04. Passwords

Blase Ur

April 11th, 2019

CMSC 23210 / 33210

THE UNIVERSITY OF CHICAGO

UCHICAGO SUPER GROUP
Security, Usability, & Privacy
Education & Research


123456
12345
123456789
password
iloveyou
princess
rockyou
1234567
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger
sunshine
chocolate
password1
soccer
anthony
friends
butterfly
purple
angel
jordan
liverpool
justin
loveme
football
basketball
superman
tinkerbell
playboy
jasmine
brandon
elizabeth
andrea
carlos
flower
hottie
cookie
bubbles
dragon
jennifer
spongebob
whatever
secret
pretty
barbie
chelsea
angels
andrew
shadow
summer
melissa
matthew
softball
666666
hello
1234567890

c|net

Search CNET | Reviews | News | Video | How To | Deals | Download | Sign In / Join | US Ed

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.

PCWorld

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

COMPUTERWORLD FROM IDG

INSIDER

NEWS

Russian credential theft shows why the password is dead

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

theguardian

US world opinion sports soccer tech arts lifestyle fashion business

Google aims to kill passwords by the end of this year

GIZMODO

The Tech That Will Kill Passwords

Adam Clark Estes

12/04/14 2:30pm · Filed to: PASSWORDS

Why Passwords?

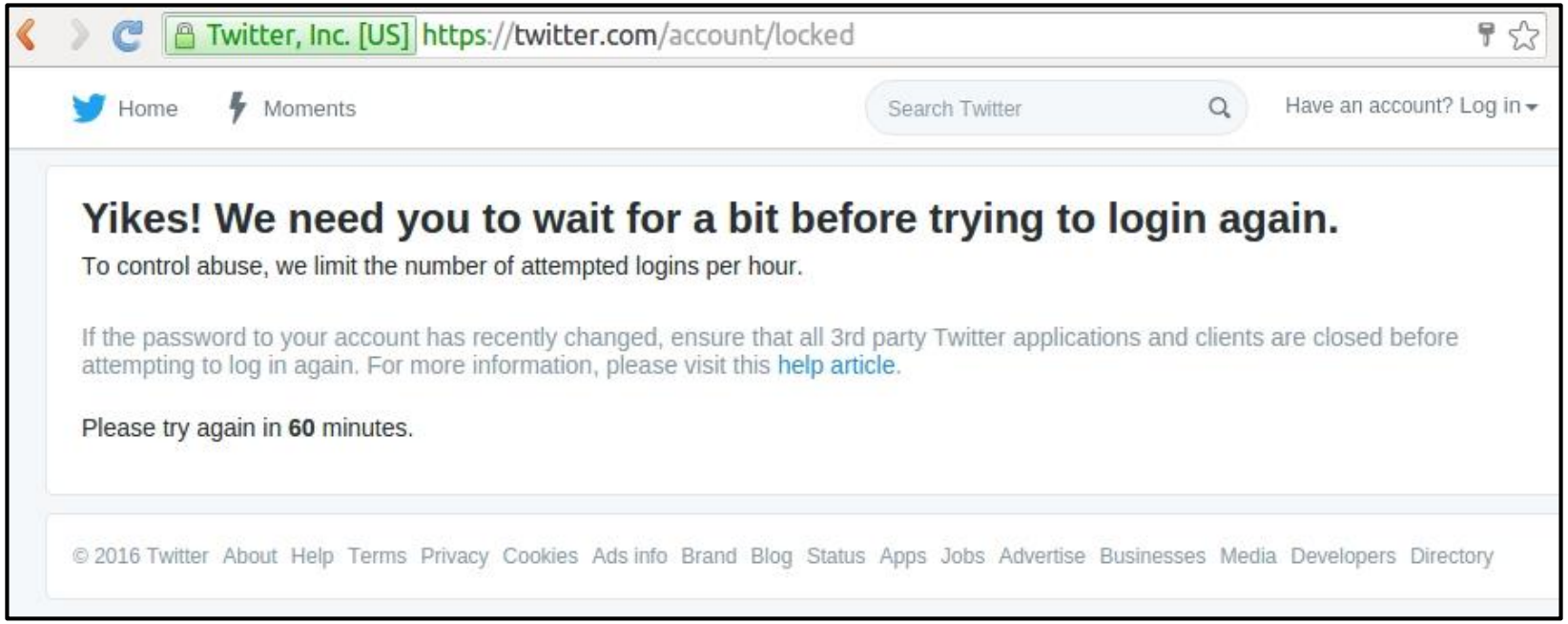
- Familiar to people
- Nothing to carry
- Difficult to coerce
- Easy to deploy, revoke, and replace

Threats to Password Security

- Online attack against live system

Threats to Password Security

- Online attack against live system
  - Rate-limiting



Threats to Password Security

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

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.

