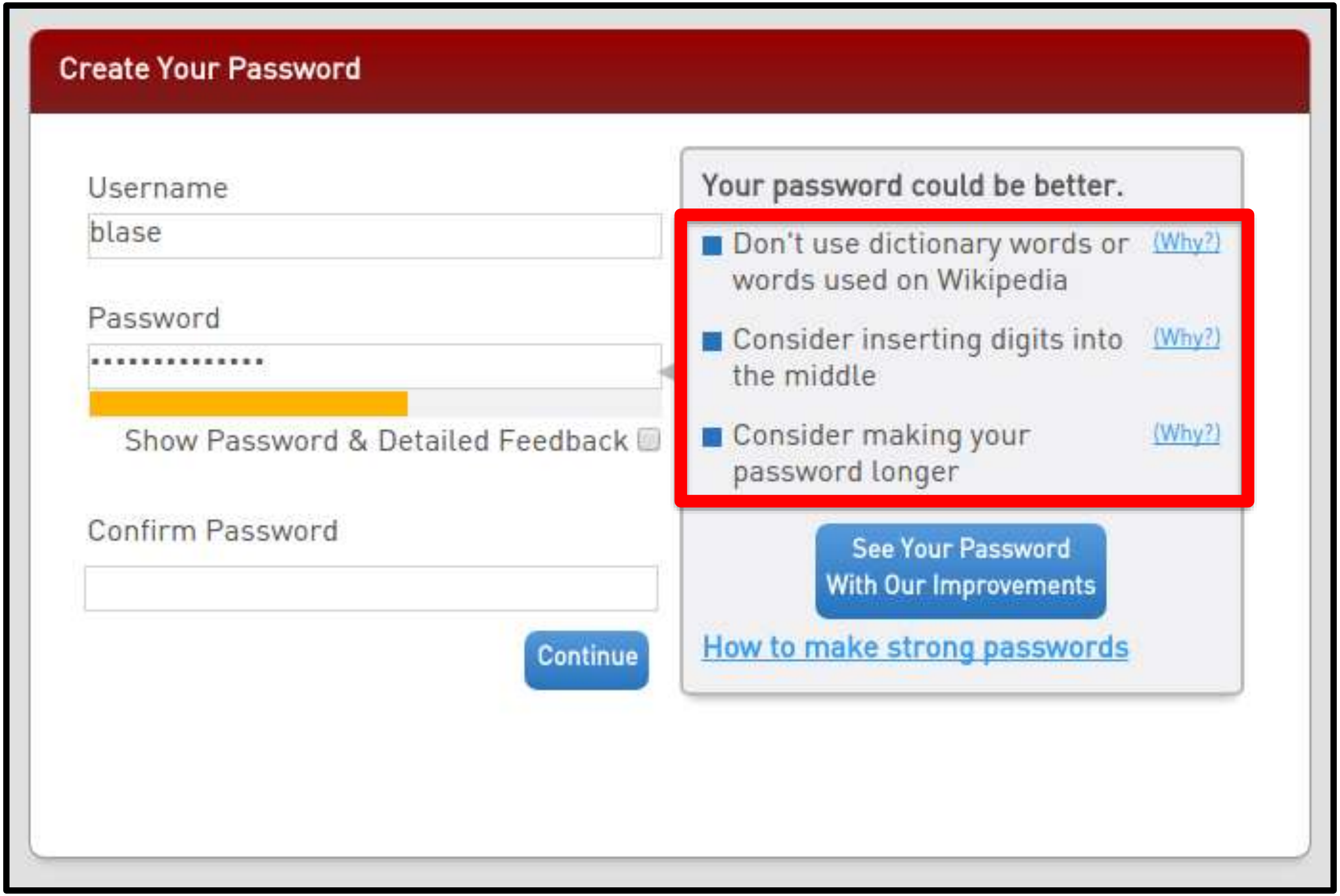
Confirm Password

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 □

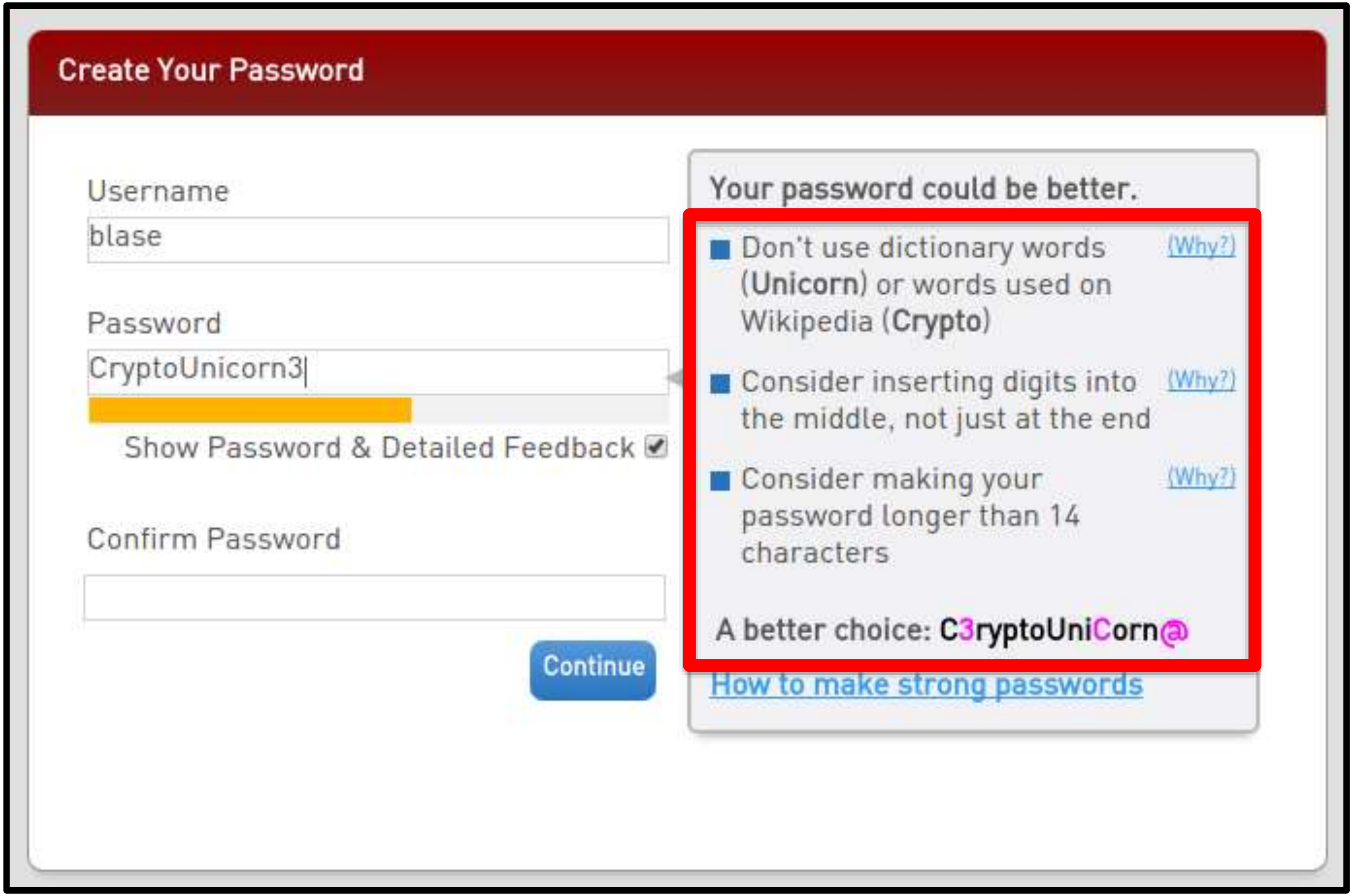
Confirm Password

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

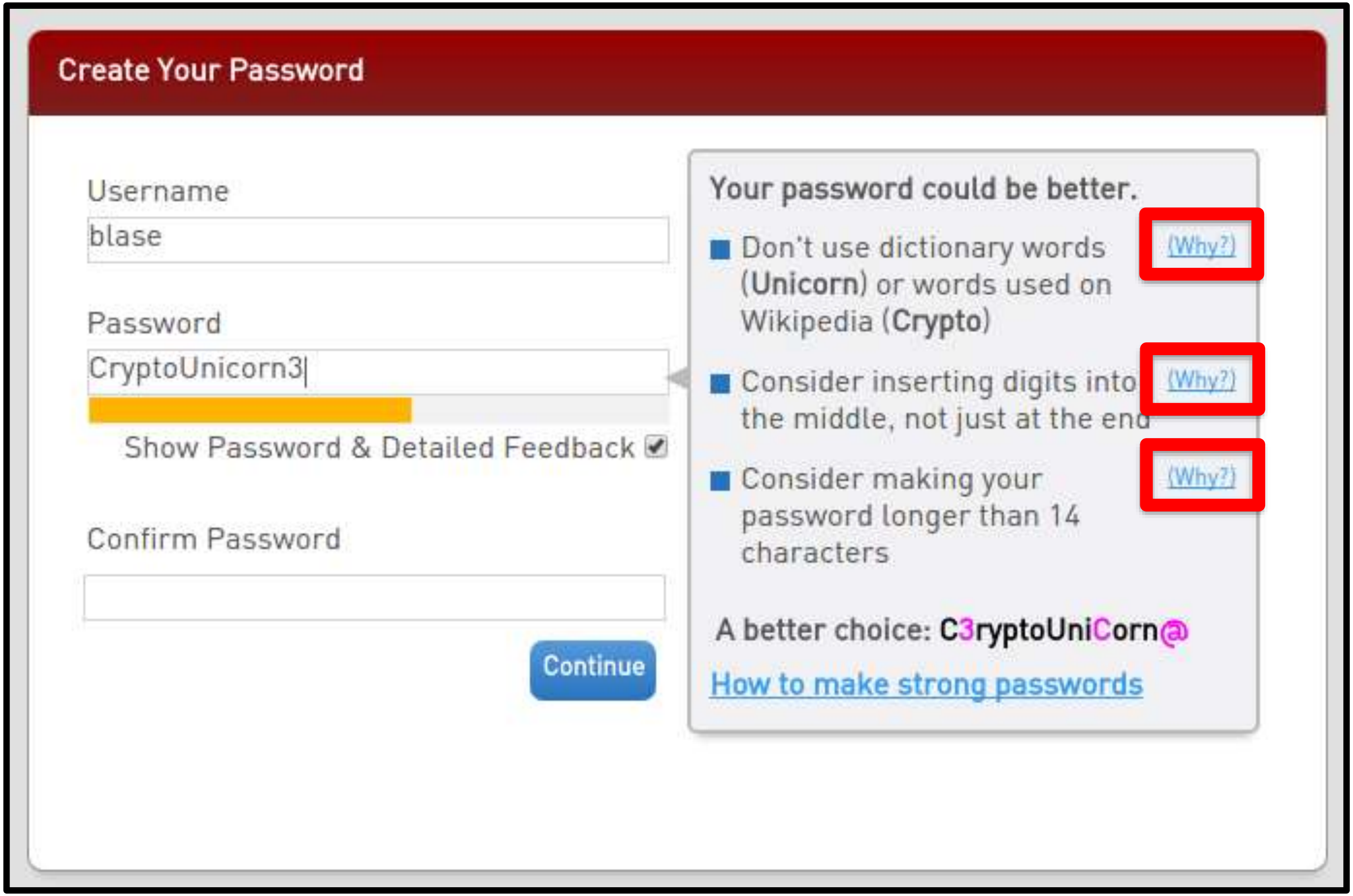
Your password could be better.

- 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

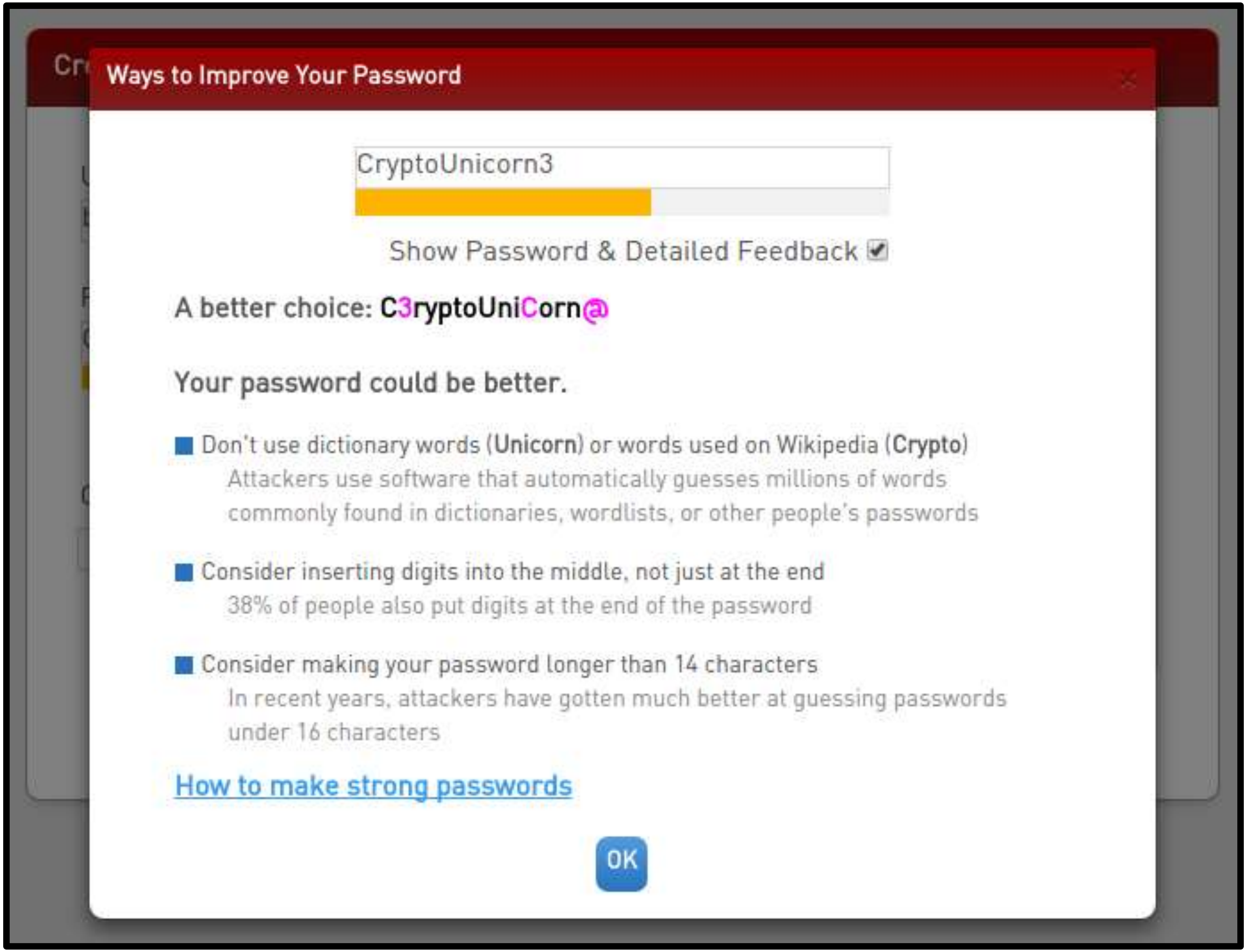
Your password could be better.

