04. Studying Passwords

Blase Ur, April 5th, 2017
CMSC 23210 / 33210

THE UNIVERSITY OF CHICAGO

Security, Usability, & Privacy Education & Research

Announcements

- On Monday:
  - Privacy discussion
  - PSET 1 presentations
  - Key verification
- Reading for Monday will be on Piazza

Today's class

- A whirlwind tour of passwords (AKA how a class project led to 13+ papers)
  - Goal: understand how to align the study methods to the problem of interest
- Project ideas

Authentication

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

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
- 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., CMU Andrew ID)
  - PKI Certificate Authorities

Pa$$w0rds

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 Are Passwords So Prevalent?

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

Best Practices for Storing Passwords

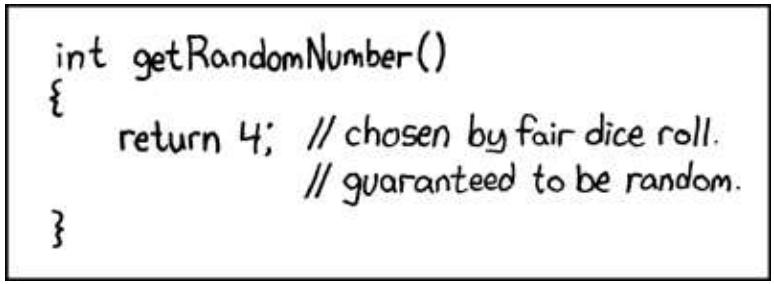
- **Hash** and **salt** passwords
- Hash function: one-way function
  - Traditionally designed for efficiency (e.g., MD5)
  - Password-specific hash functions (e.g., bcrypt, scrypt, PBKDF2)

Best Practices for 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

Example Using MD5 (BAD!!!!)

- H(“blase”) = 12b872adb2588c668d706d847fc1da7e
- H(“blaze”) = 9084994342186c542e75b2fc5241c547
- H(“blase”) = 12b872adb2588c668d706d847fc1da7e
- Salt w/ randomness! e.g., “4”



- Store “*username*, 4” H(“blase4”) = 8379931f960303082bf2edaf767cd418

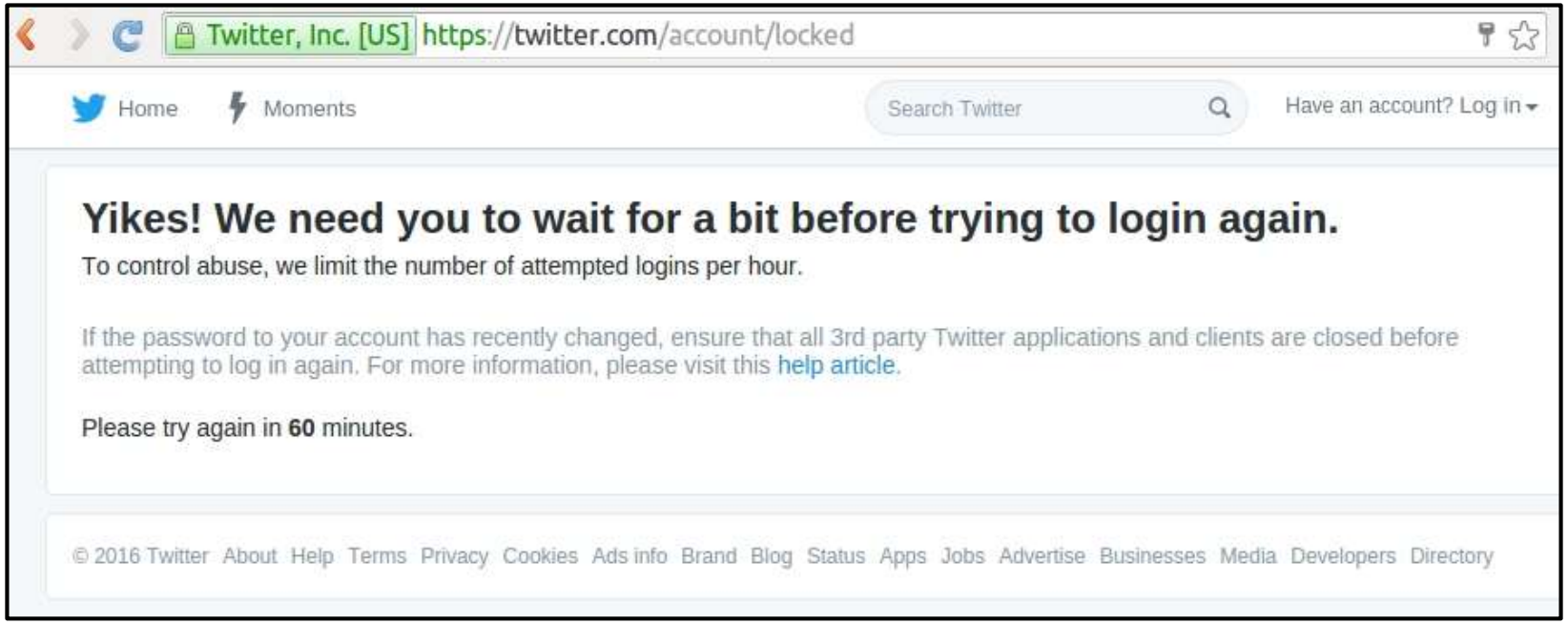
Threats to Password Security

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

Threats to Password Security

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

Threats to Password Security

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

Anatomy of an Offline Attack

Anatomy of an Offline Attack

- Attacker compromises database

Anatomy of an Offline Attack

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

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

Anatomy of an Offline Attack

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

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

- Attacker makes and hashes guesses

Anatomy of an Offline Attack

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

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

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

Anatomy of an Offline Attack

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

`$2a$04$iHdEgkI681VdDMc3f7edau9phRwORvhYjqWAIb7hb4B5uFJO1g4zi`

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

Anatomy of an Offline Attack

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

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

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

What if a goldmine of passwords appeared?

rockyou

- 32 million passwords
  - Plaintext (not hashed)
  - ~16 million unique

123456789
12345
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
fuckyou
123123
football
secret
andrea
carlos
jennifer
joshua
bubbles
1234567890
superman
hannah
amanda
loveyou
pretty
basketball
andrew
angels
tweety
flower
playboy
hello
elizabeth
hottie
tinkerbell
charlie
samantha
barbie
chelsea
lovers
teamo
jasmine
brandon
666666
shadow
melissa
eminem
matthew
robert
danielle
forever
family
jonathan
987654321
computer
whatever
dragon
vanessa
cookie
naruto
summer
sweety
spongebob
joseph
junior
softball
taylor
yellow
daniela
lauren
mickey
princesa
alexandra
alexis
jesus
estrella
miguel
william
thomas
beautiful
mylove
angela
poohbear
patrick
iloveme
sakura
adrian
alexander
destiny
christian
121212
sayang
america
dancer
monica
richard
112233
princess1
555555
diamond
carolina
steven
rangers
louise
orange
789456
999999
shorty
11111
nathan
snoopy
gabriel
hunter
cherry
killer
sandra
alejandro
buster
george
brittany
alejandra
patricia
rachel
tequiero
7777777
cheese
159753
arsenal
dolphin
antonio
heather
david
ginger
stephanie
peanut
blink182
sweetie
222222
beauty
987654
victoria
honey
00000
fernando
pokemon
maggie
corazon
chicken
pepper
cristina
rainbow
kisses
manuel
myspace
rebelde
angel1
ricardo
babygurl
heaven
55555
baseball
martin
greenday
november
alyssa
madison
mother
123321
123abc
mahalkita
batman
september
december
morgan
mariposa
maria
gabriela
iloveyou2
bailey
jeremy
pamela
kimberly
gemini
shannon
pictures
asshole
sophie
jessie
hellokitty
claudia
babygirl1
angelica
austin
mahalko
volleyball
freedom
vampire
lovely1

But users are not the enemy!

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., []~!@#$%^&*()?<>./_-+=).