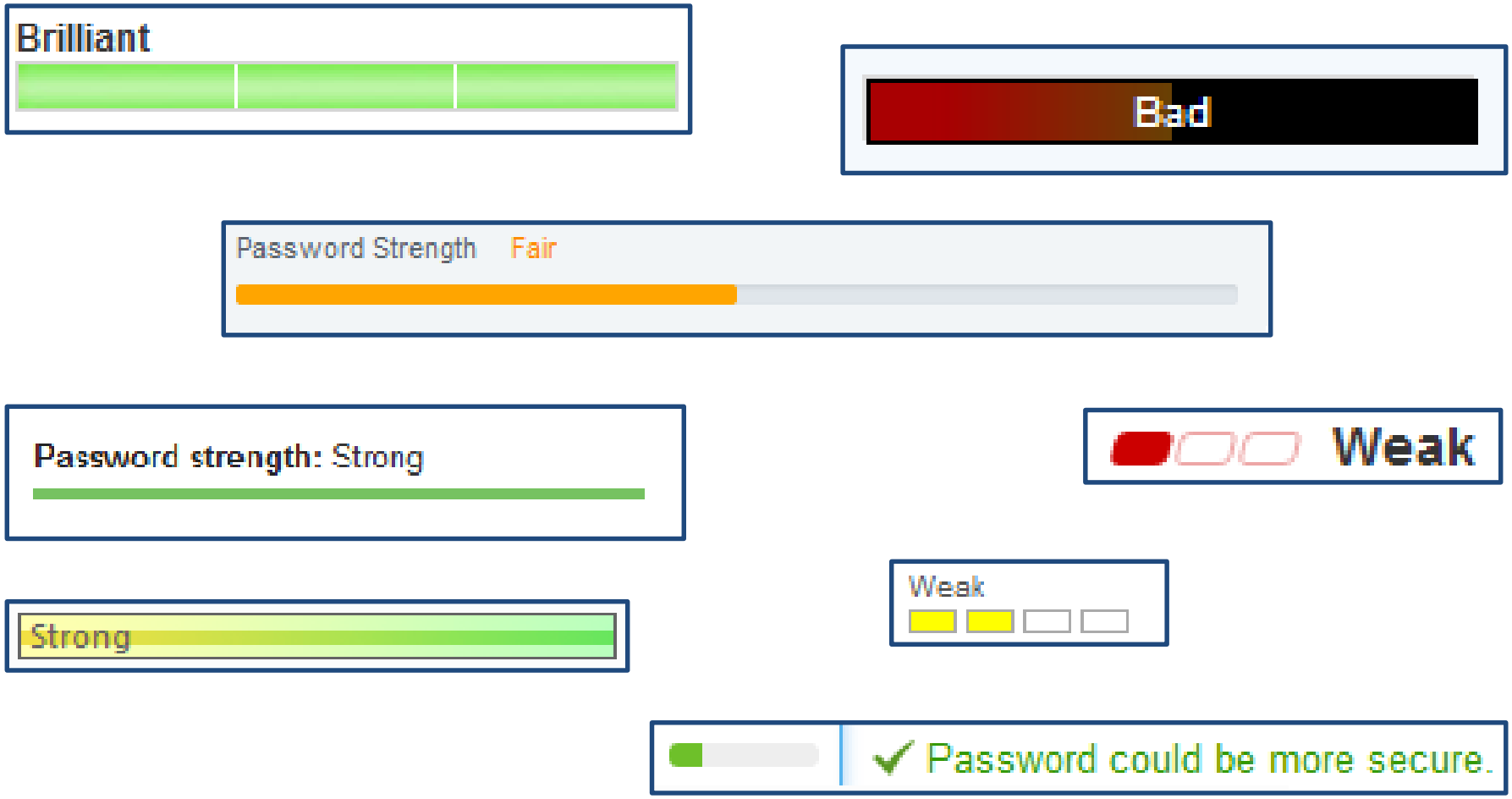
Problem 2: Inaccurate Feedback

Problem 3: Unhelpful Feedback

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.