- 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



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
```

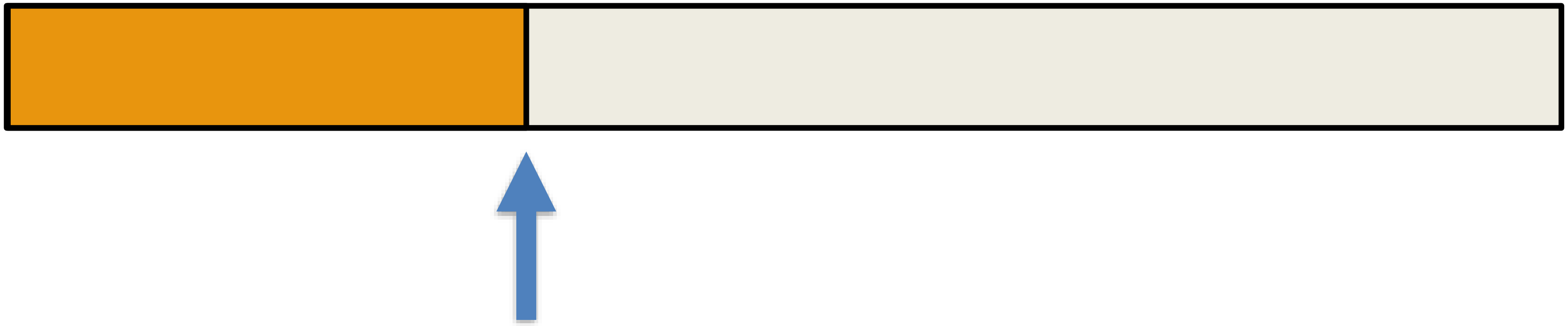
- 12+ characters, 3+ classes (3class12)

```
Password1234
```

Dimension 2: Stringency

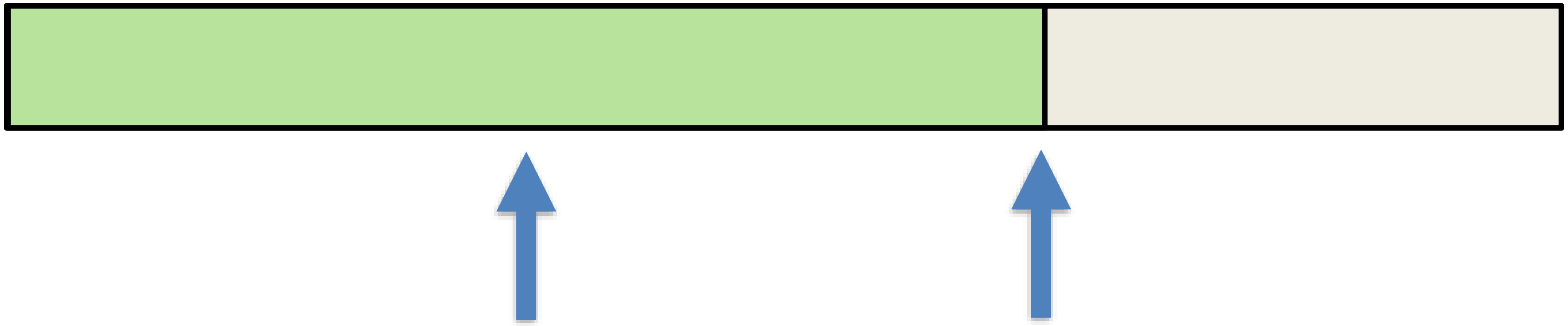
- Low
- Medium
- High

Dimension 2: Stringency



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

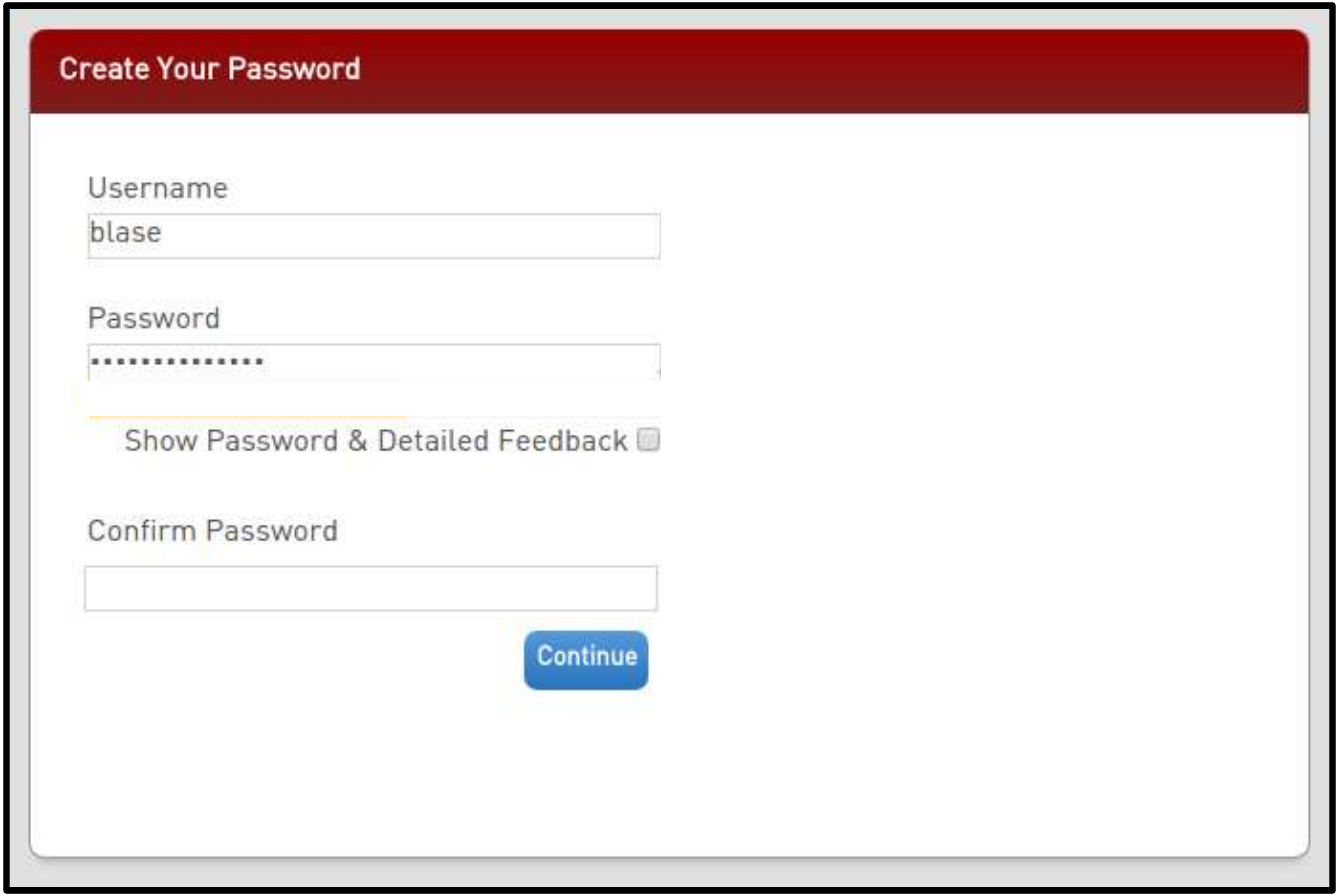
Dimension 2: Stringency



• 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

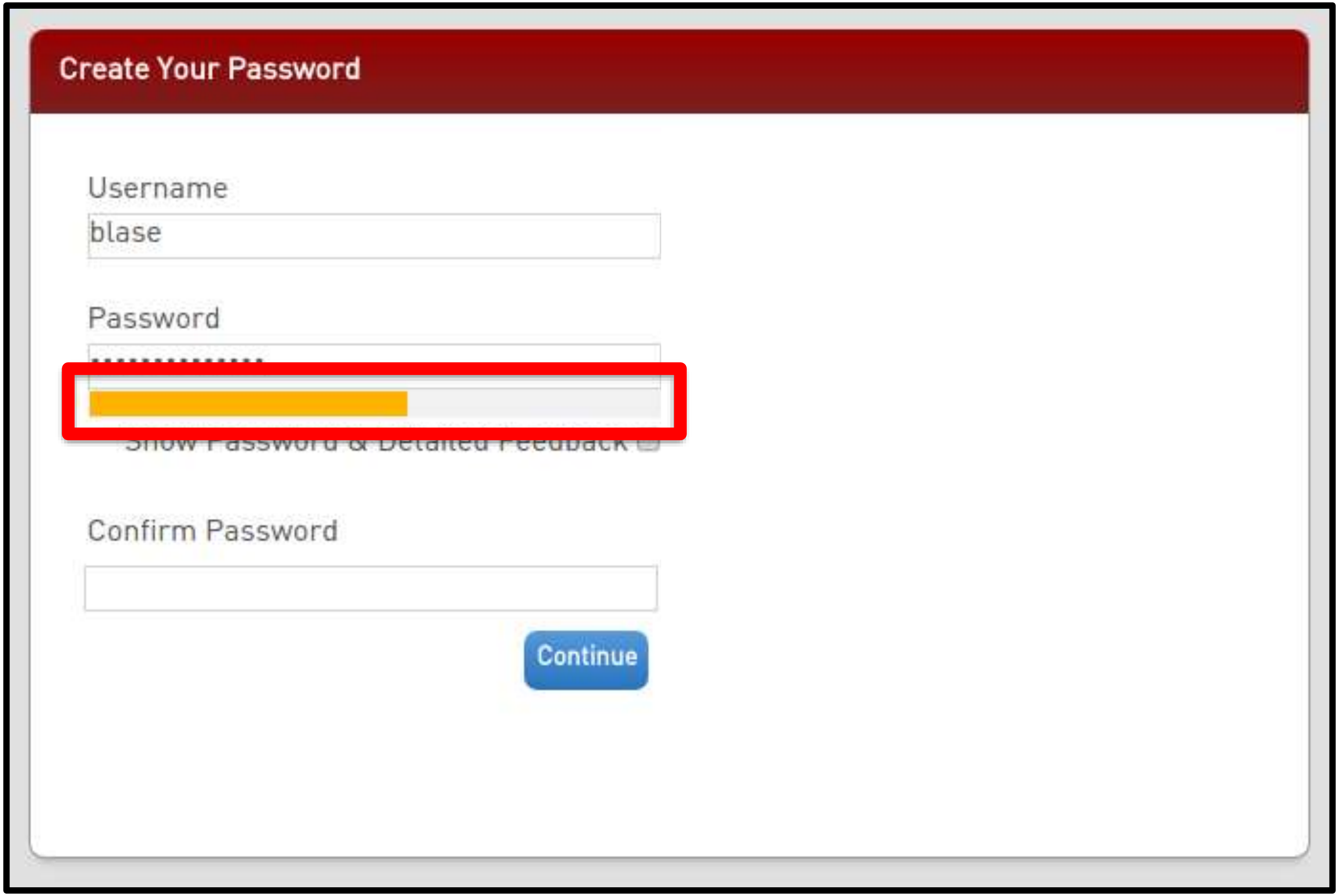
Password

••••••••••••••

Show Password & Detailed Feedback □

Confirm Password

Bar Only



Create Your Password

Username