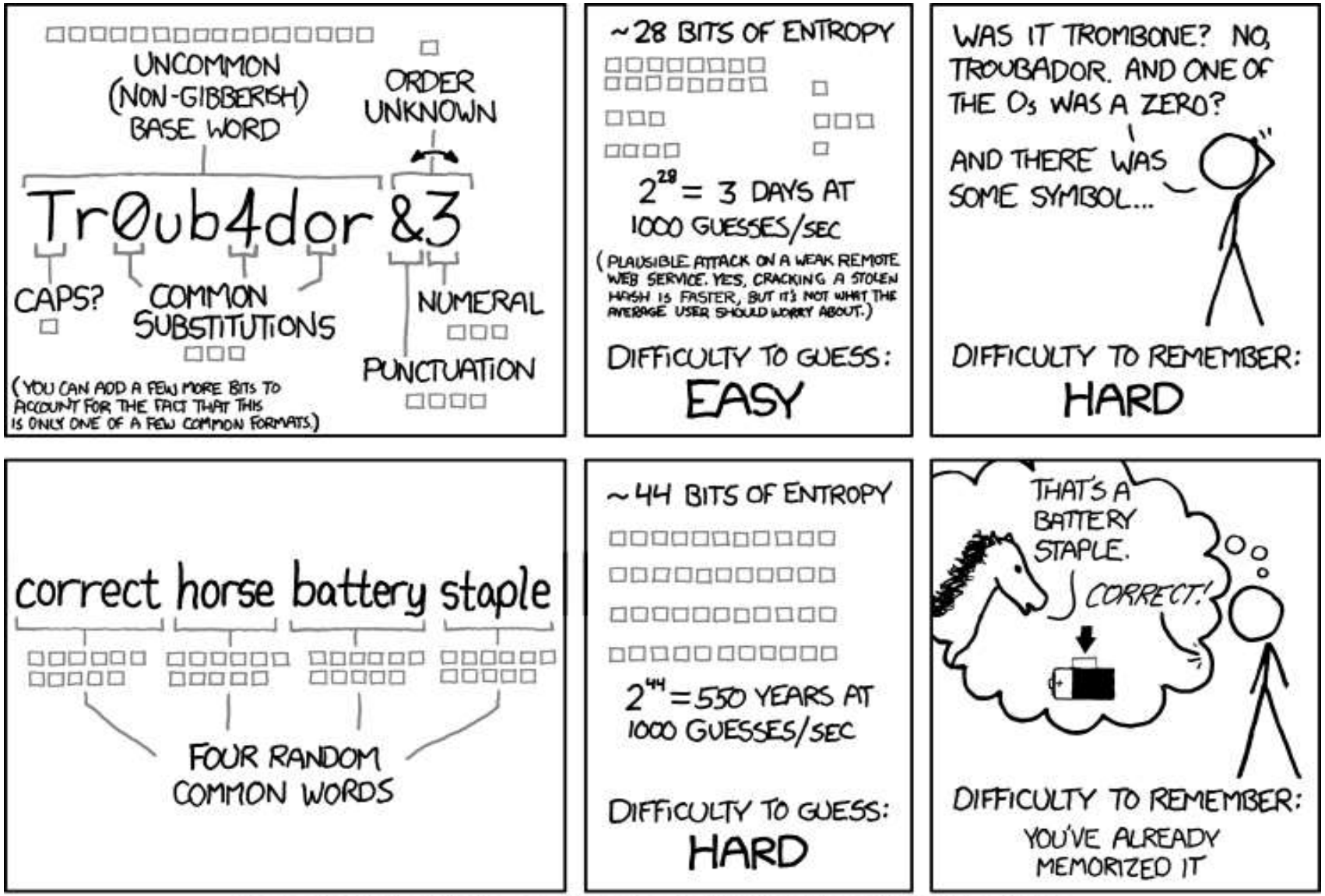
Cannot Contain

- 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).*

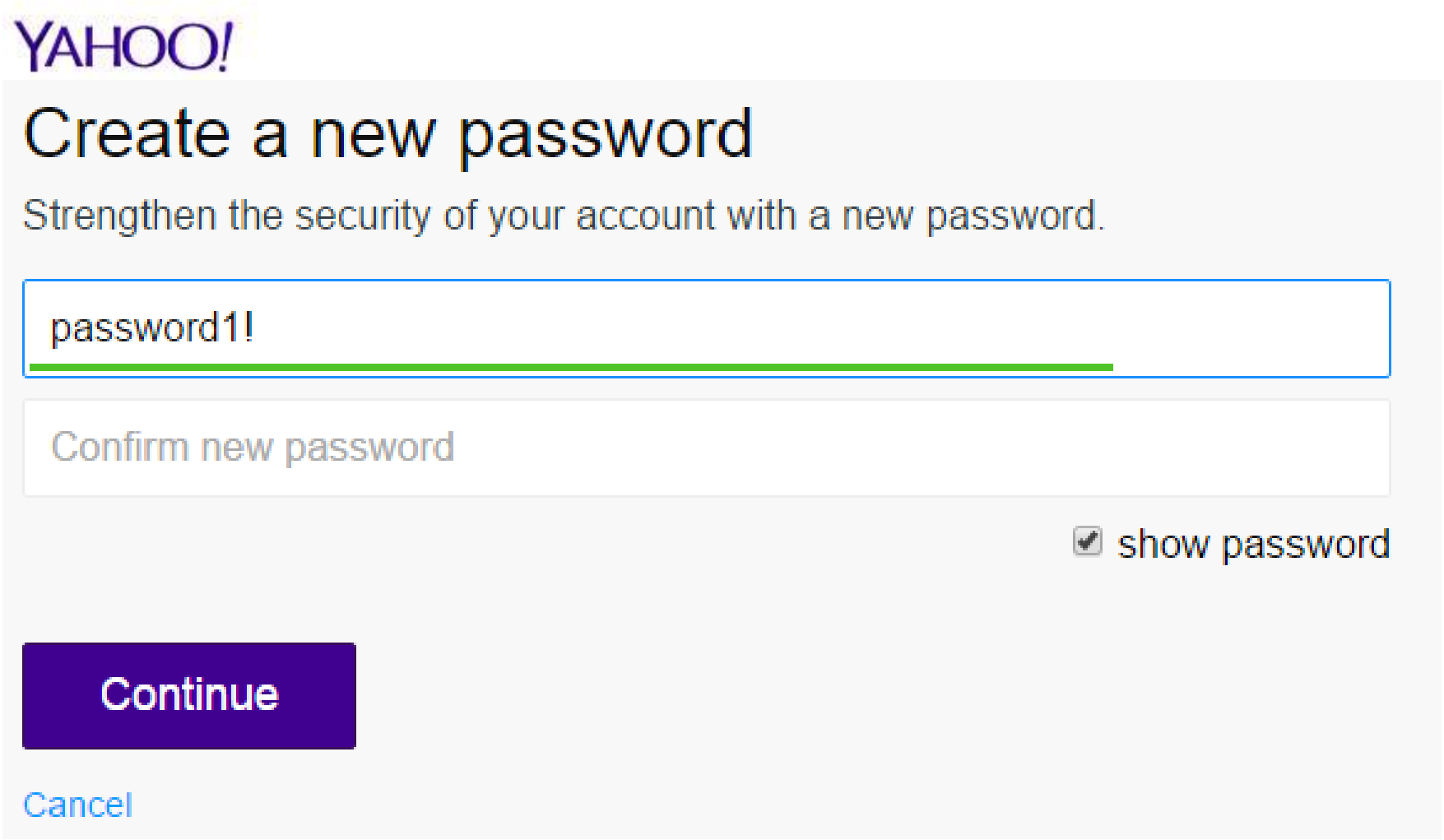
Additional Policies

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

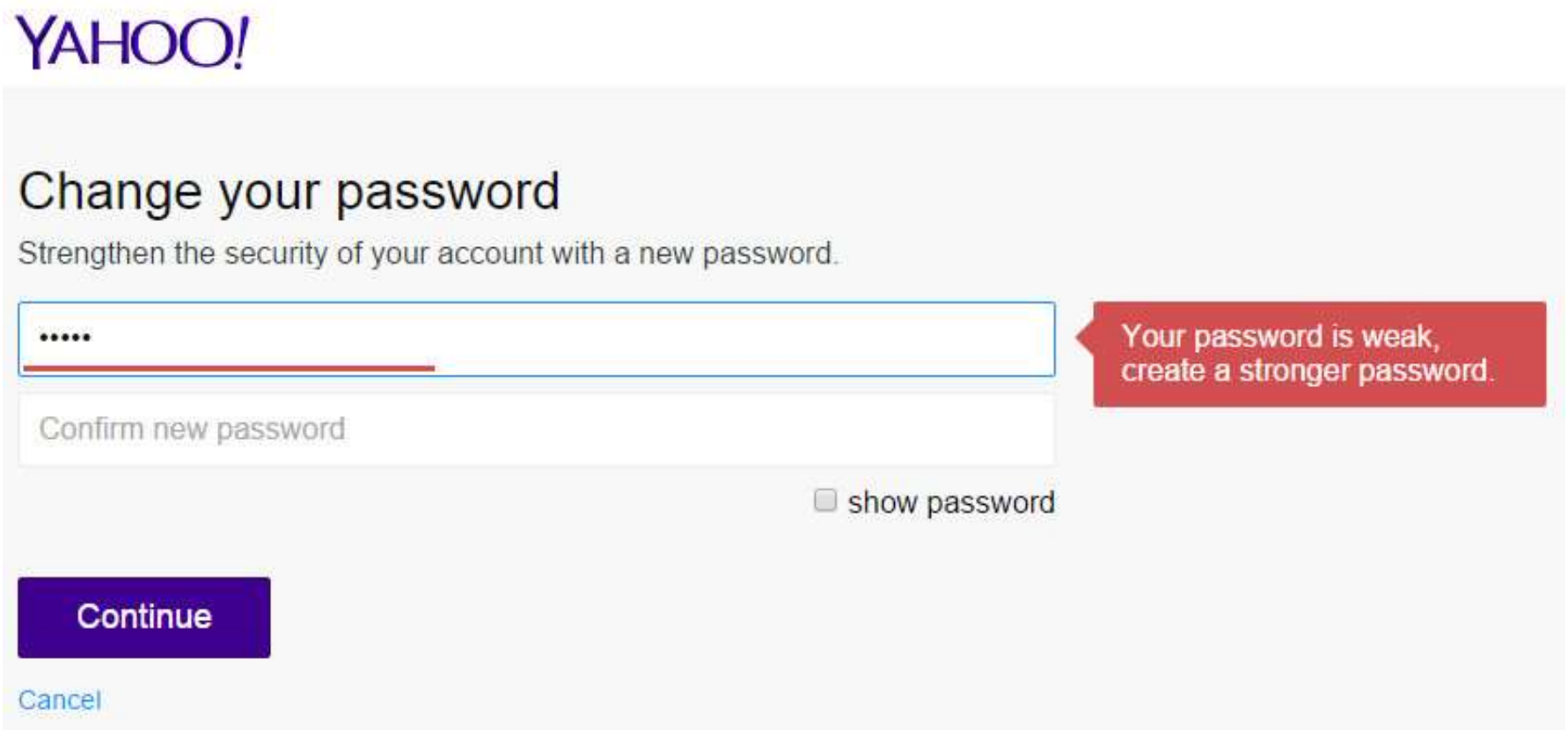


THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Problem 2: Inaccurate Scoring



Problem 3: Unhelpful Feedback



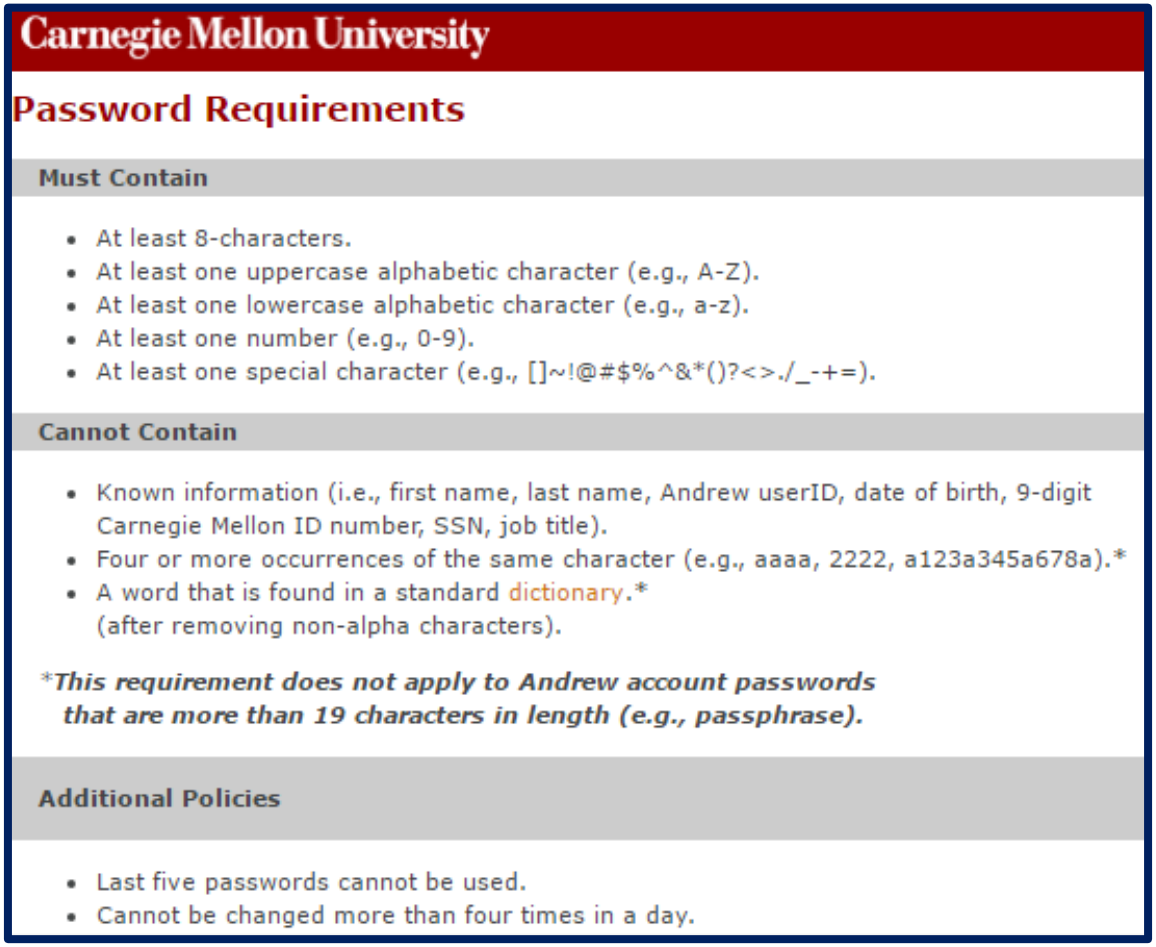
Problem 3: Unhelpful Feedback

Ultimate goal: Help users create better* passwords

Better =

- -More secure?
- -More memorable?
- -More likable?
- -Balance usability & security?

Password-Composition Policies



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.

Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor. Encountering Stronger Password Requirements: User Attitudes and Behaviors. In *Proc. SOUPS*, 2010.

Study goal(s):
*Understand attitudes & behaviors related to creating a new password
*Understand impact of more complex requirements

Method(s):
*Paper survey of 470 CMU affiliates

Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor. Encountering Stronger Password Requirements: User Attitudes and Behaviors. In *Proc. SOUPS*, 2010.

Method

- Passers-by filled out survey in person
  - Demographics
  - Password handling
  - Password composition
  - Password storage/reuse
  - User sentiment

Results

- New requirements can be annoying, but are perceived as good for security
- Forgetting passwords → help desk
- Reusing a password seemed more likely than writing a password down
- Dictionary words & names >80%
- Assumptions about entropy wrong

How do we measure password strength?