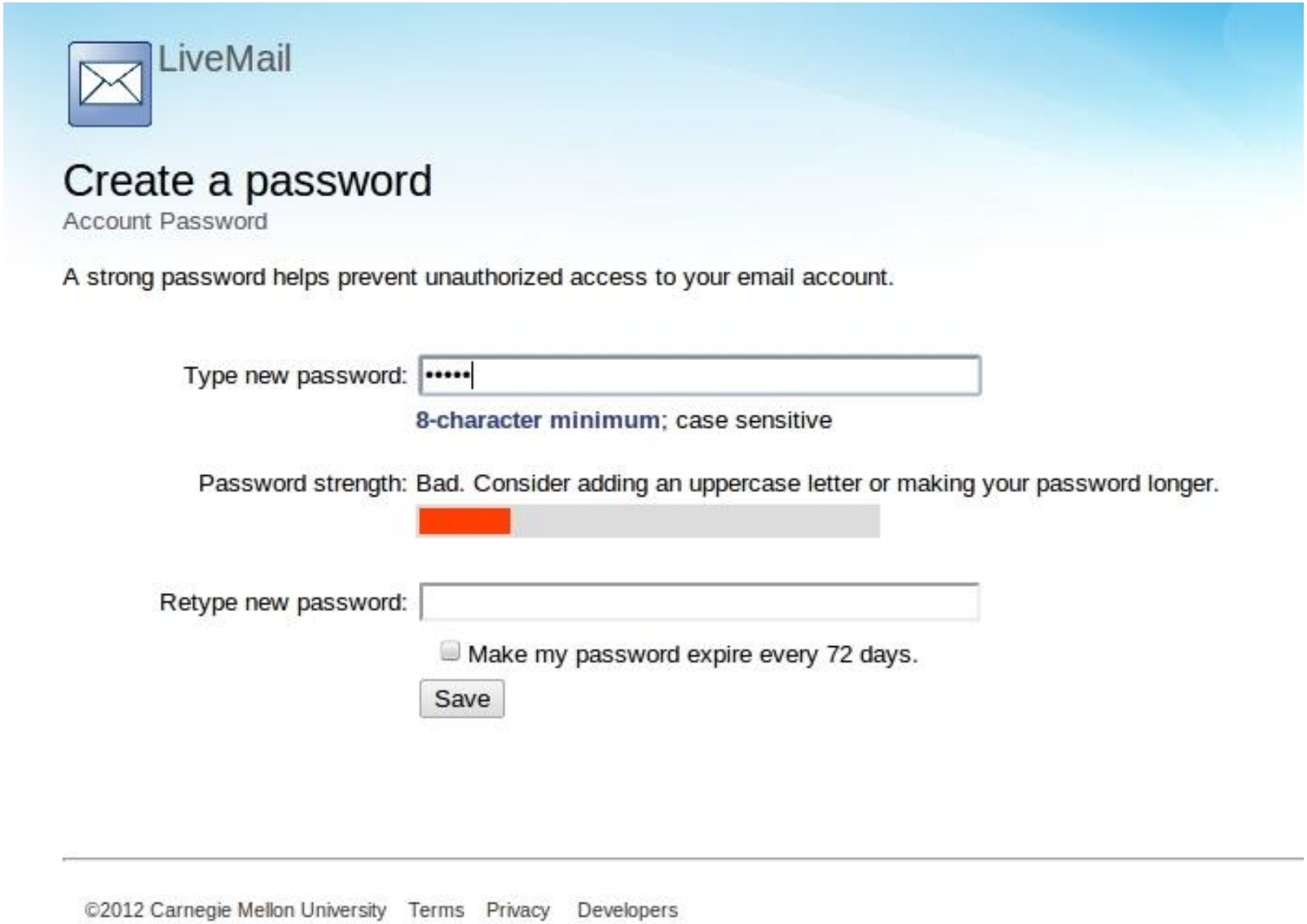
Meters Are Ubiquitous



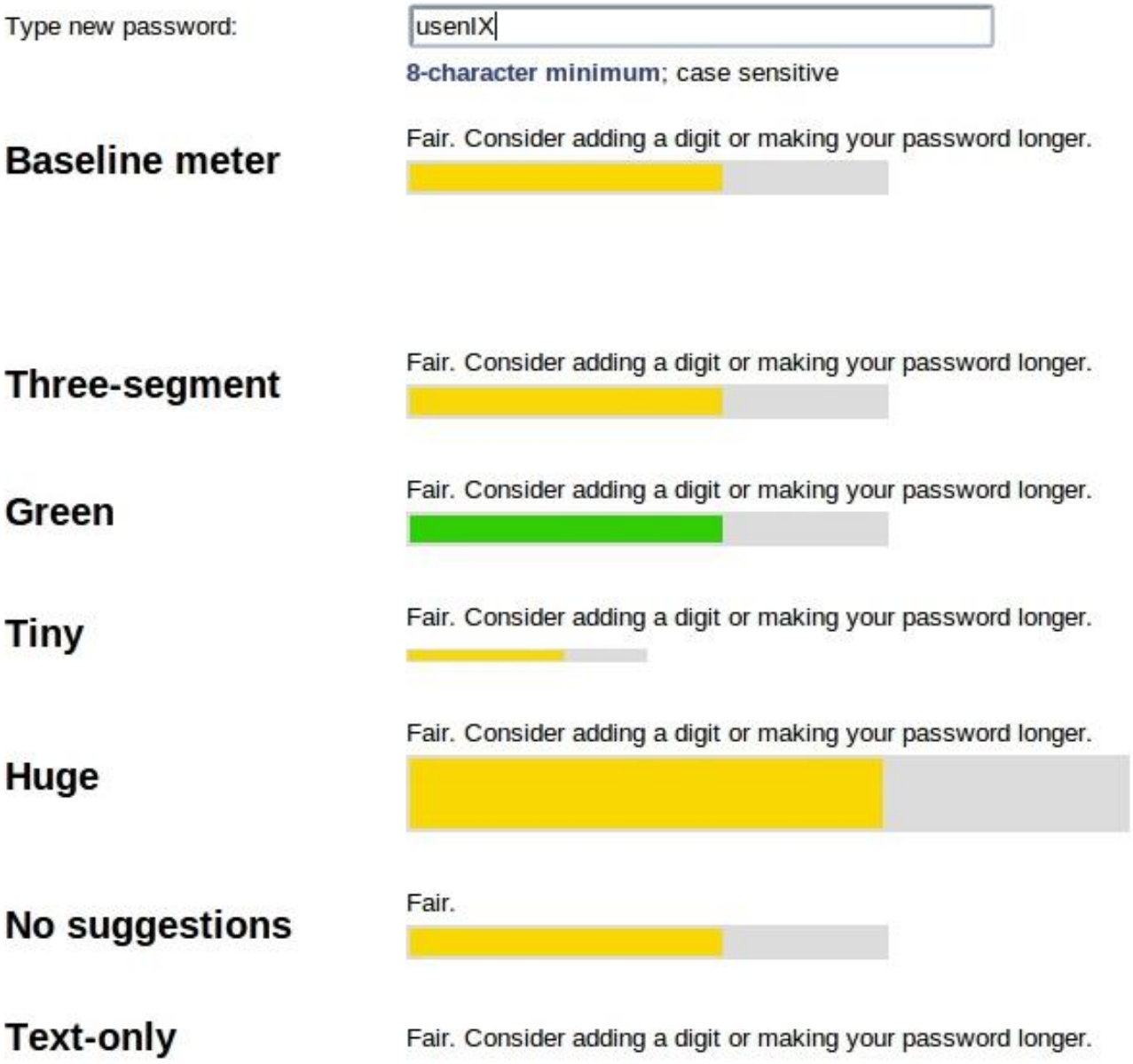
Test Meters' Impact

- 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