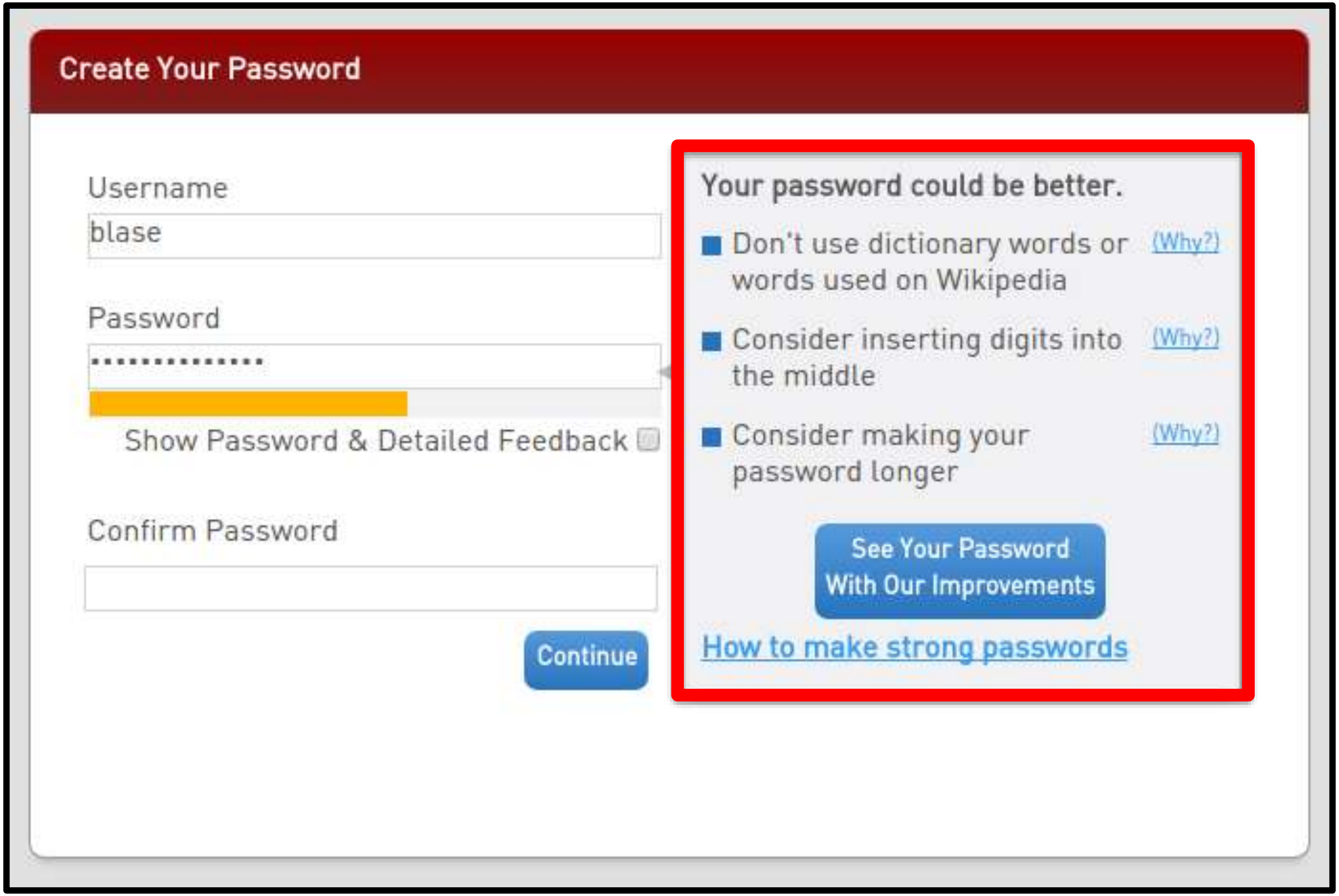
blase

Password

Show Password & Detailed Feedback □

Confirm Password

Public (Non-Sensitive) Feedback



Create Your Password

Username

blase

Password

••••••••••••••

Show Password & Detailed Feedback □

Confirm Password

Continue

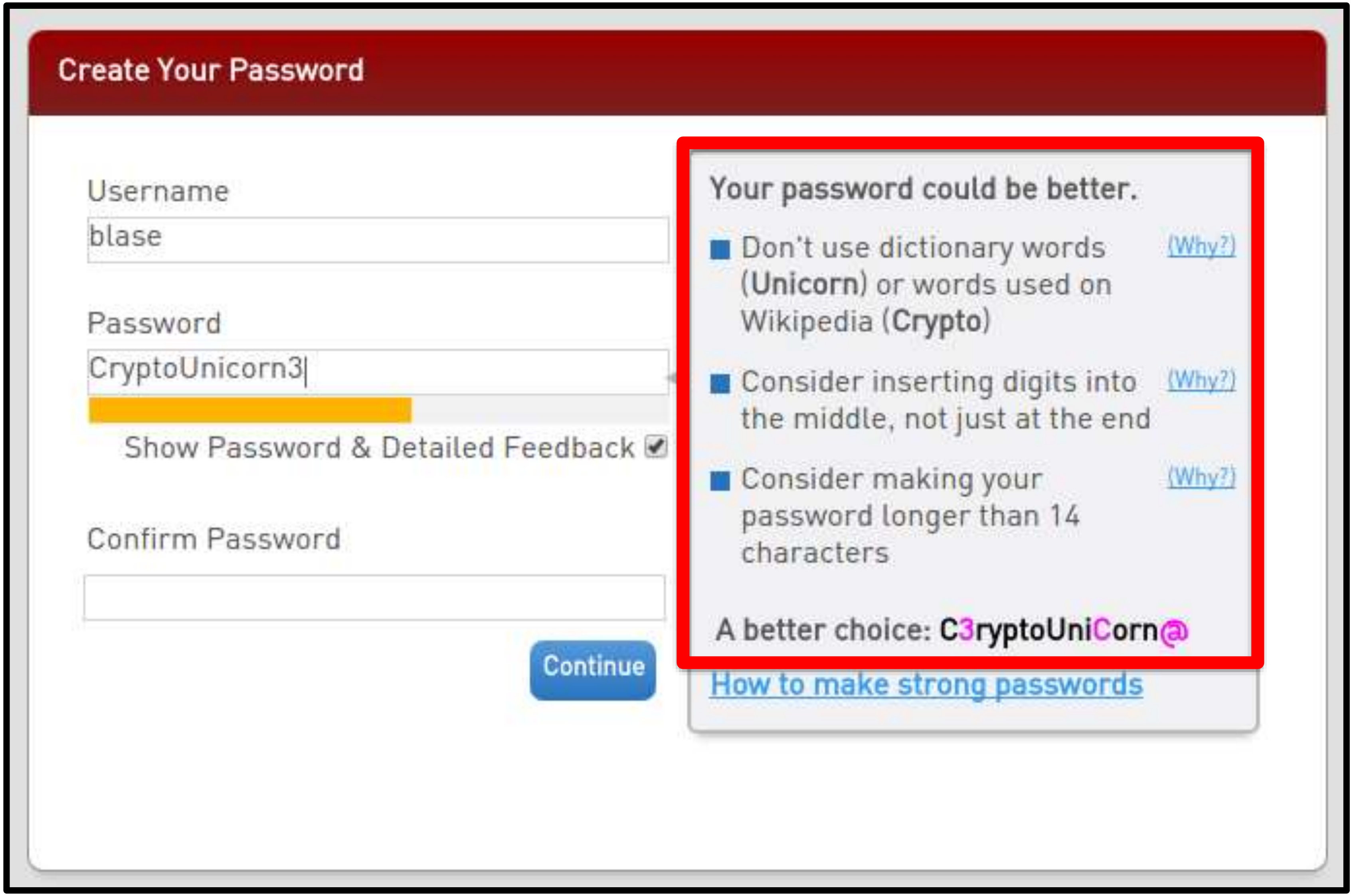
Your password could be better.

- 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

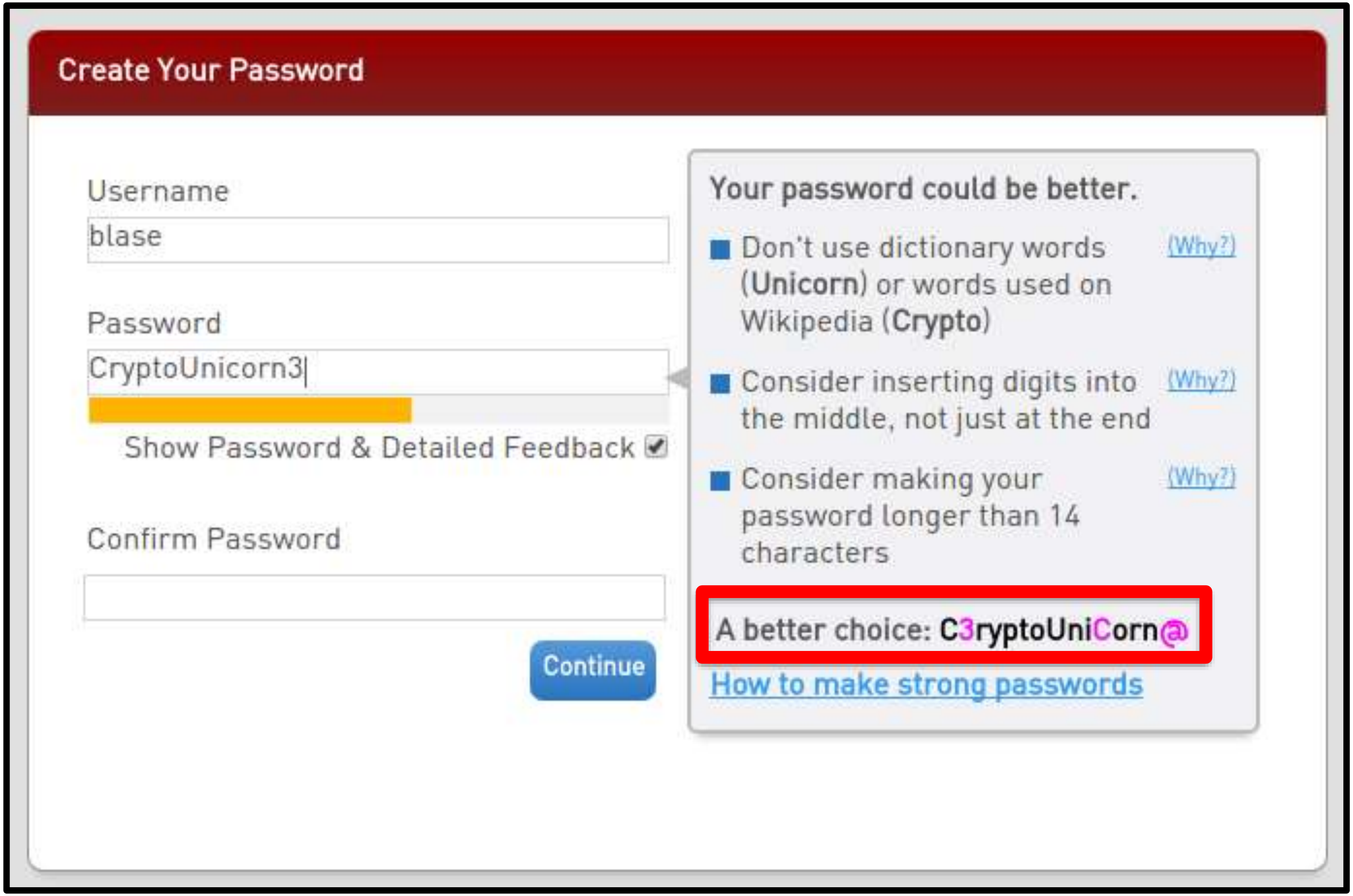
Your password could be better.

- 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



Username

blase

Password

CryptoUnicorn3

Show Password & Detailed Feedback ☑

Confirm Password

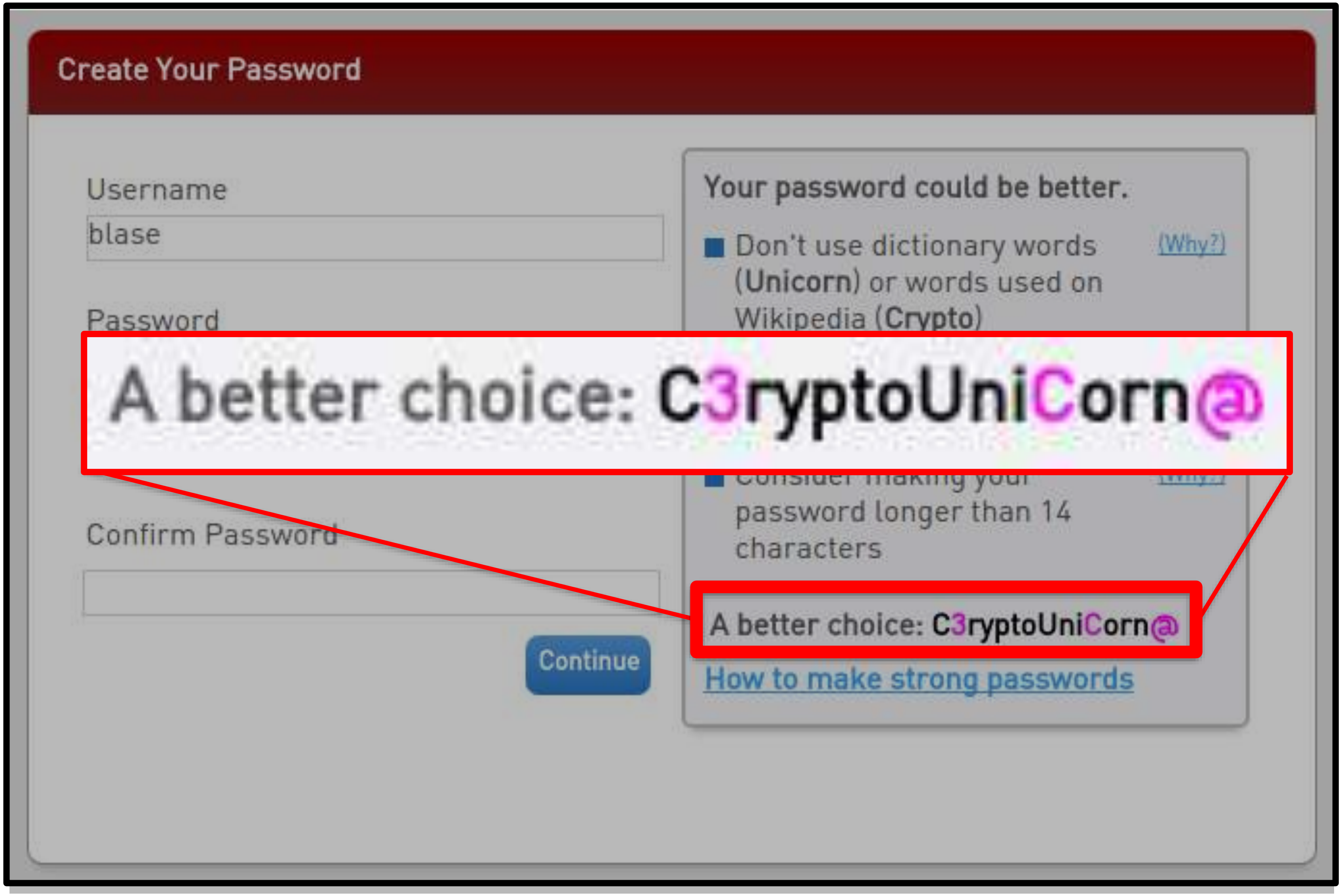
Your password could be better.