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

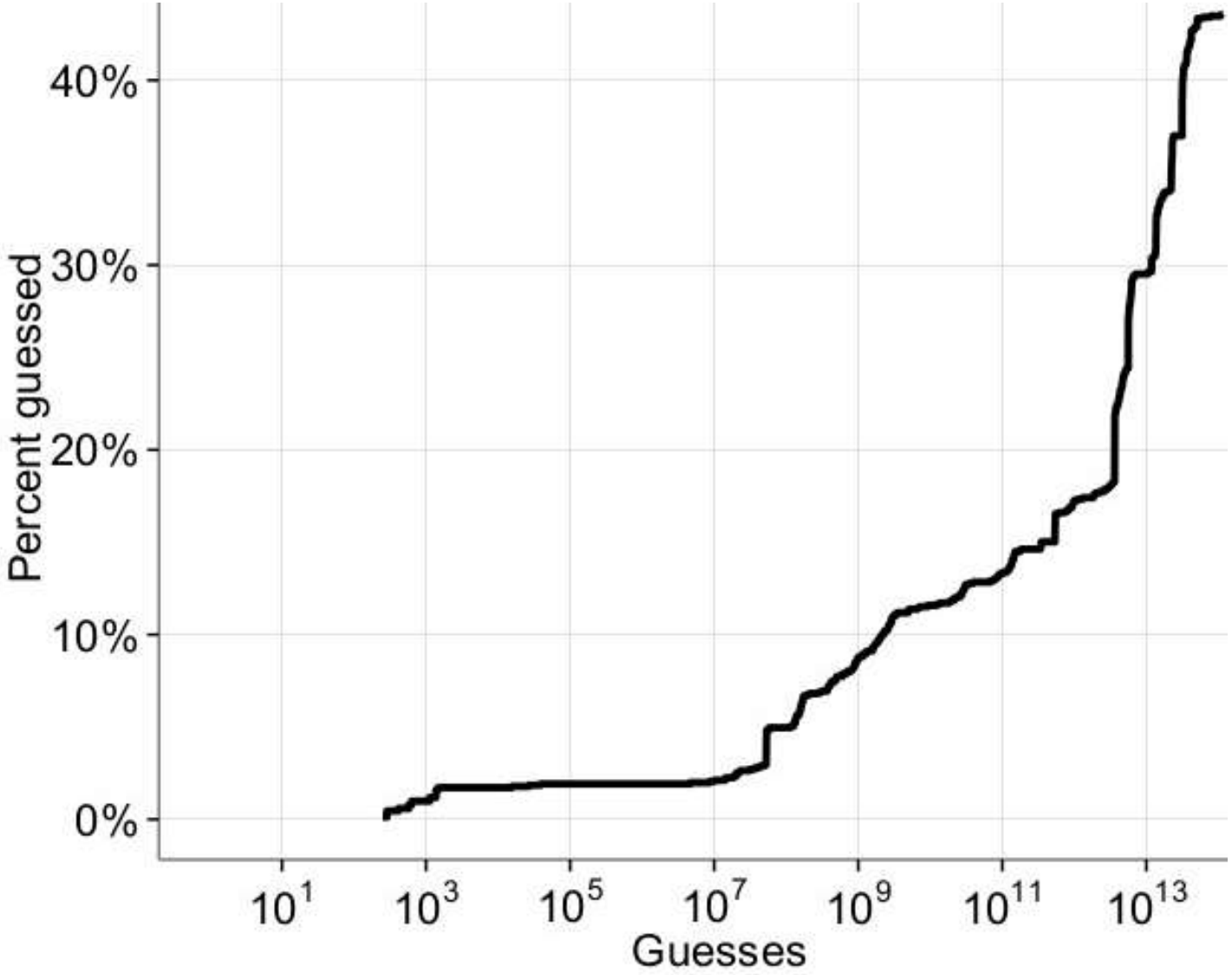
j@mesb0nd007!