Visual Differences



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

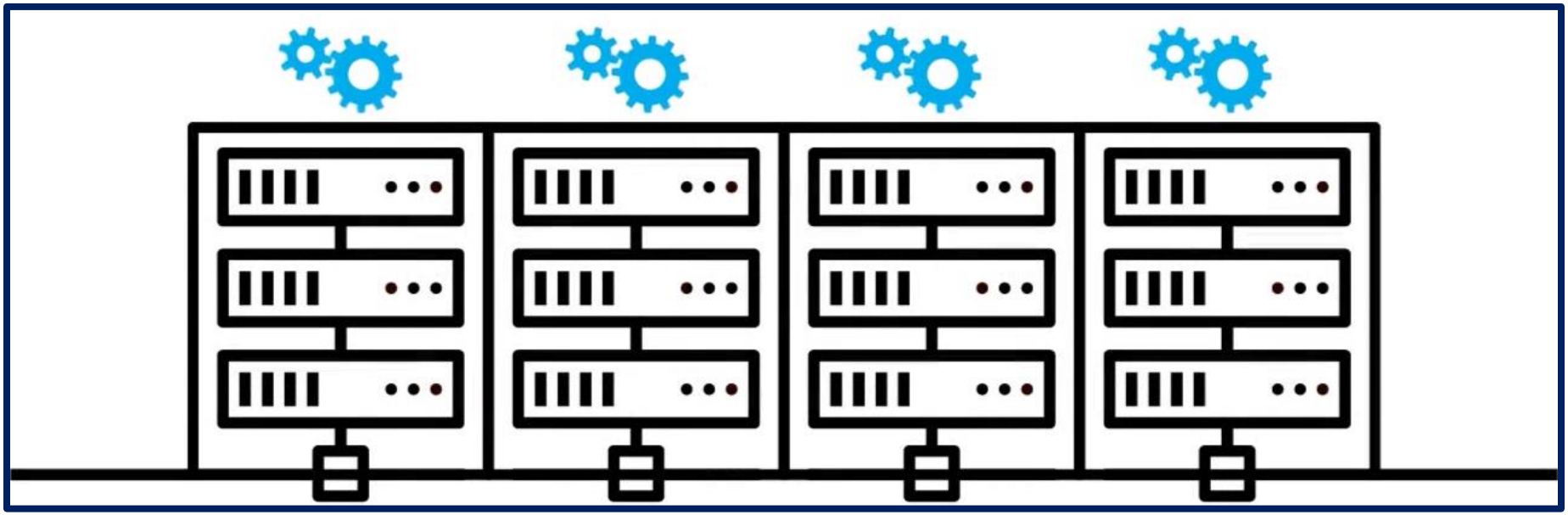
Fair. Consider adding a digit or making your password longer.