- 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

Confirm Password

Your password could be better.

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

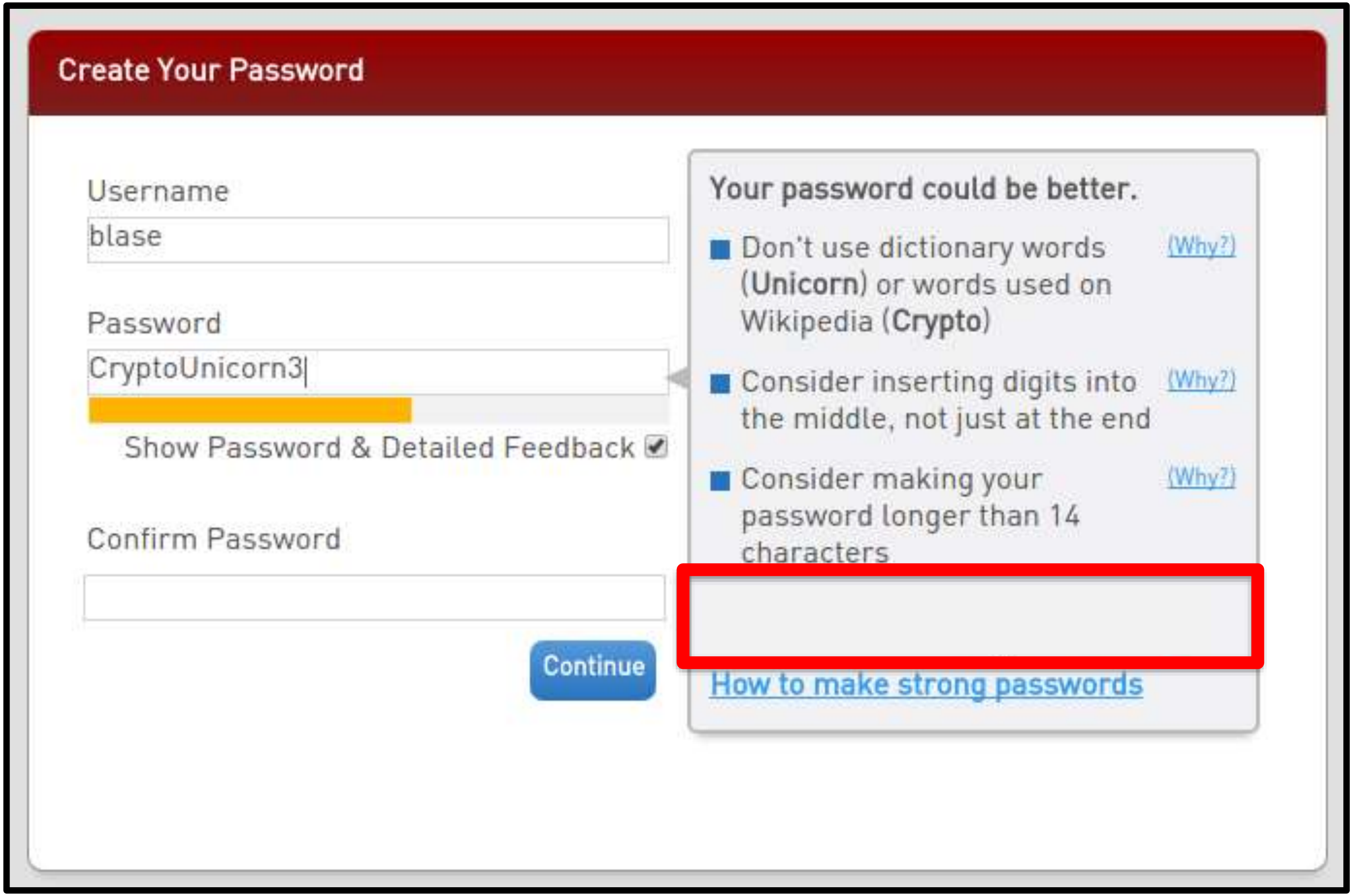
- Consider making your password longer than 14 characters

A better choice: C3ryptoUniCorn@

A better choice: C3ryptoUniCorn@

How to make strong passwords

Standard, No Suggested Improvement



Create Your Password

Username

blase

Password

CryptoUnicorn3

Show Password & Detailed Feedback ☑

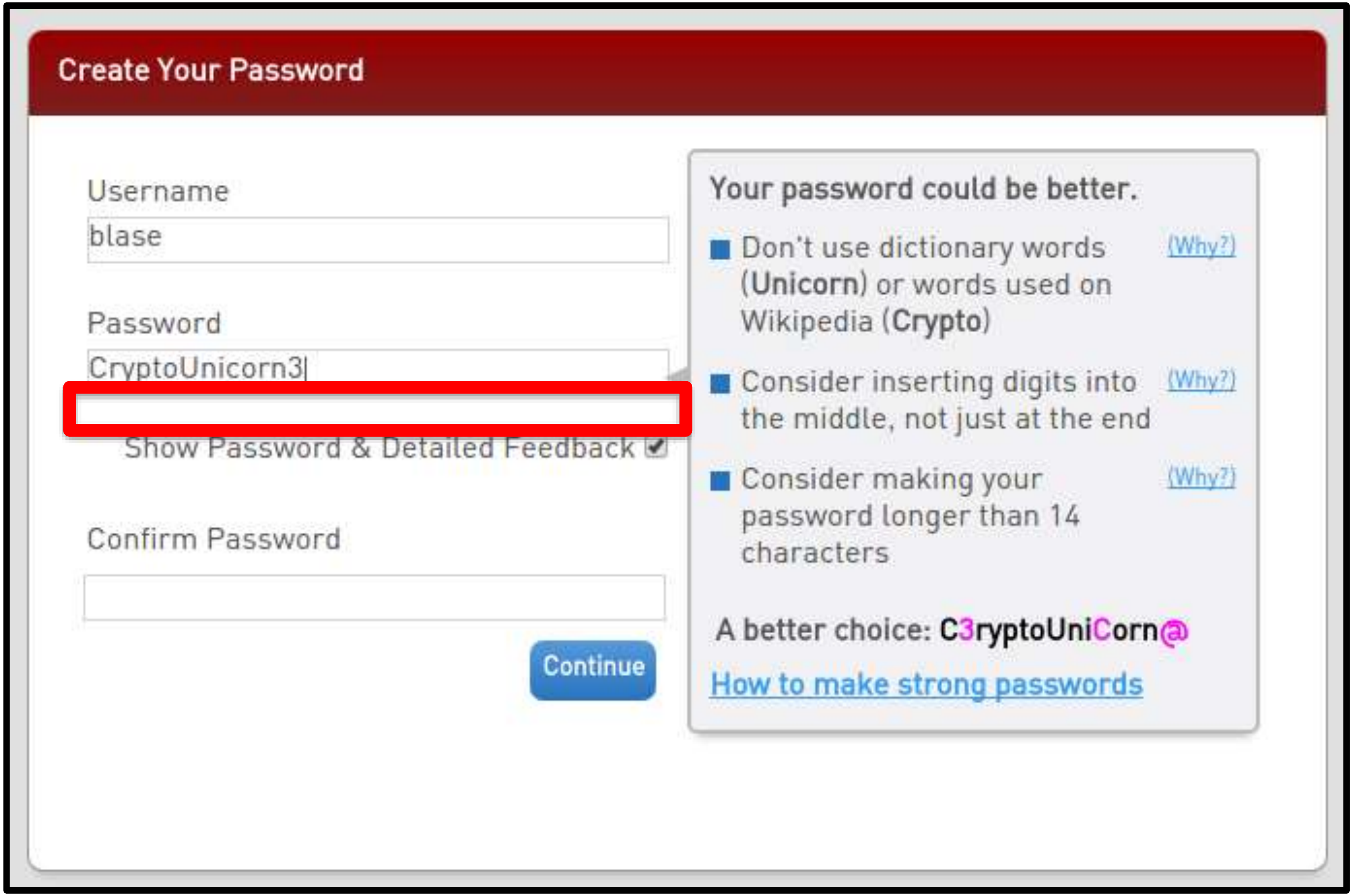
Confirm Password

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

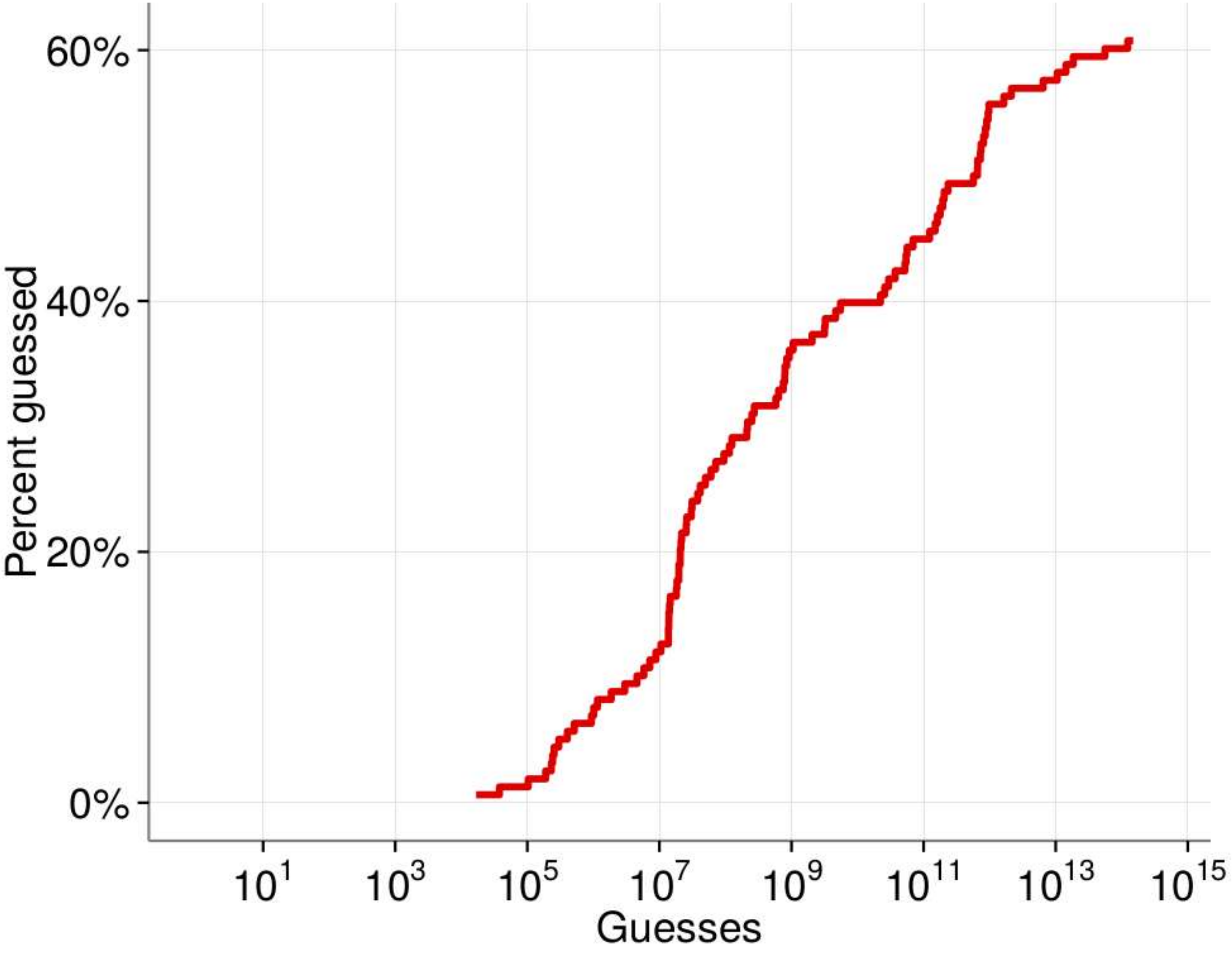
Your password could be better.

- 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?)