Guess # 366,163,847,194

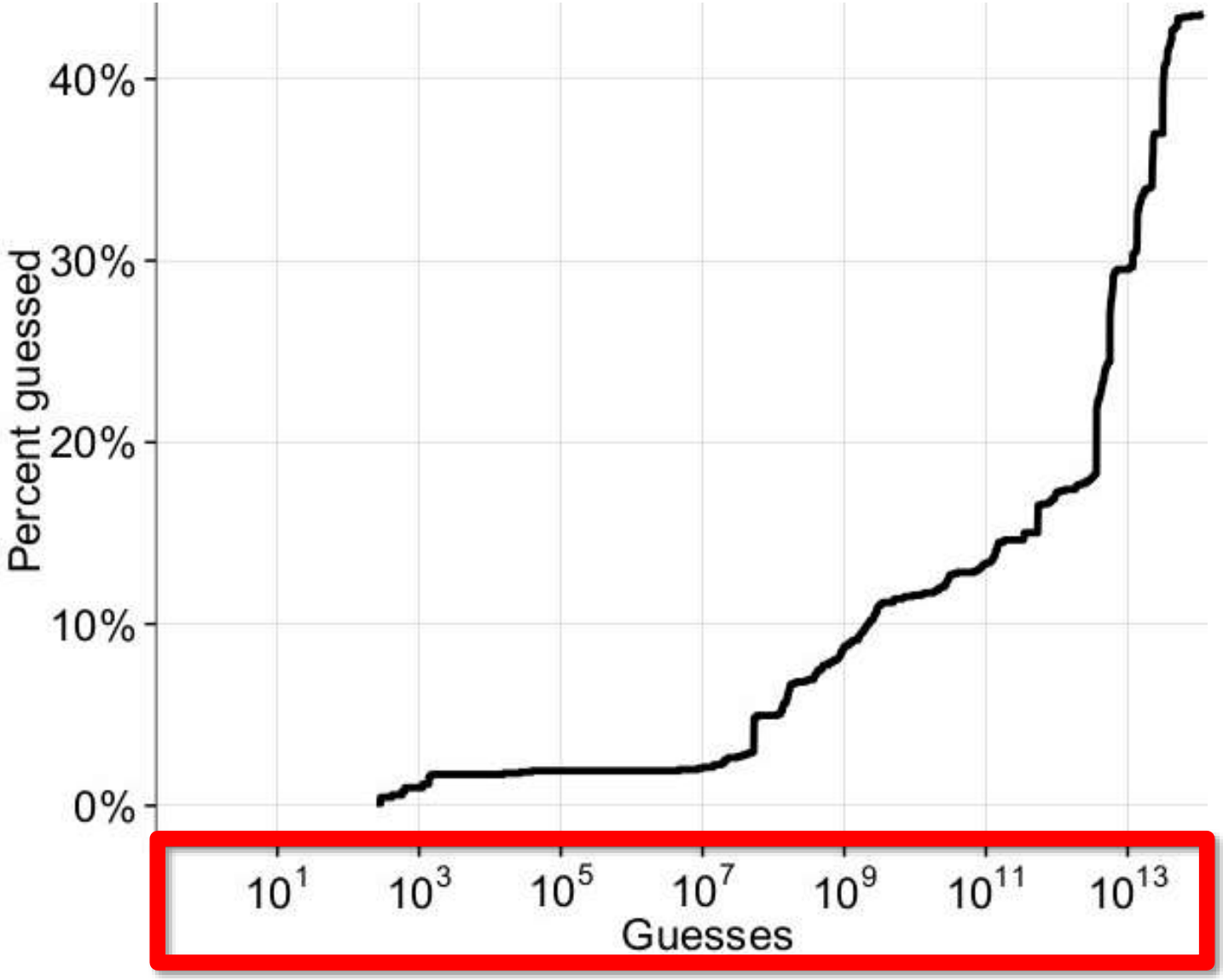
`n(c$JZX!zKc^bIAX^N`

Guess # past cutoff

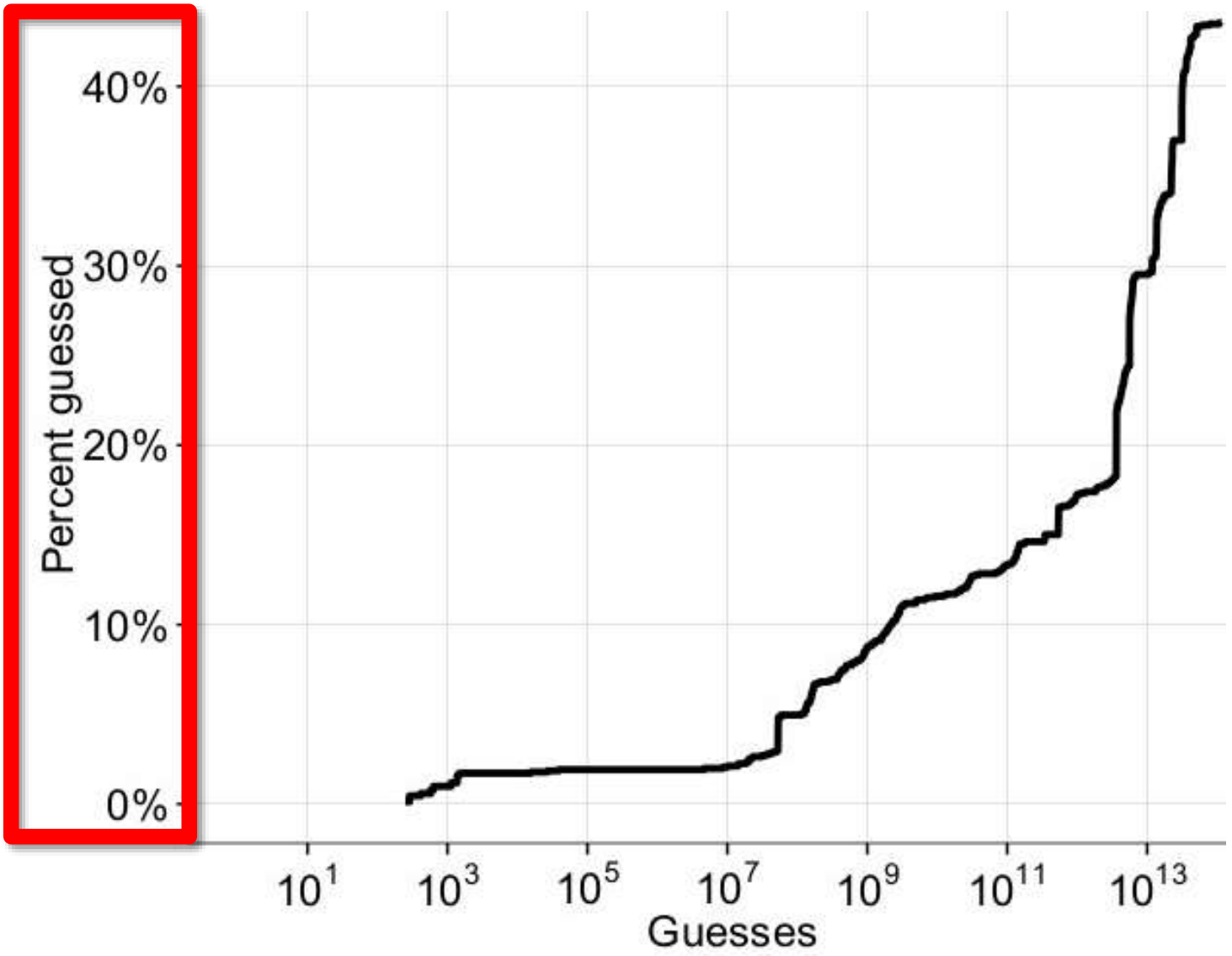
Guessability Plots



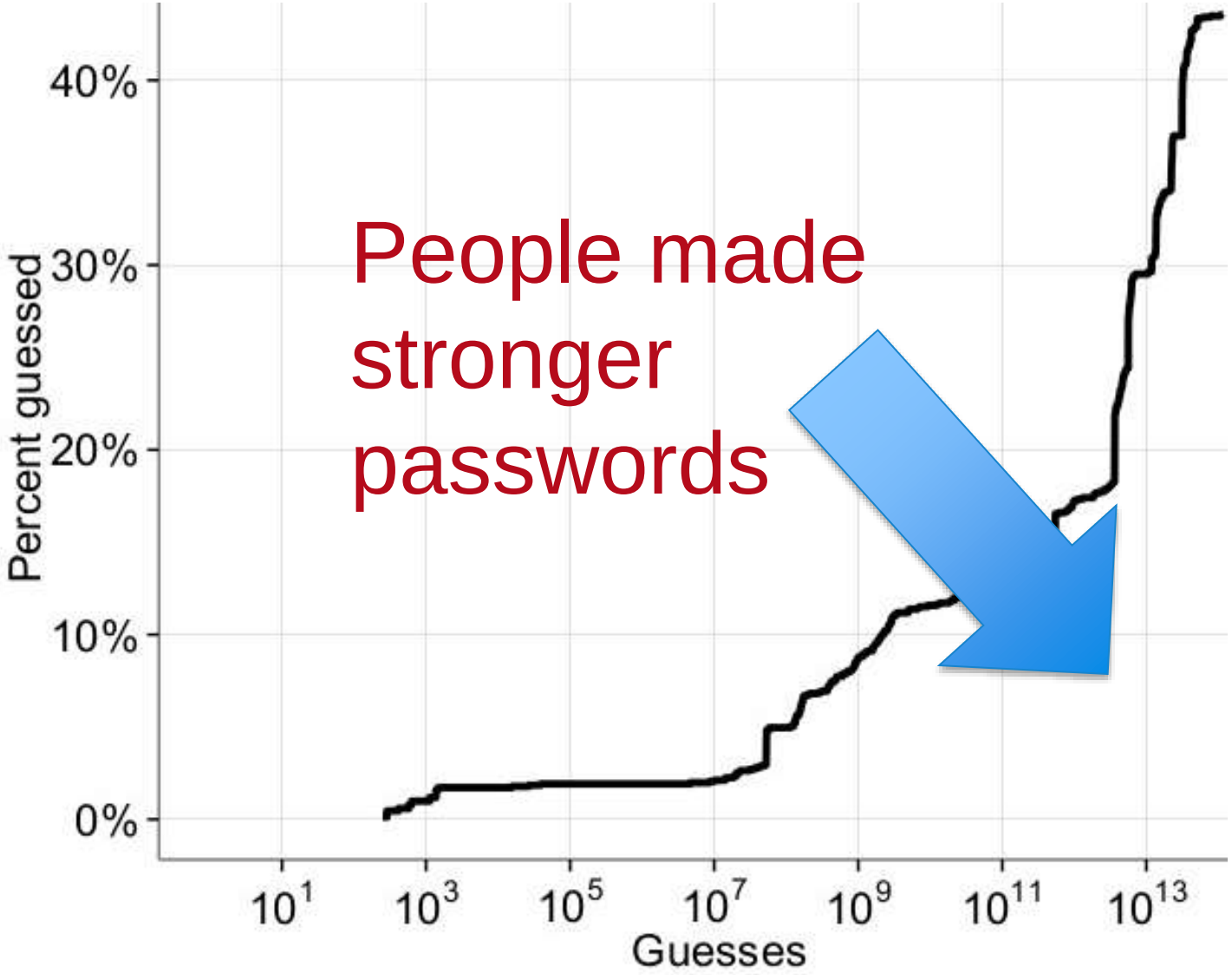
Guessability Plots



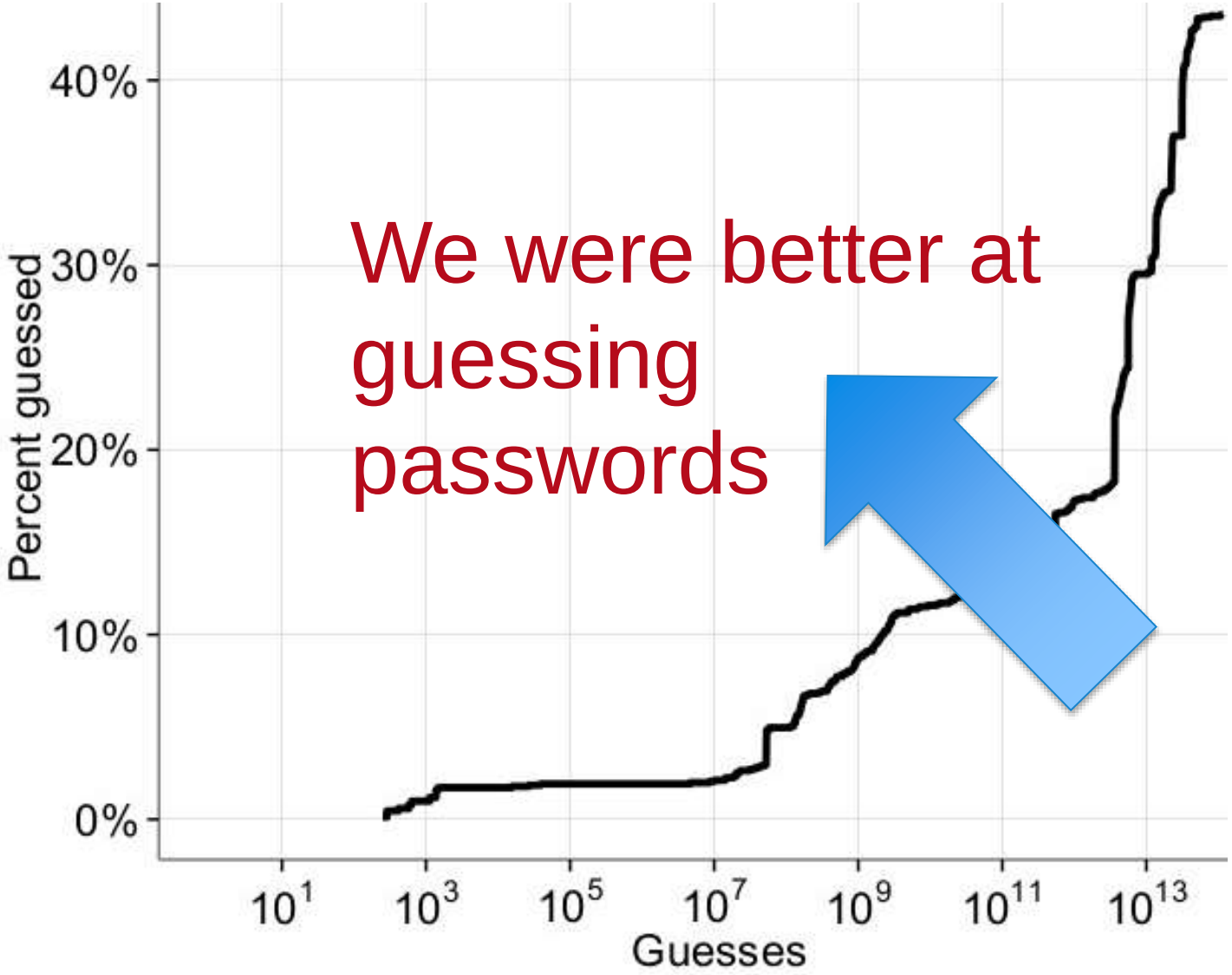
Guessability Plots



Guessability Plots



Guessability Plots



Security & Privacy Impact of Meters

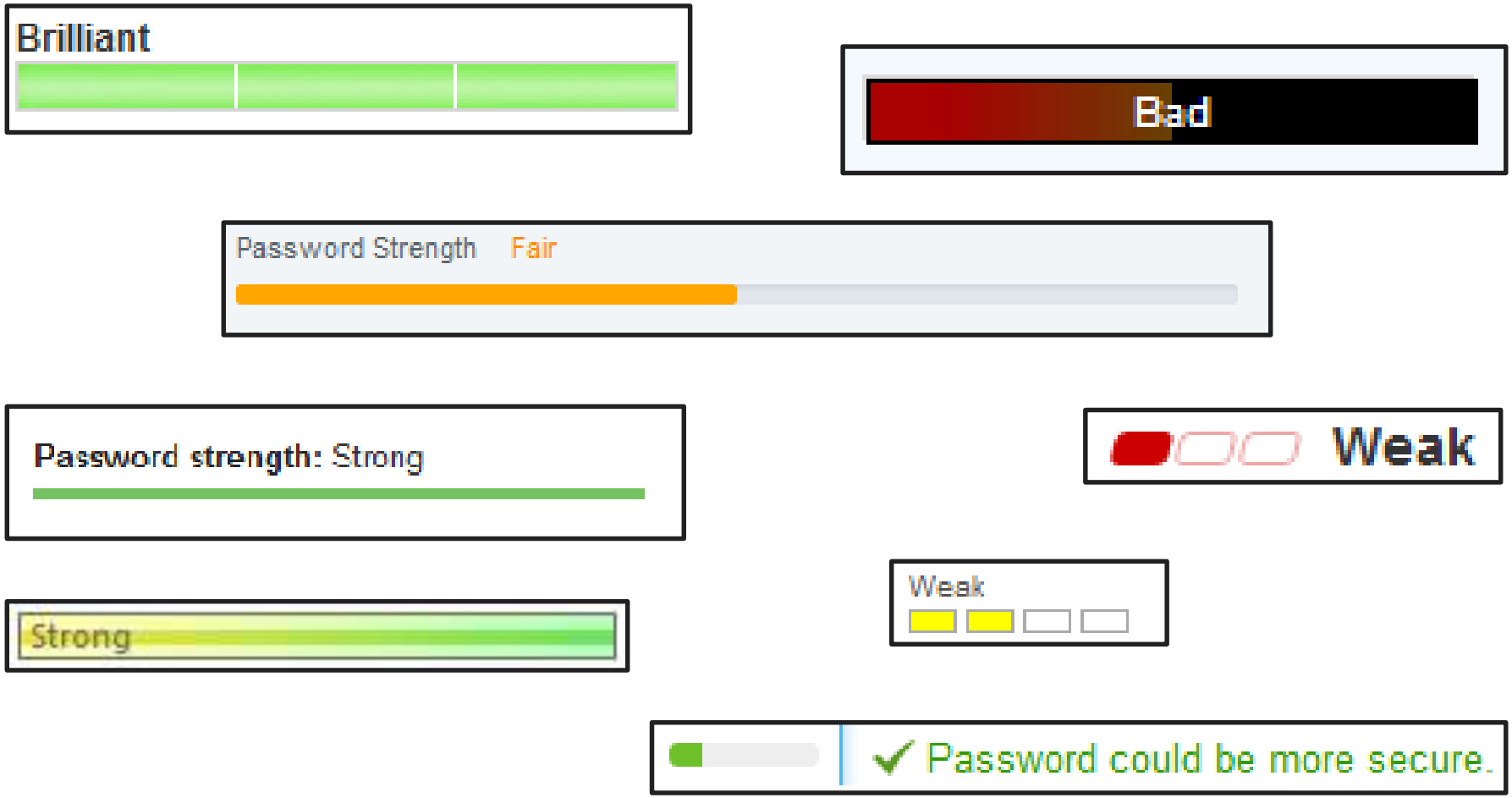
Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In *Proc. USENIX Security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

Study goal(s):
*How do meters impact security & usability of password creation?
*What meter features matter?

Method(s):
*Online study (task + survey) of 2,931 MTurk users

Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor. Encountering Stronger Password Requirements: User Attitudes and Behaviors. In *Proc. SOUPS*, 2010.