Scoring Differences

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

Approach

4 password sets

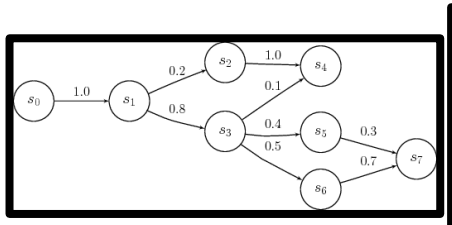
```
password
iloveyou
teamo123
…
```

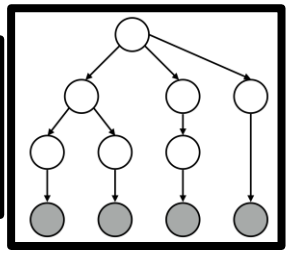
```
passwordpassword
1234567812345678
!1@2#3$4%5^6&7*8
…
```

```
Pa$$w0rd
iLov3you!
1QaZ2W@x
…
```

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

✖ 5 approaches





KoreLogic SECURITY

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!`

Understand Origin of Passwords

LEFTbrown8!

Understand Origin of Passwords

LEFTbrown8!

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

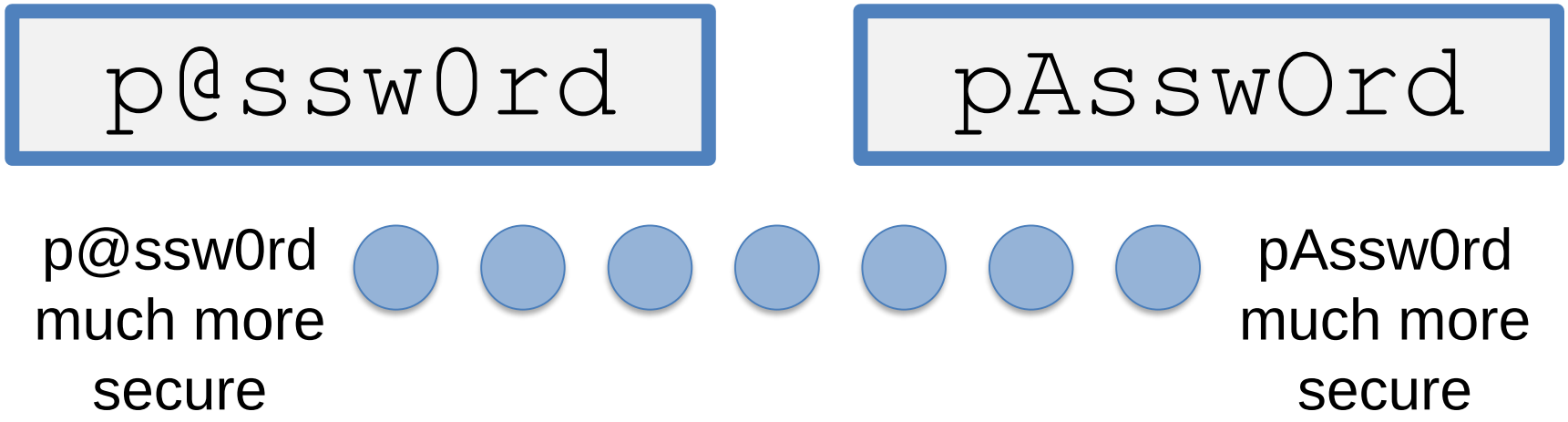
- Online study
  - Compensated $5 for ~30 minutes
- 165 participants from Mechanical Turk
  - Age 18+, live in United States
  - Median age 33
  - 49% female, 51% male
  - 16% CS or related degree or job
  - 4% student/professional in computer security