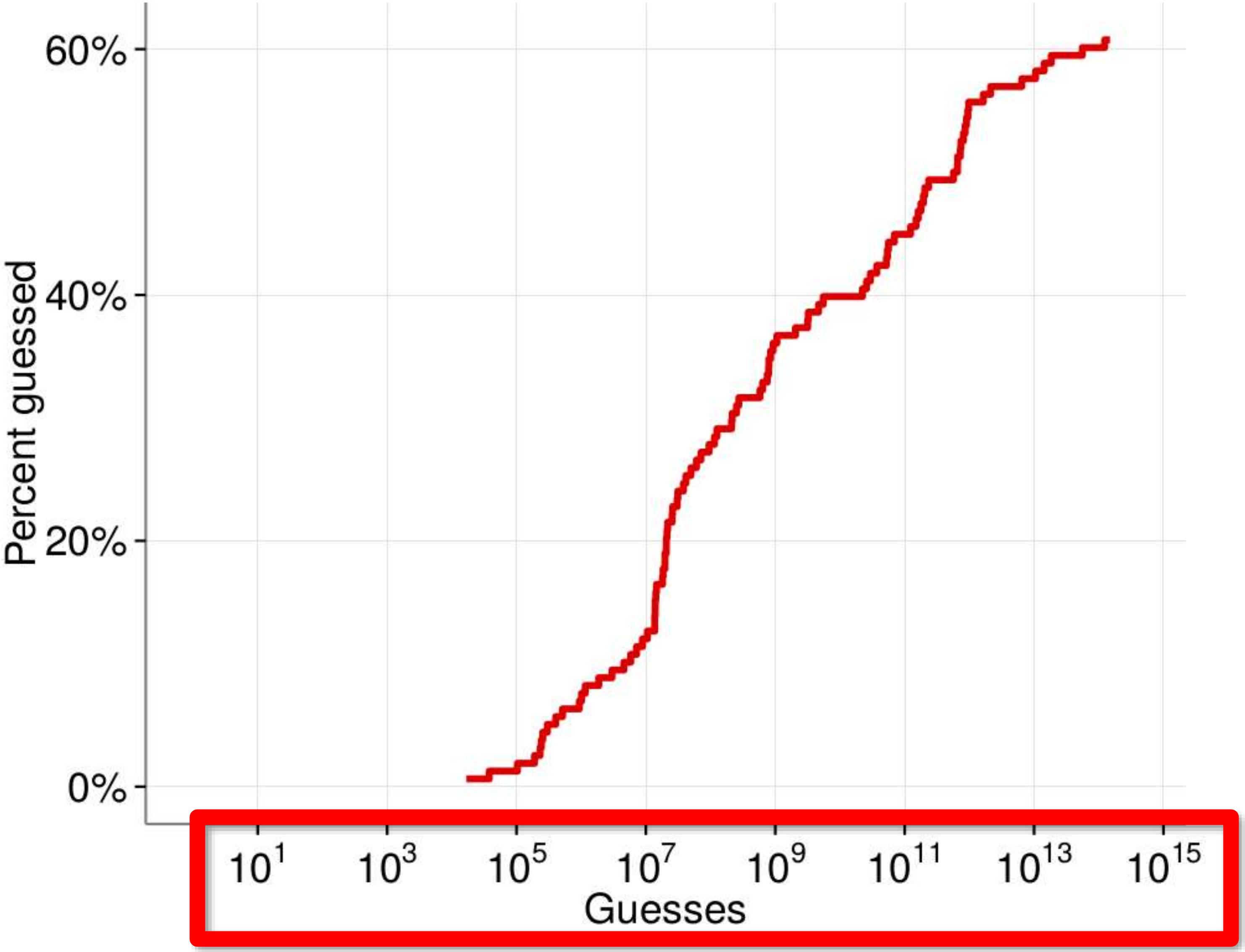
A better choice: **C3ryptoUniCorn@**

How to make strong passwords

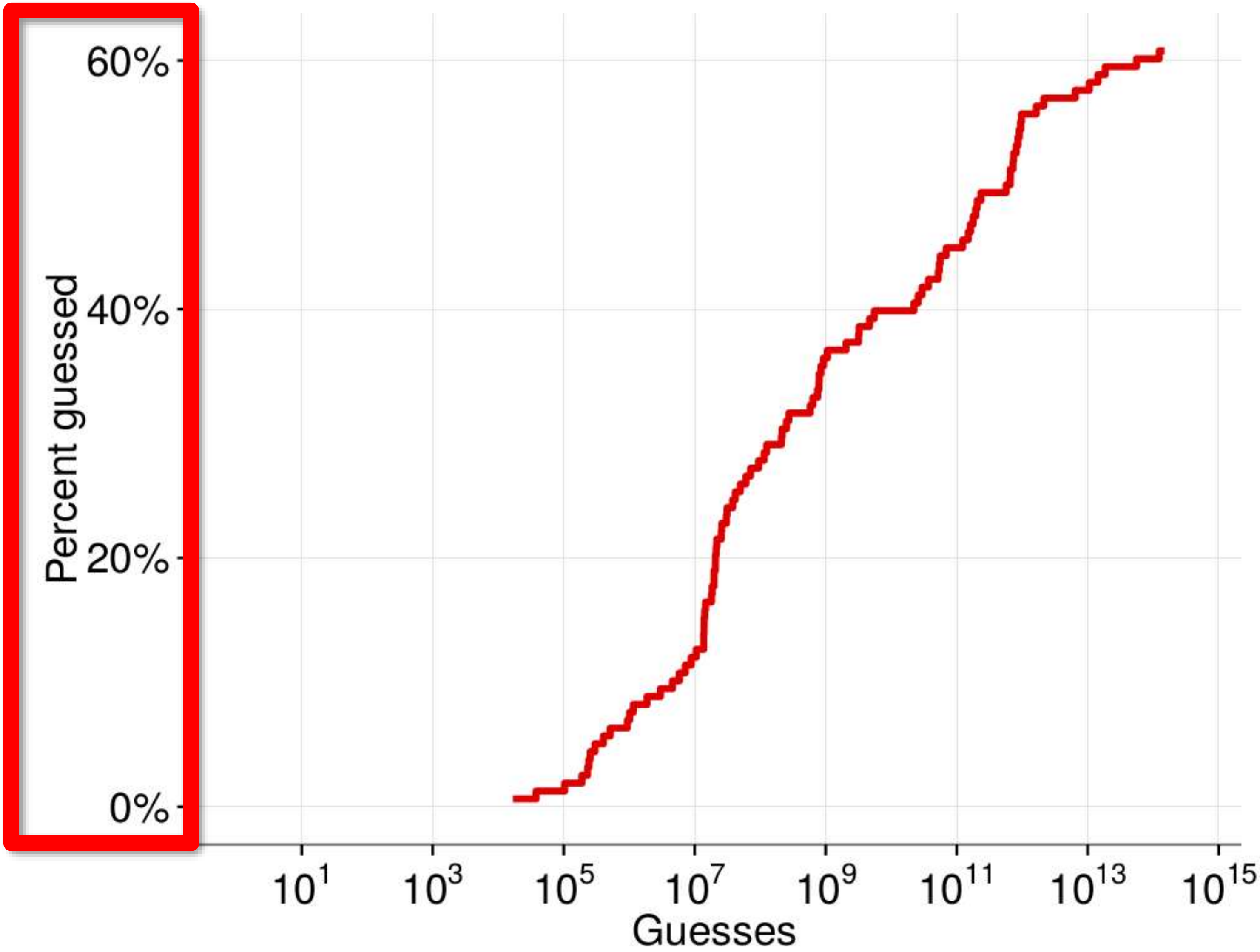
Measure Password Guessability



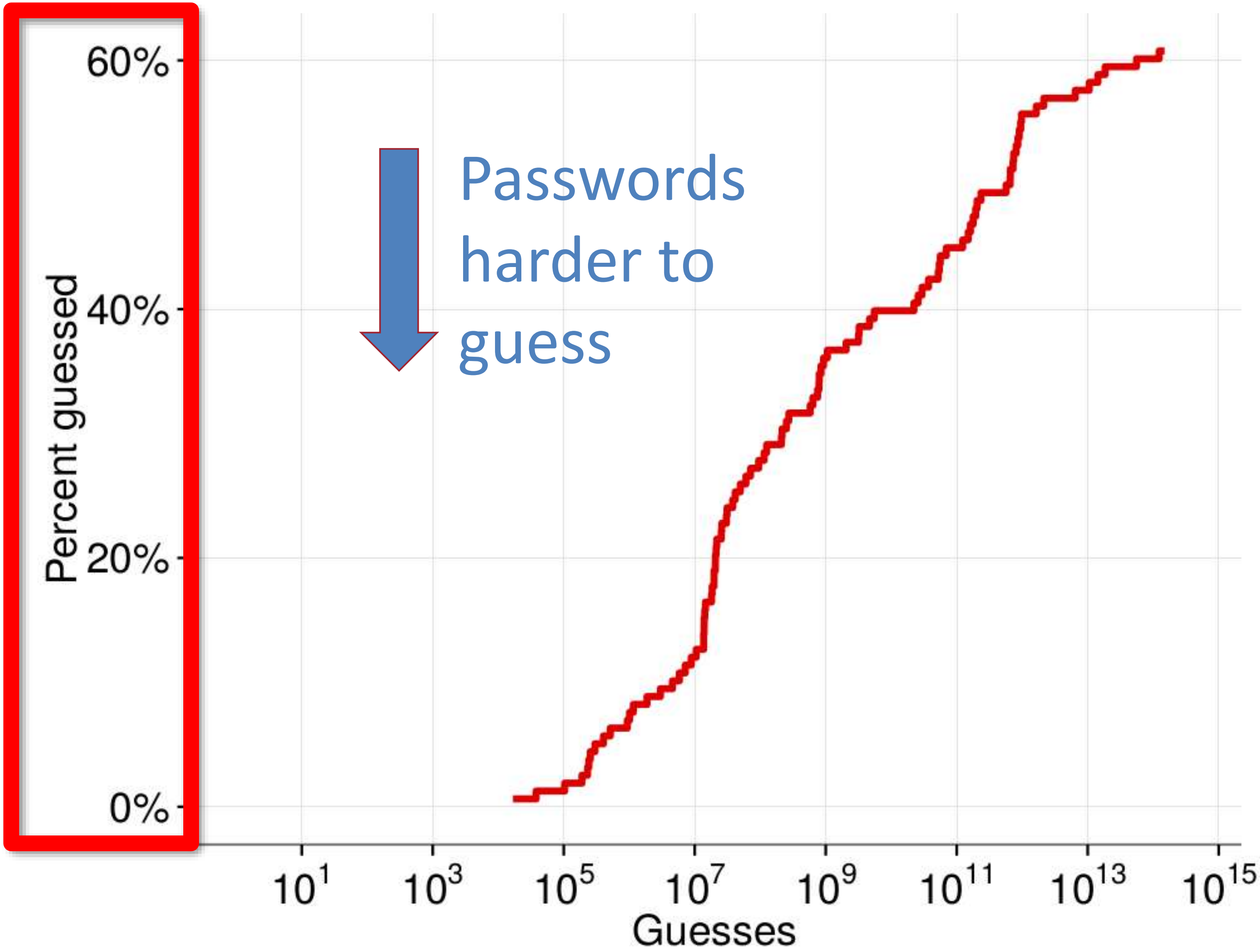
Measure Password Guessability



Measure Password Guessability

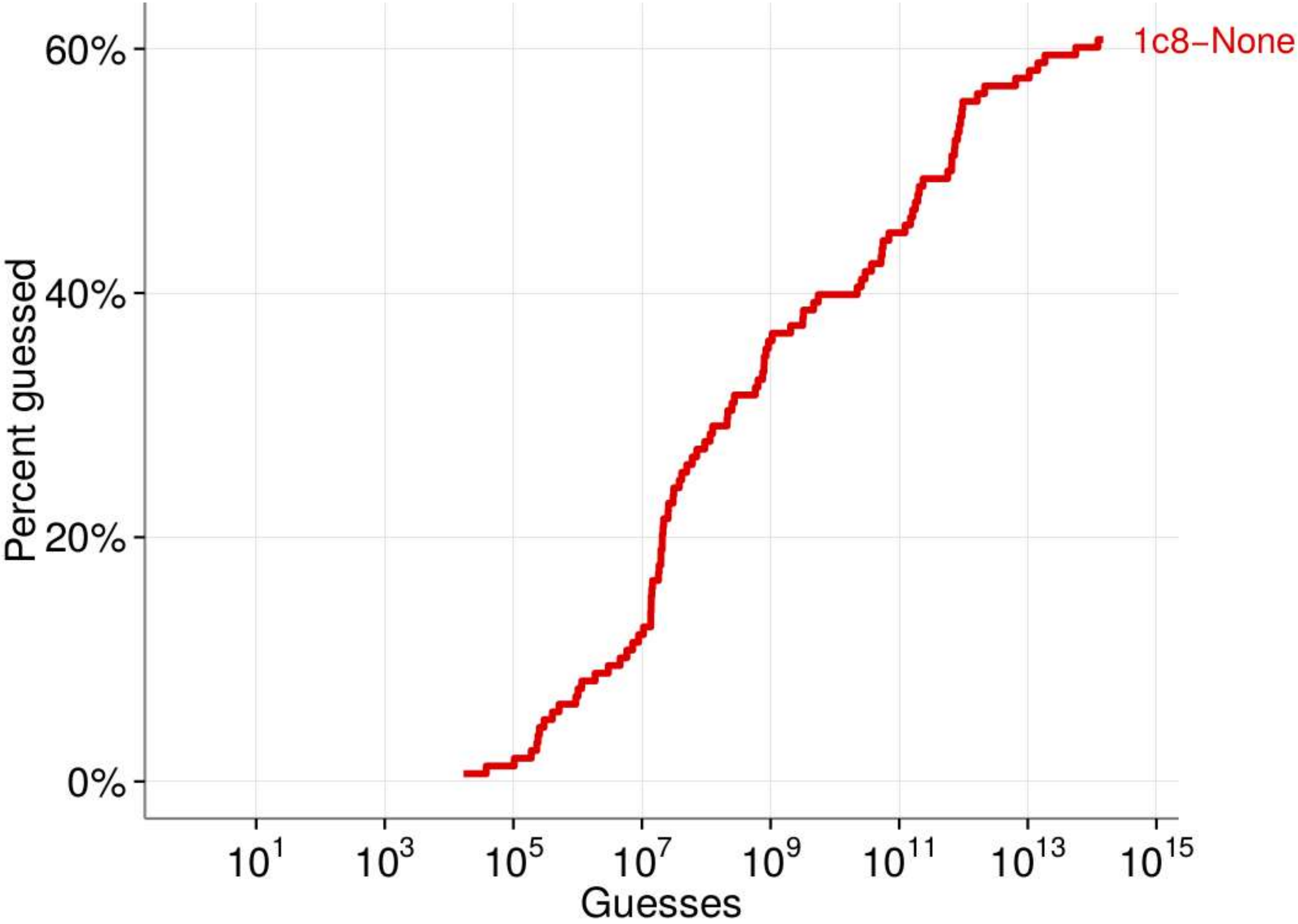


Measure Password Guessability

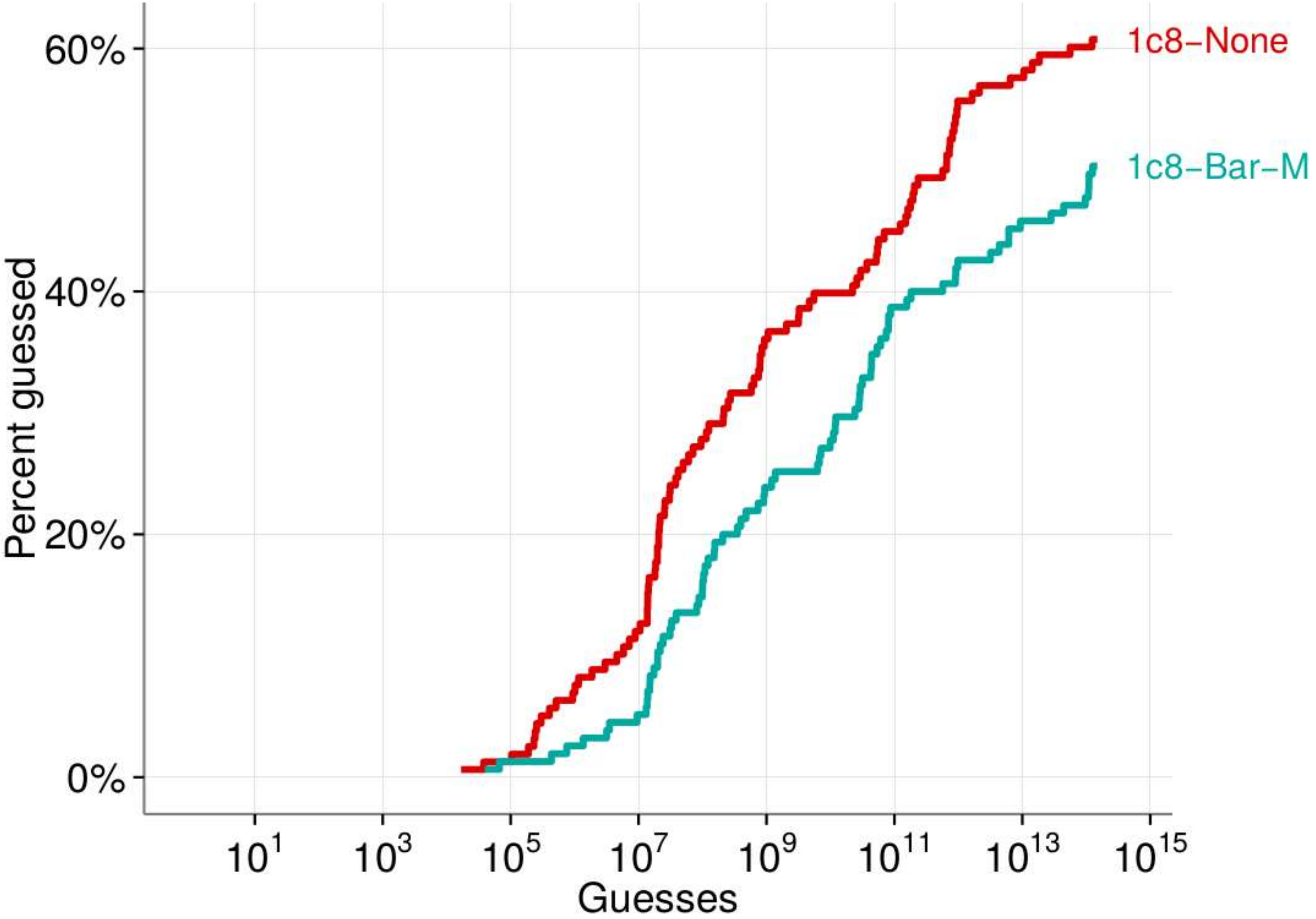


Passwords harder to guess

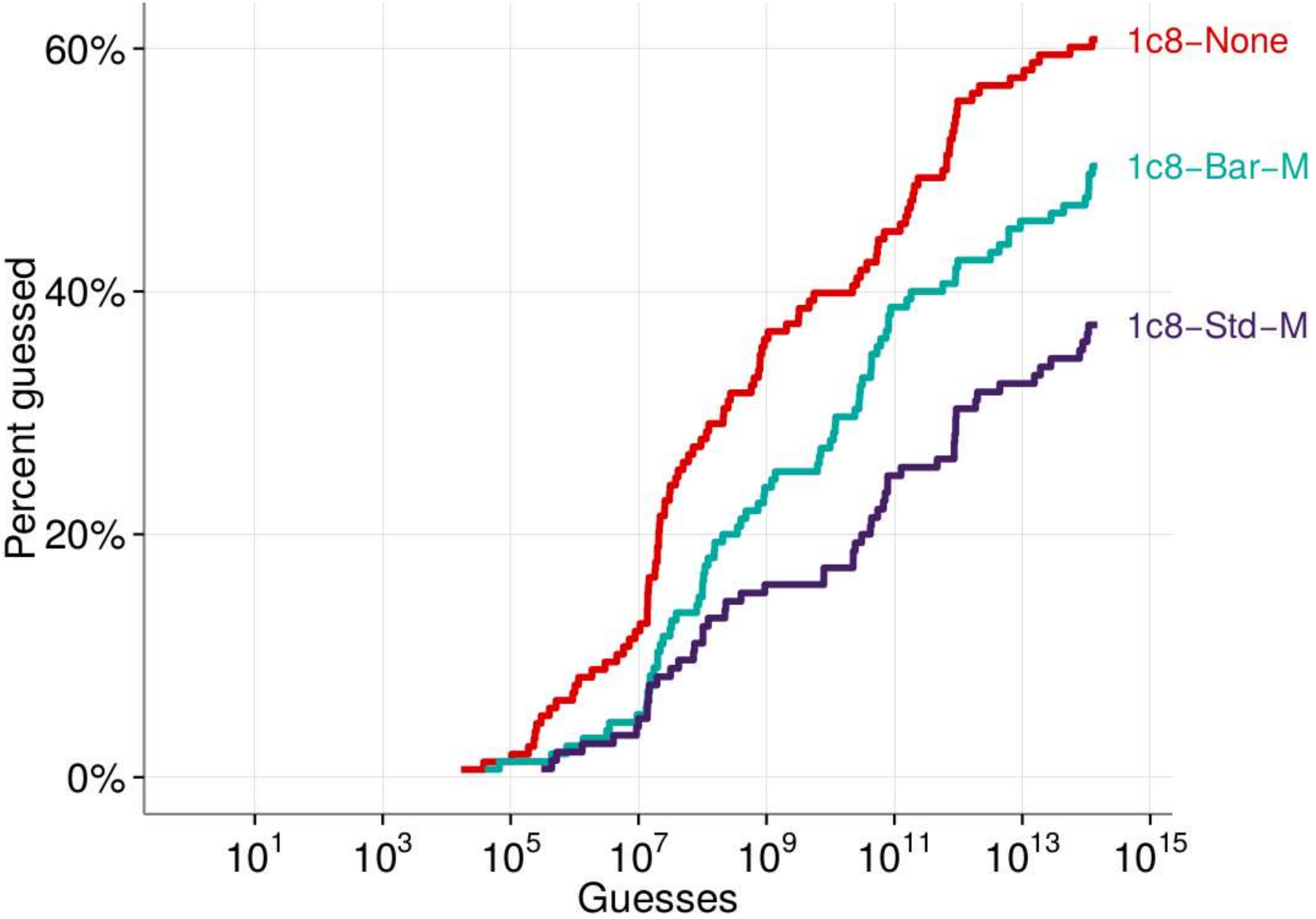
Measure Password Guessability



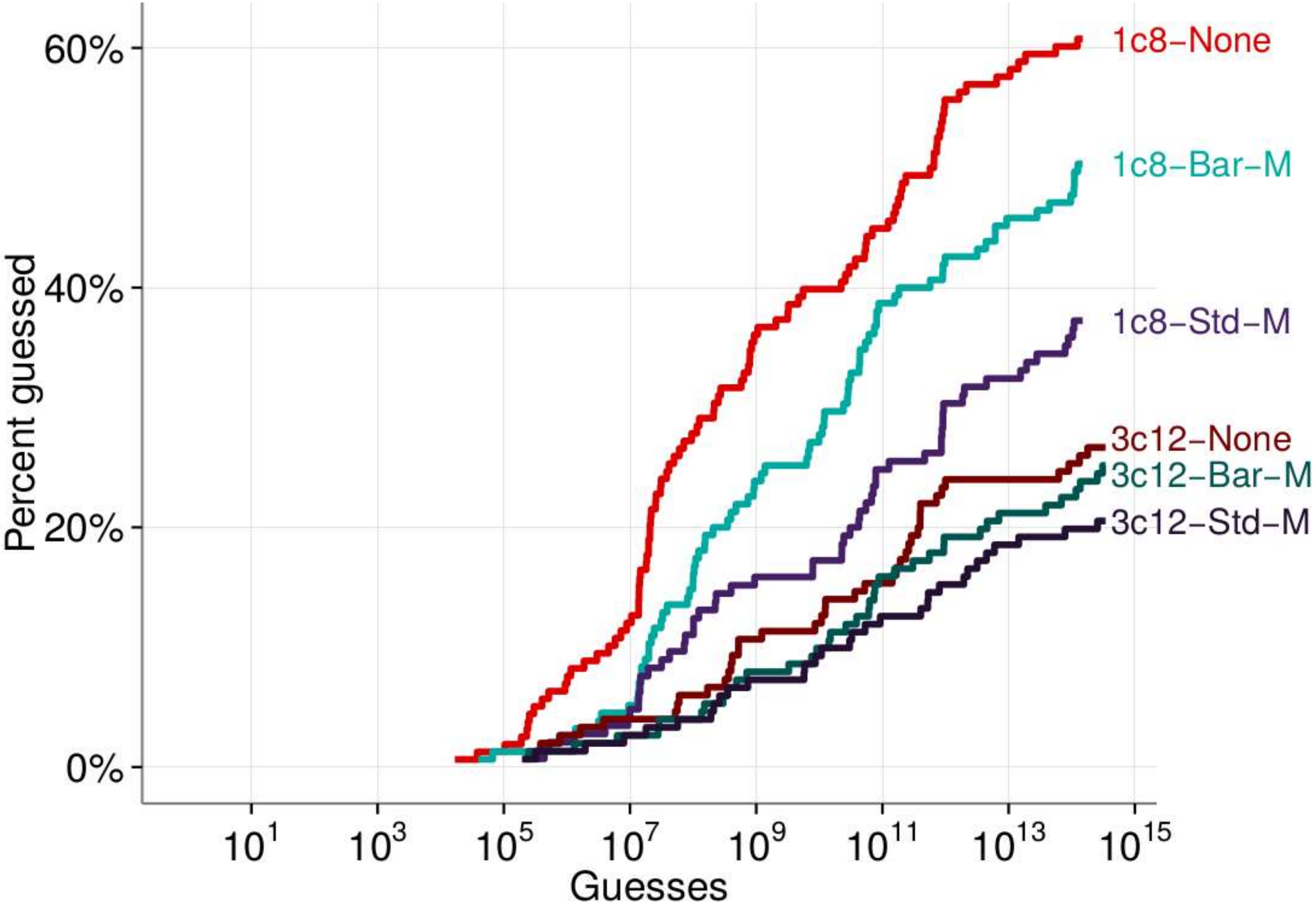
Feedback → More Secure Passwords



Feedback → More Secure Passwords



Feedback → More Secure Passwords



Usability Results

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

Feedback → More Secure Passwords

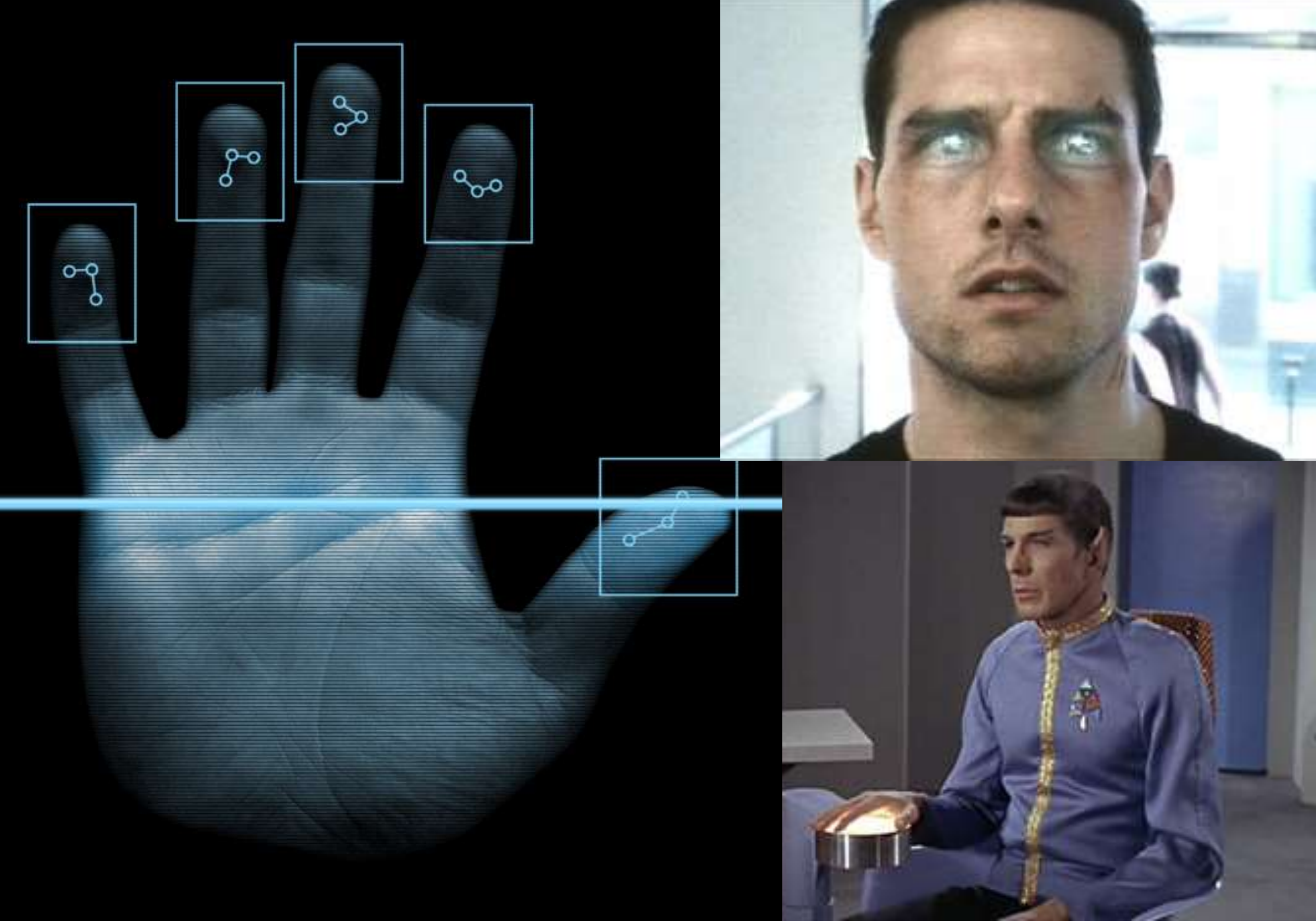
`https://github.com/cupslab/password_meter`

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

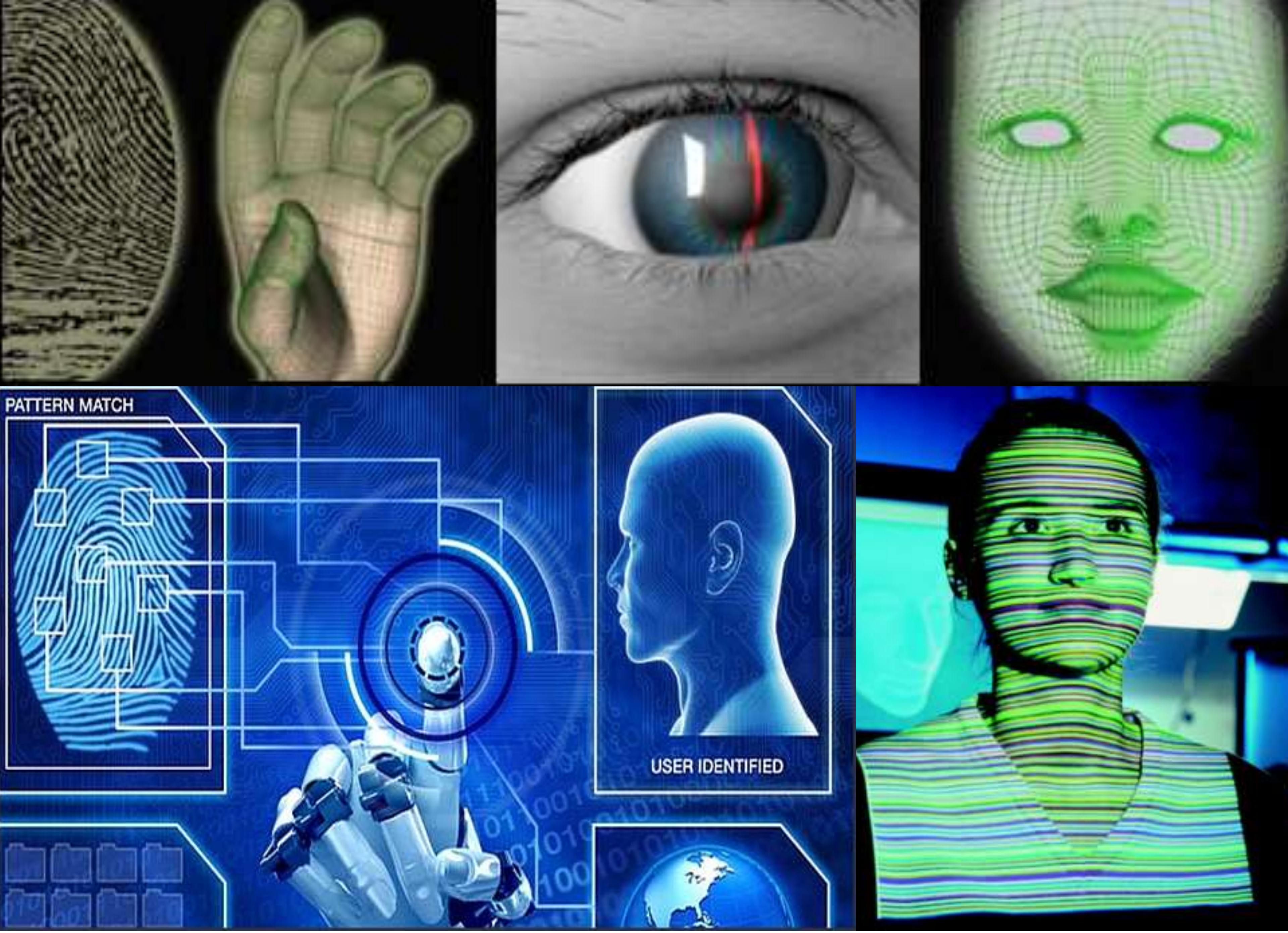
What about Biometrics?

nages on previous slide fair use from androidcentral.com and businessinsider.com. Photo above fair use from abcnews.com

nages fair use from wordpress.com and kaspersky.com, as well as Creative Commons from matsuyuki on Flickr



nages fair use from ccmcinc.com, filmjunk.com, and discovermagazine.com



Images fair use from fbi.gov, ifsecglobal.com, and siemens.com

Biometrics

- Fingerprint
- Iris scans or retina scans
- Face recognition
- Finger/hand geometry
- Voice or speech recognition
- The way you type
- (Many others)

Practical Challenges for Biometrics

- Immutable (can’t be changed)
- Potentially sensitive data
- High equipment costs
- Sensitive to changes in the environment