Security & Privacy Impact of Meters



Test Impact of Password Meters

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

Study Design

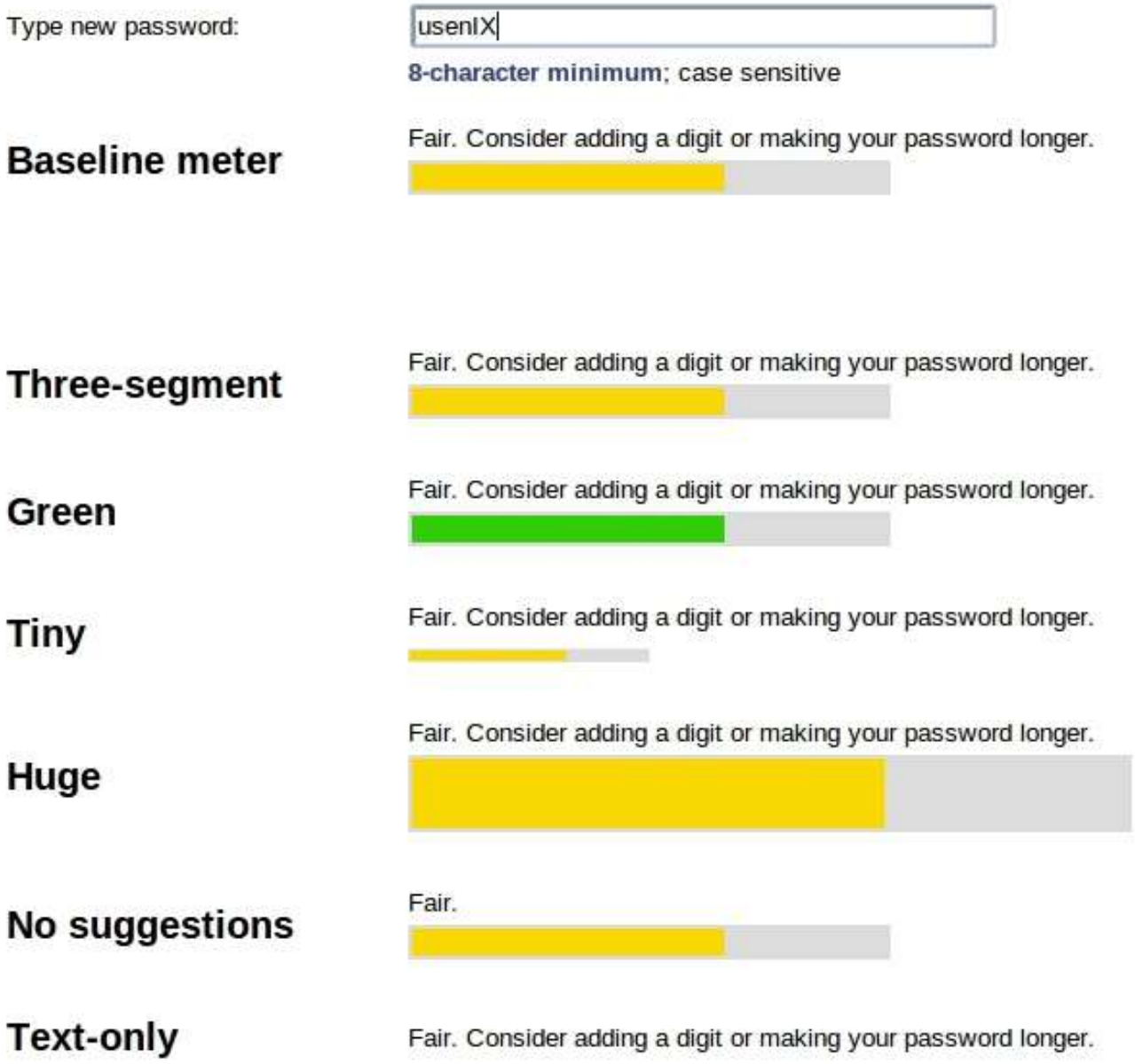
- Password creation
  - Consent process
  - Create password
  - Survey about creating the password
- Recall 1 (right after)
  - Enter password
- Recall 2 (Automated email after 48 hours)
  - Enter password
  - Survey about how they remembered(?) it

Metrics

- Security
  - How guessable is the password? (modeling)
- Usability
  - Write-downs (survey + measurement)
  - Reusing password (survey)
  - Keystroke analysis (measurement)
  - Timing data (measurement)
  - Sentiment about creation (survey)

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.

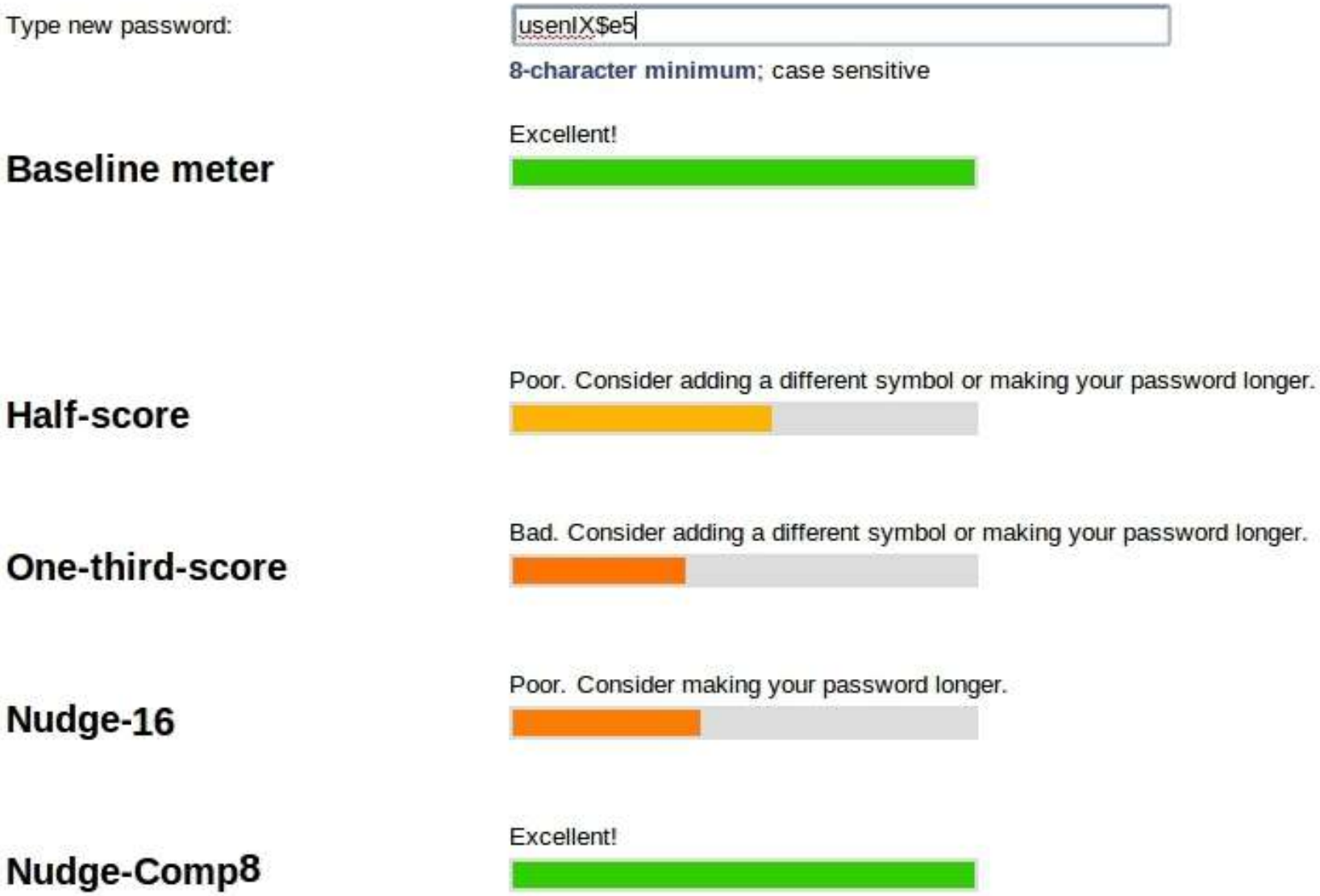
No suggestions

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

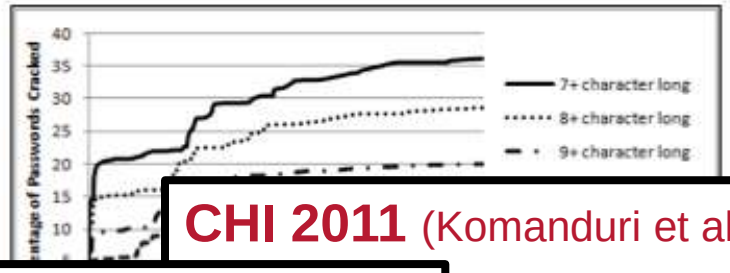
Does this protocol have external validity?