Study Tasks

1. Evaluating password pairs

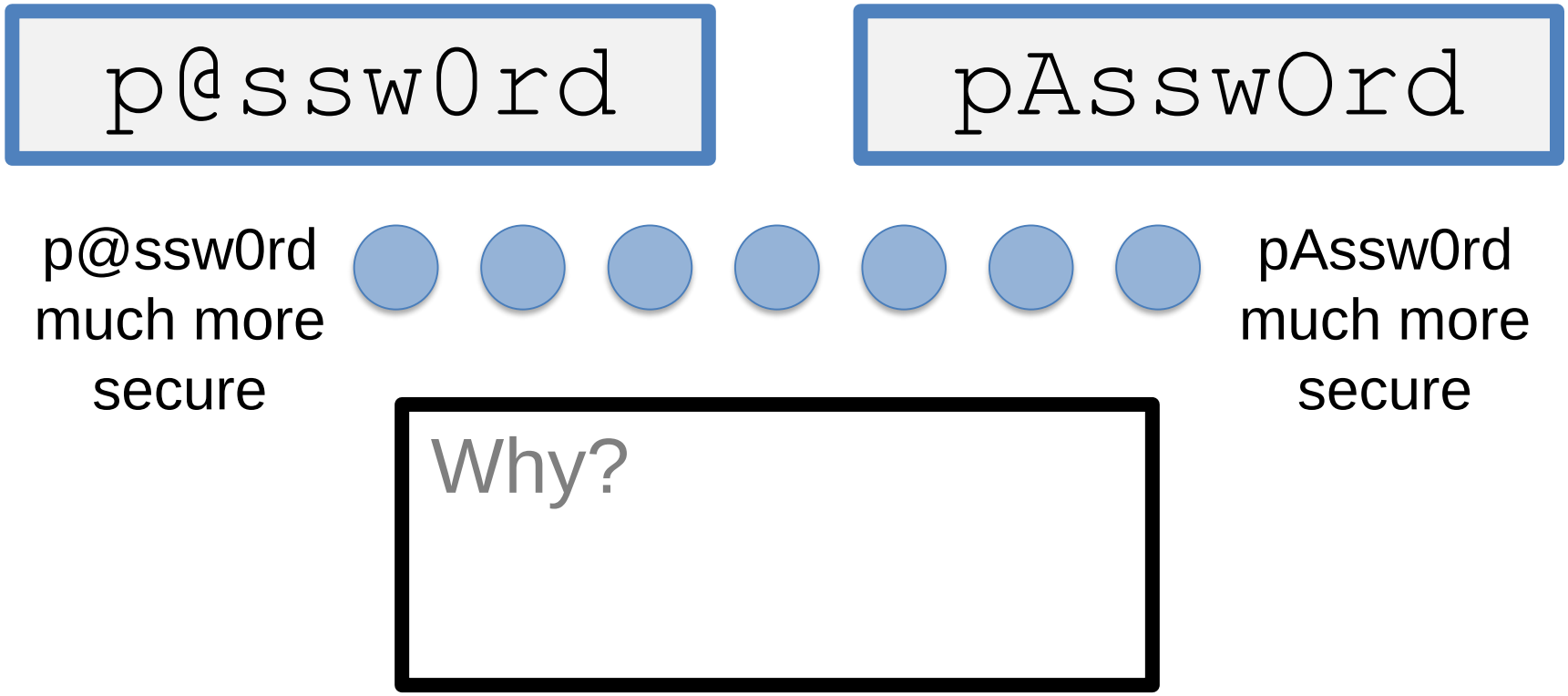
Study Tasks

1. Evaluating password pairs



Study Tasks

1. Evaluating password pairs



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`

Evaluating Password Pairs

`iloveyou88`

`ieatkale88`

Evaluating Password Pairs

`iloveyou88`

`ieatkale88`

4,000,000,000 × more secure!

Evaluating Password Pairs

`brooklyn16`

`brooklynqy`

Evaluating Password Pairs

`brooklyn16`

`brooklynqy`

Evaluating Password Pairs

`brooklyn16`

`brooklynqy`

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

Perception: How Many Guesses?

Perception: How Many Guesses?

- 2 guesses (Min)

Perception: How Many Guesses?

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

Perception: How Many Guesses?