- Biometrics can change over time

iPhone 5S Touch ID

9:41 AM
100%
Fingerprints
Success
Touch ID is ready. Your print can be used for unlocking your iPhone.
Continue

Android 4.0 Face Unlock

•Images fair use from androidcentral.com, creativebits.org, and businessinsider.com.

Smartphone Biometrics

Smartphone Biometrics

- Purpose is to reduce the number of times a user must enter his/her password

Smartphone Biometrics

- Purpose is to reduce the number of times a user must enter his/her password
- Falls back to the password

Smartphone Biometrics

- Purpose is to reduce the number of times a user must enter his/her password
- Falls back to the password
- Face recognition can be tricked by a photo

Smartphone Biometrics

- Purpose is to reduce the number of times a user must enter his/her password
- Falls back to the password
- Face recognition can be tricked by a photo
- Fingerprint recognition can be tricked by a gummy mold

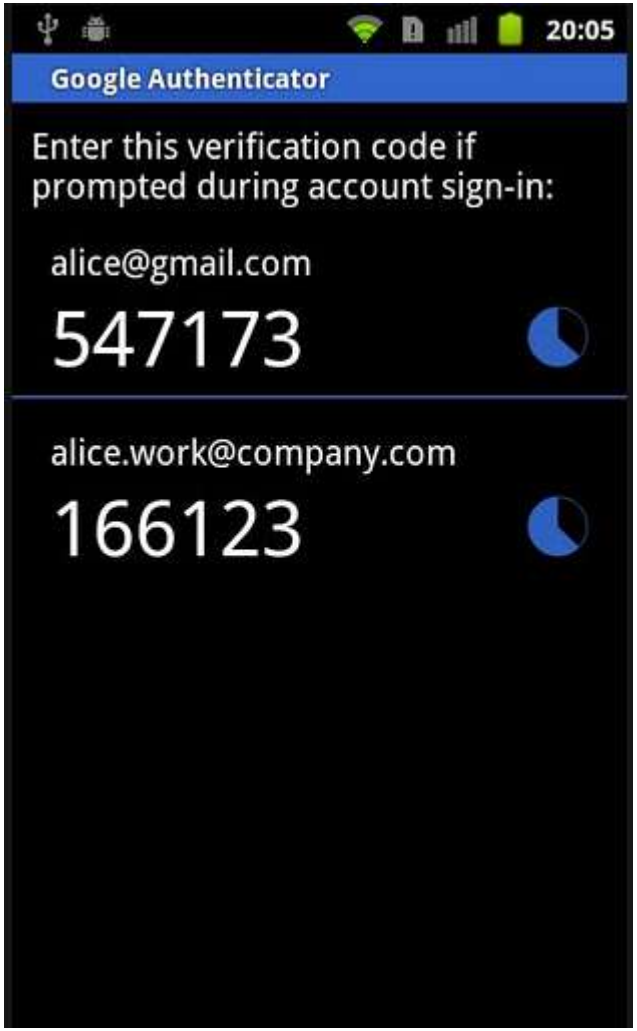
Smartphone Biometrics

- Purpose is to reduce the number of times a user must enter his/her password
- Falls back to the password
- Face recognition can be tricked by a photo
- Fingerprint recognition can be tricked by a gummy mold
- Users find fingerprint unlock convenient, but do not particularly like face unlock

Practical Authentication

Single Sign-On

Two-Factor Auth



Enter this verification code if prompted during account sign-in:

alice@gmail.com

547173

alice.work@company.com

166123

Physical Tokens

- Codes based on a cryptographic key
  - Token manufacturer also knows the key
- What if there is a breach?

Resetting Accounts

- I forgot my password!
- Send an email?