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

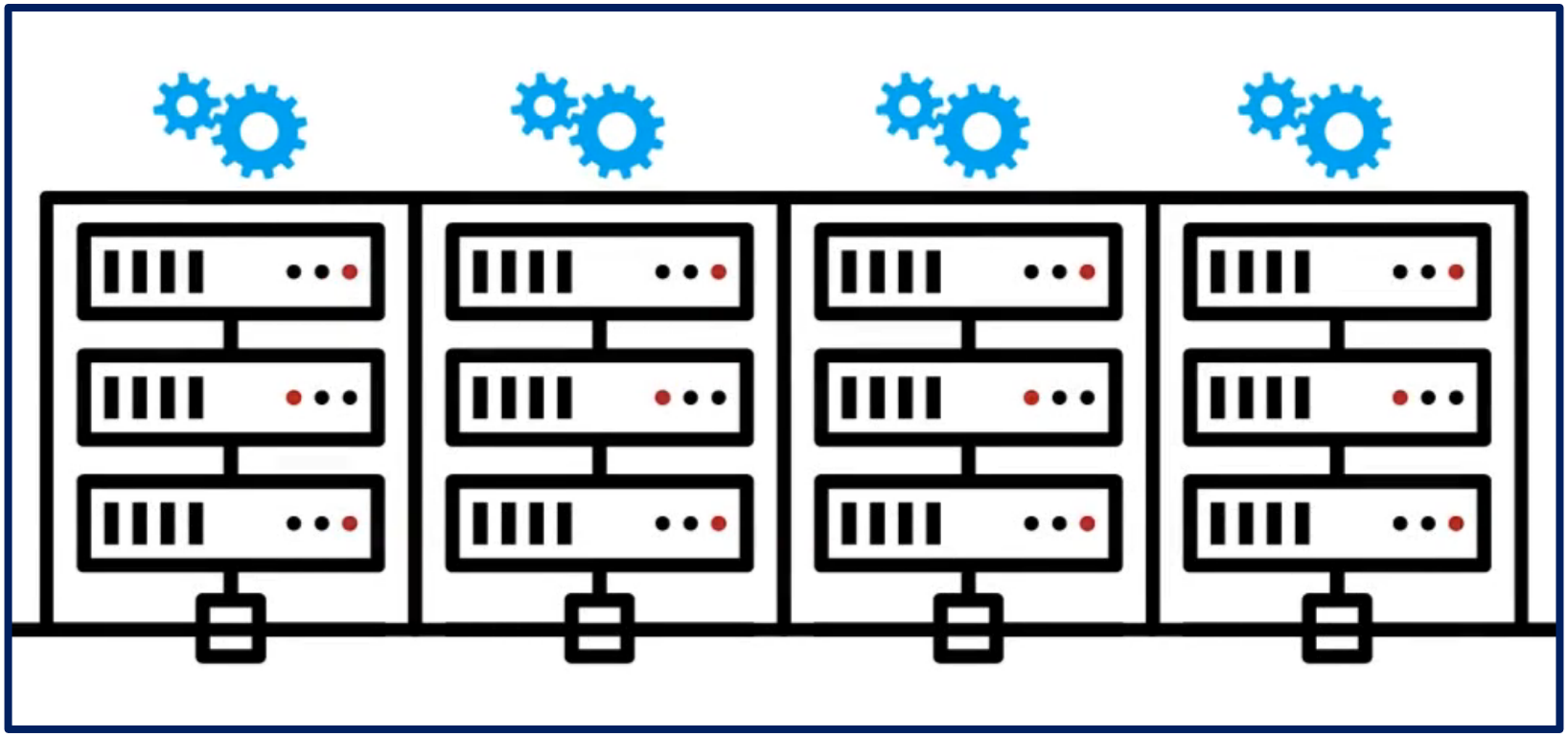
Conclusions

- 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

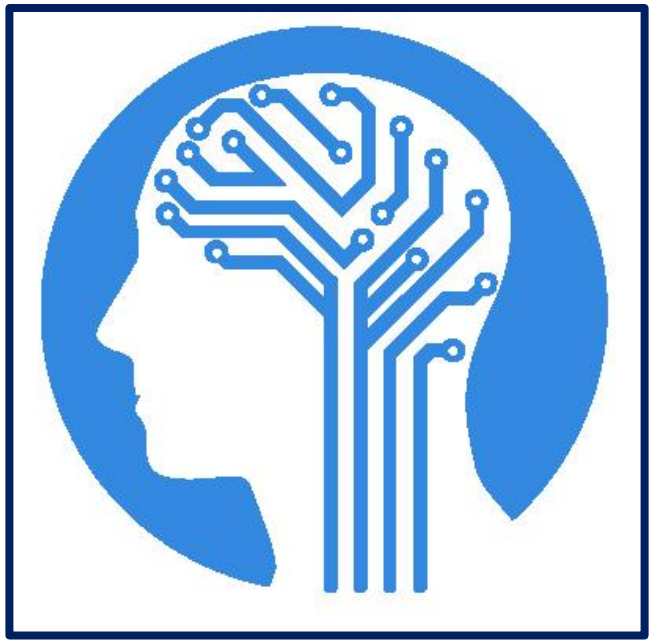
Better Password Scoring



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



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%