- Security questions?
- In-person verification?
- Other steps?
- (No backup)

Password Managers

- Trust all passwords to a single master password
  - Also trust software

LastPass ****

1Password

Conclusions

- Authentication is really hard!
  - Hard for system administrators
  - Hard for users
- Unfortunately, authentication is necessary

Access Control

- Access control lists
  - Owner, Group, Other
  - chown
  - chmod
- Role-based access control
- Attribute-based access control
- Context-based access control

Access Control

- Role-based access control
  - Authorization based on role (e.g., “Uchicago student”)
- Attribute-based access control
  - Authorization based on attribute(s) (e.g., “Over 7 feet tall”)
- Context-based access control
  - Authorization decision depends on the context (e.g., time of day)

Access Control in the Internet of Things

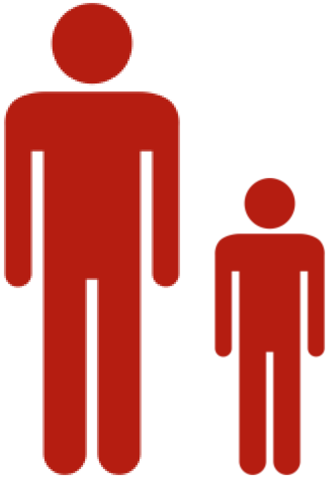
Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, Blase Ur. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In *Proc. USENIX Security*, 2018.

Factor: Time of Day

“I would not want anyone trying to use the mower at night. The neighbors would most likely get mad.”

Icon made by Freepik from www.flaticon.com

Factor: People Around



◀ Child

“They would be allowed to use it whenever I am home with them.”

Factor: Location of User

Why not play some music?
What is going on???

“Why do you need to use it if you aren’t close?”

Factor: Location of Device

“If it is used in the bedroom then it would matter who has access.”

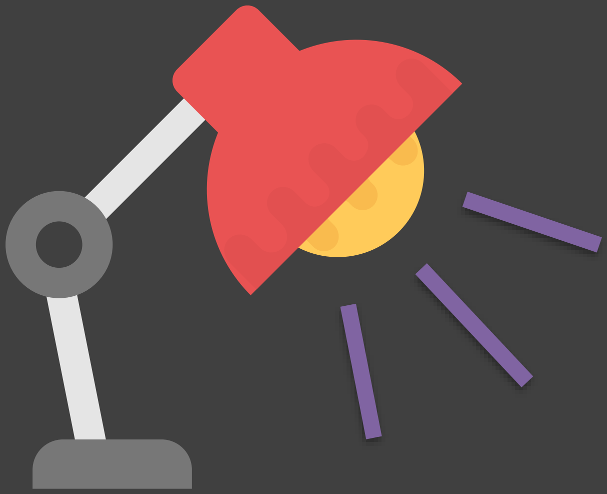
bedroom-21 - ffooty.com

Factor: Explicit Permission

“When they are authorized by the owner.”