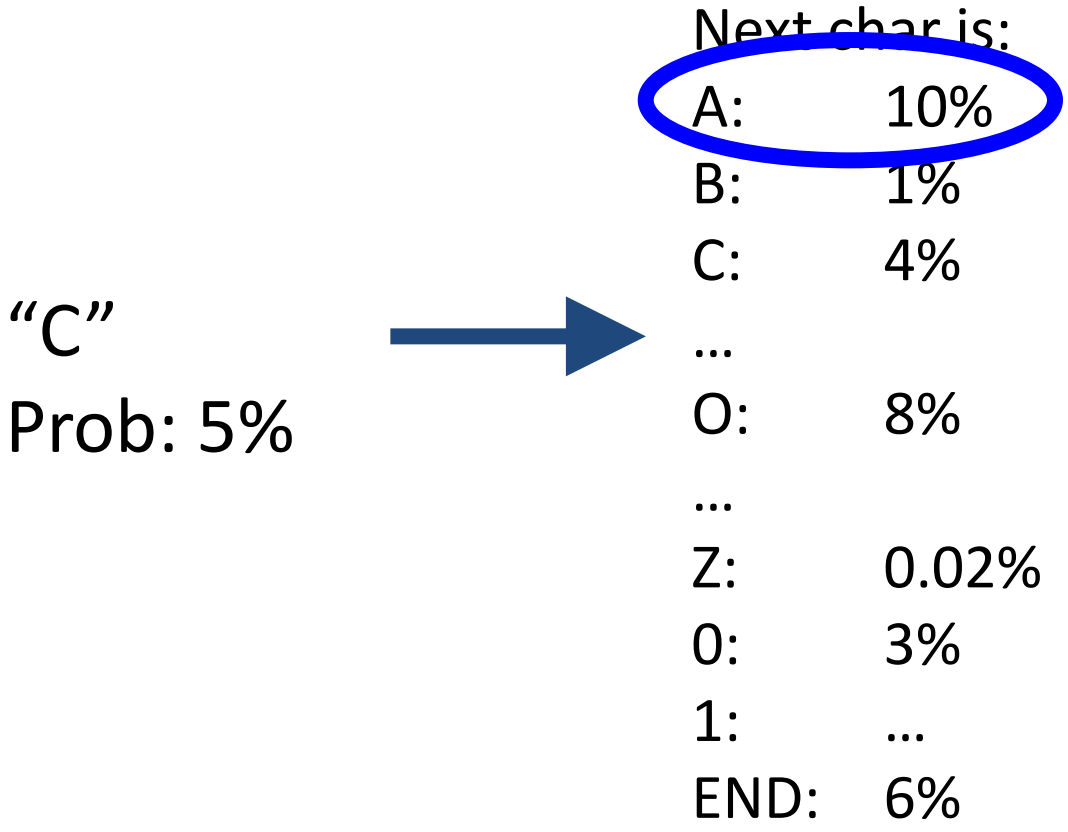
Generating Passwords

"C"
Prob: 5%

Next char is:

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

Generating Passwords



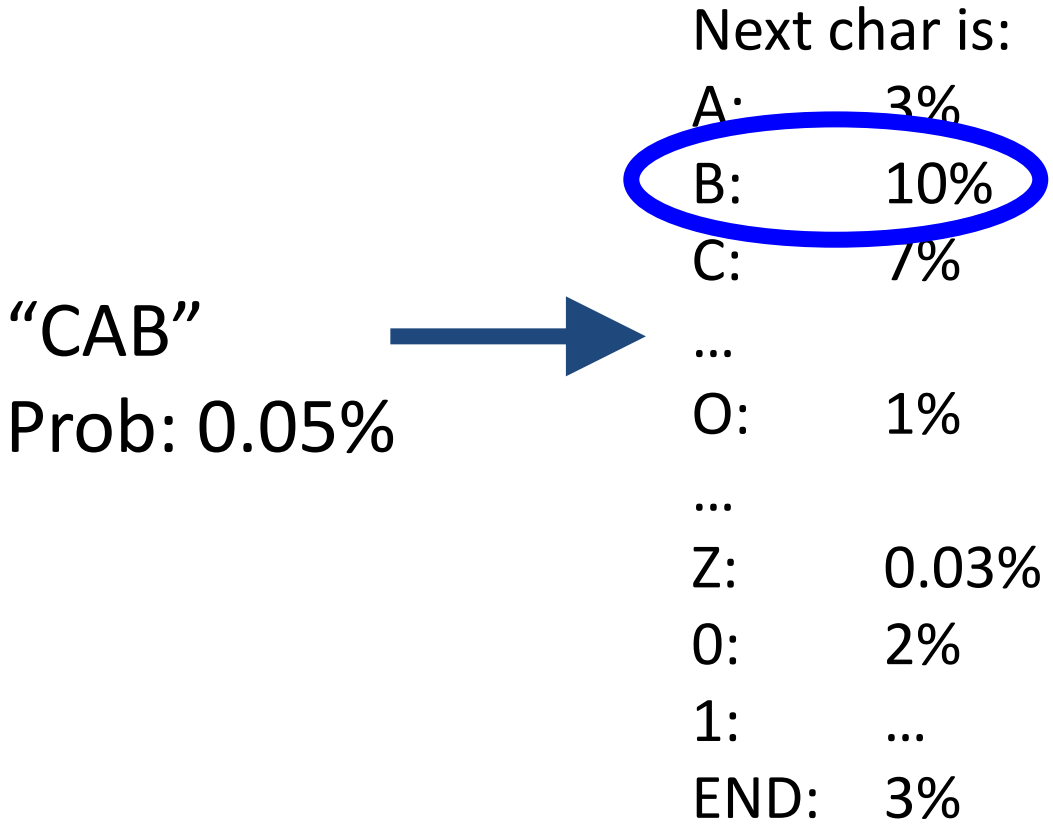
Generating Passwords

"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



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%
…