Factor: Consequences

Factor: Responsible Usage

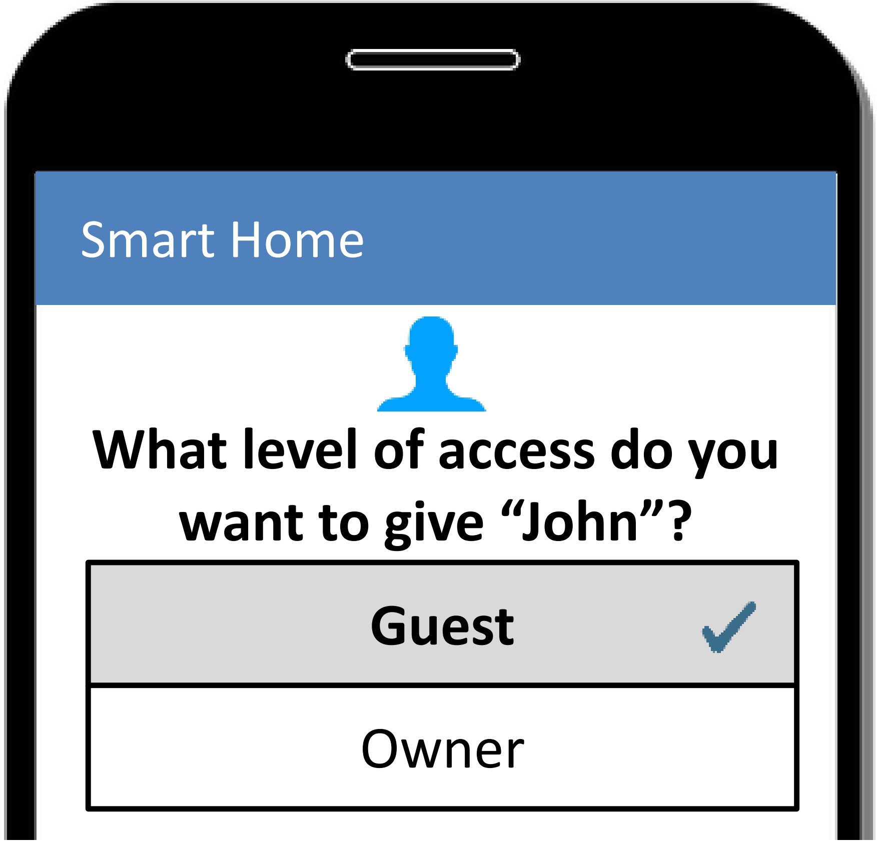


“They shouldn't use the lights if they are using them too frequently.”

Icon made by Freepik from www.flaticon.com

Design Implications
For Contextual Access Control

Current: Guest vs. Owner



Smart Home

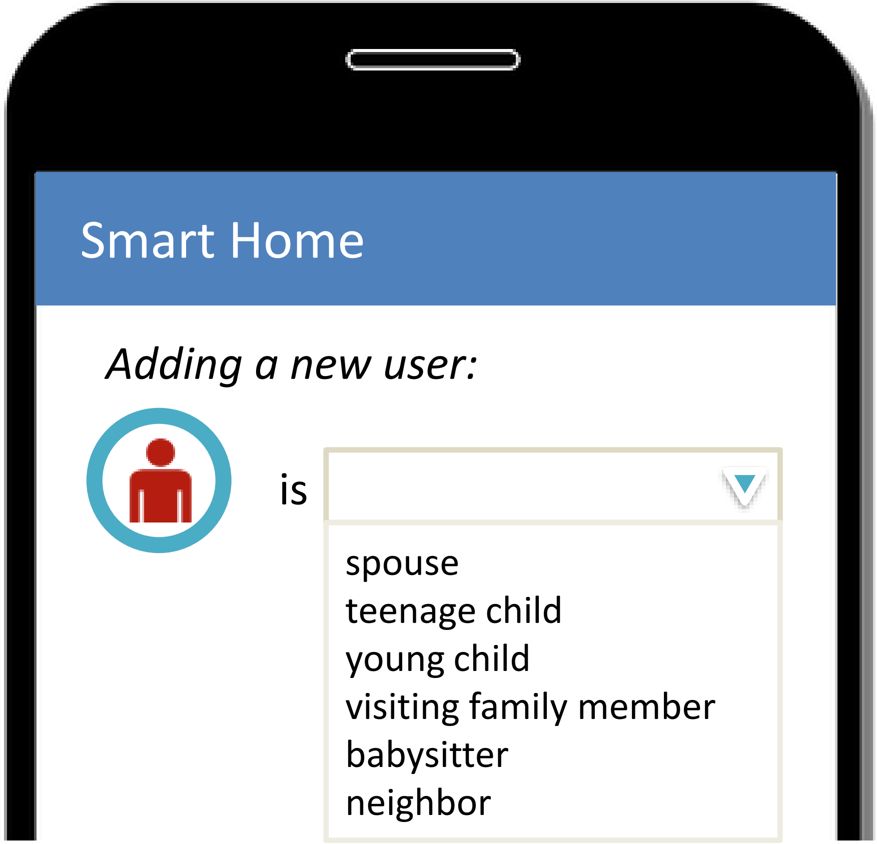
What level of access do you want to give “John”?

Guest ✓

Owner

Smartphone Icon – pixabay.com

Future: Designing for Relationships



Smart Home

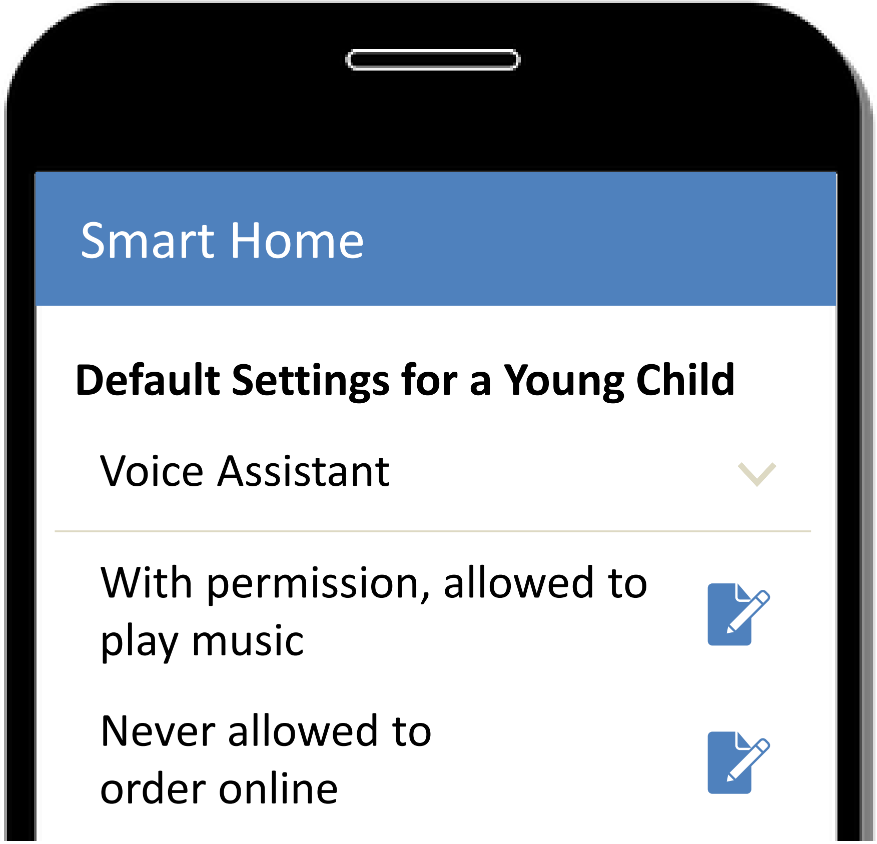
Adding a new user:

is

- spouse
- teenage child
- young child
- visiting family member
- babysitter
- neighbor

Smartphone Icon – pixabay.com

Future: Relationships and Capabilities



Smart Home

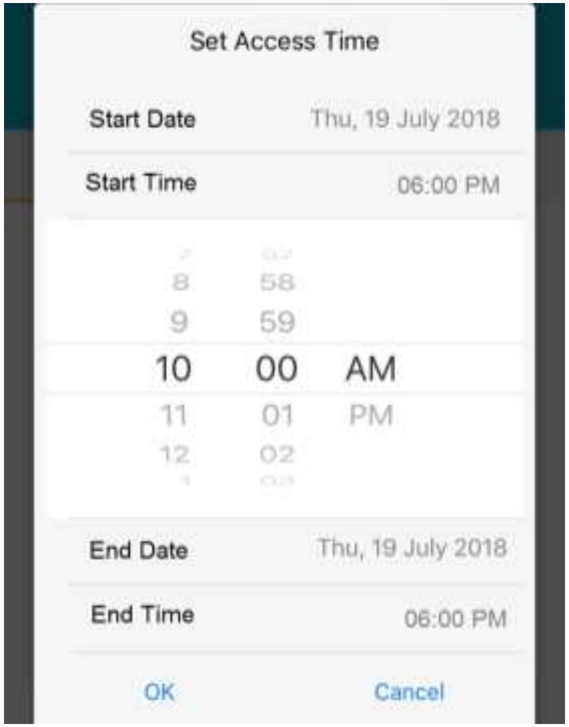
Default Settings for a Young Child

Voice Assistant

With permission, allowed to play music

Never allowed to order online

Current: Full or Temporary Access



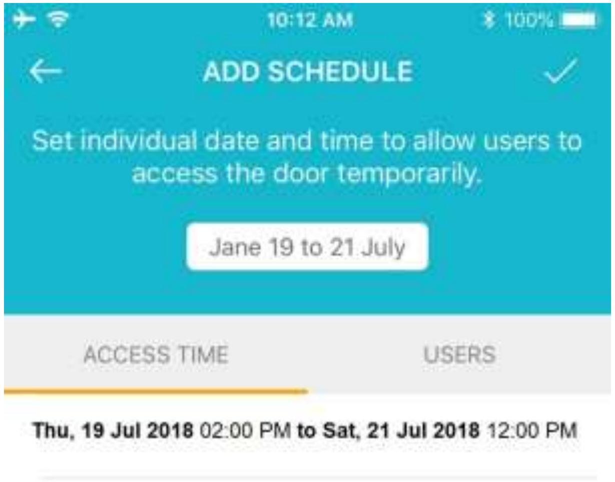
Set Access Time

Start Date Thu, 19 July 2018

Start Time 06:00 PM

End Date Thu, 19 July 2018

End Time 06:00 PM

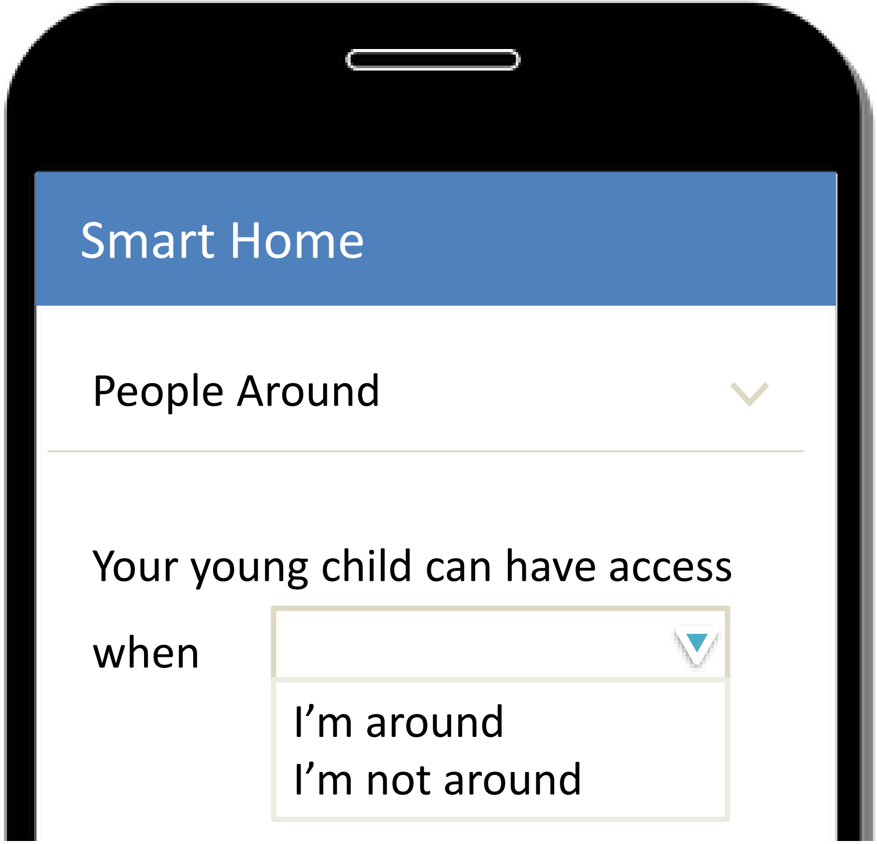


Set individual date and time to allow users to access the door temporarily.

Jane 19 to 21 July

Thu, 19 Jul 2018 02:00 PM **to Sat, 21 Jul 2018** 12:00 PM

Future: Contextual Factors



Smart Home

People Around

Your young child can have access

when

I’m around

I’m not around