Passwords research is everywhere

CCS 2005 (Narayanan and Shmatikov)

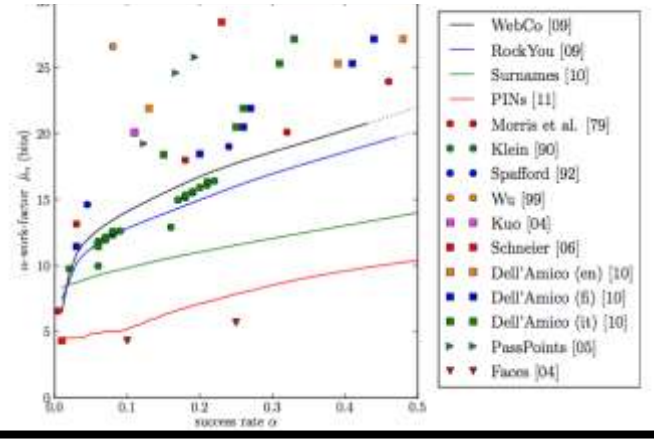
4. INDEXING ALGORITHMS

CCS 2010 (Weir et al.)



CHI 2011 (Komanduri et al.)

IEEE S&P 2012 (Bonneau)



WWW 2007

RockYou	Faithwriters	MySpace
123456	123456	password1
12345	writer	abc123
123456789	jesus1	fuckyou
password	christ	monkey1
iloveyou	blessed	iloveyou1
princess	john316	myspace1
1234567	jesuschrist	fuckyou1
rockyou	password	number1
12345678	heaven	football1
abc123	faithwriters	nicole1

(b) Ten most frequent passwords for different sites. Passwords underlined are shared by at least two services. The wide difference likely depend on background (e.g., Faithwriters) or password rules (e.g., MySpace).

NDSS 2012 (Castelluccia et al.)

. - & _ % ? / + ^ , =) ' (~ : < " ; ` [| >

uency of occurrence of symbols in passwords created in sive8 condition.

… but good data is hard to find

- Small data sets
- Experimental rather than field data
- Self-reported surveys
- Leaked data of questionable validity
- Minimal-value accounts
- No access to plaintext passwords

Are the results generalizable?

Real Passwords

Michelle Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, Blase Ur. Measuring Password Guessability for an Entire University. In *Proc. CCS*, 2013.

Study goal(s):
*Compare passwords used in studies to real passwords
*What factors correlate with password strength?

Method(s):
*Collaborate with InfoSec office to study real passwords

Michelle Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, Blase Ur. Measuring Password Guessability for an Entire University. In *Proc. CCS*, 2013.

Our Data

- 25,000 **real, high-value** passwords
- Contextual data – logs, survey
- What factors correlate with strength?
  - New (to passwords) statistical methods
  - Find new results, confirm prior results
- What to do without field data?
  - Comparison with leaked and study data

Carnegie Mellon

What are CMU passwords?

- 25,459 accounts for faculty, staff, and students
  - Plus 17,104 deactivated accounts
- Single-sign-on for email, financial, grades, registration, health, etc.
- Password requirements:
  - Minimum 8 characters
  - Upper, lower, digit, symbol
  - Dictionary check (241,497 words)

Other CMU data

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

Handling real data securely

- ISO personnel audited and ran our code
  - Isolated machine accessed only by ISO
  - Fun with remote debugging
- Aggregated outputs only
  - All outputs personally reviewed by ISO director

Decryption and anonymization

- Legacy system stored passwords reversibly
  - Decrypted passwords stored only in RAM
- Data sources joined with hashed, salted user ID
  - Salt known only to one staff member
- For analysis, demographic groups binned to minimum 50 users
  - Sometimes required combining categories

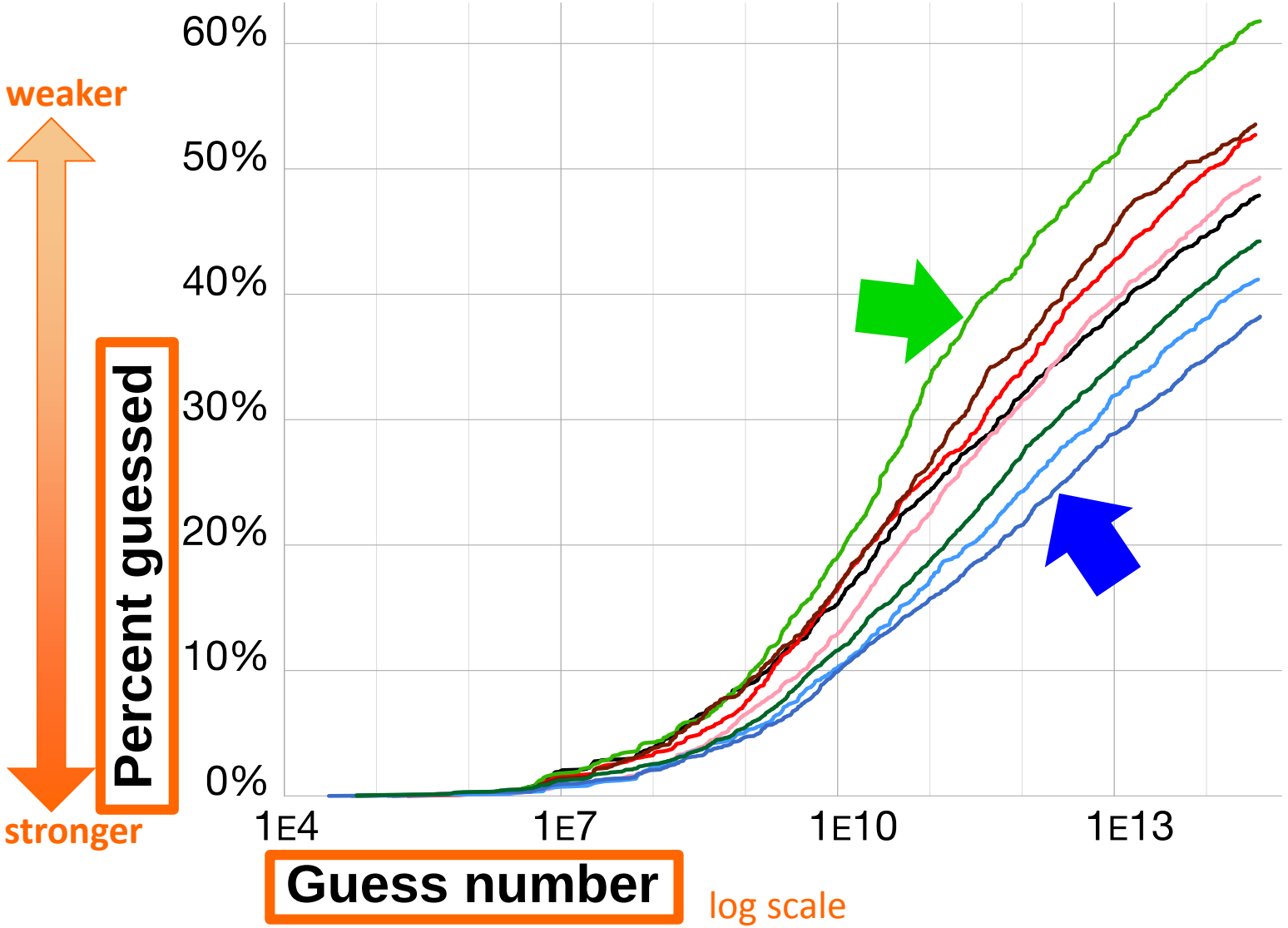
Part 1: Factors affecting strength

- Calculate a strength metric for each password
- Use statistics to correlate password strength with demographics, behavior, etc.

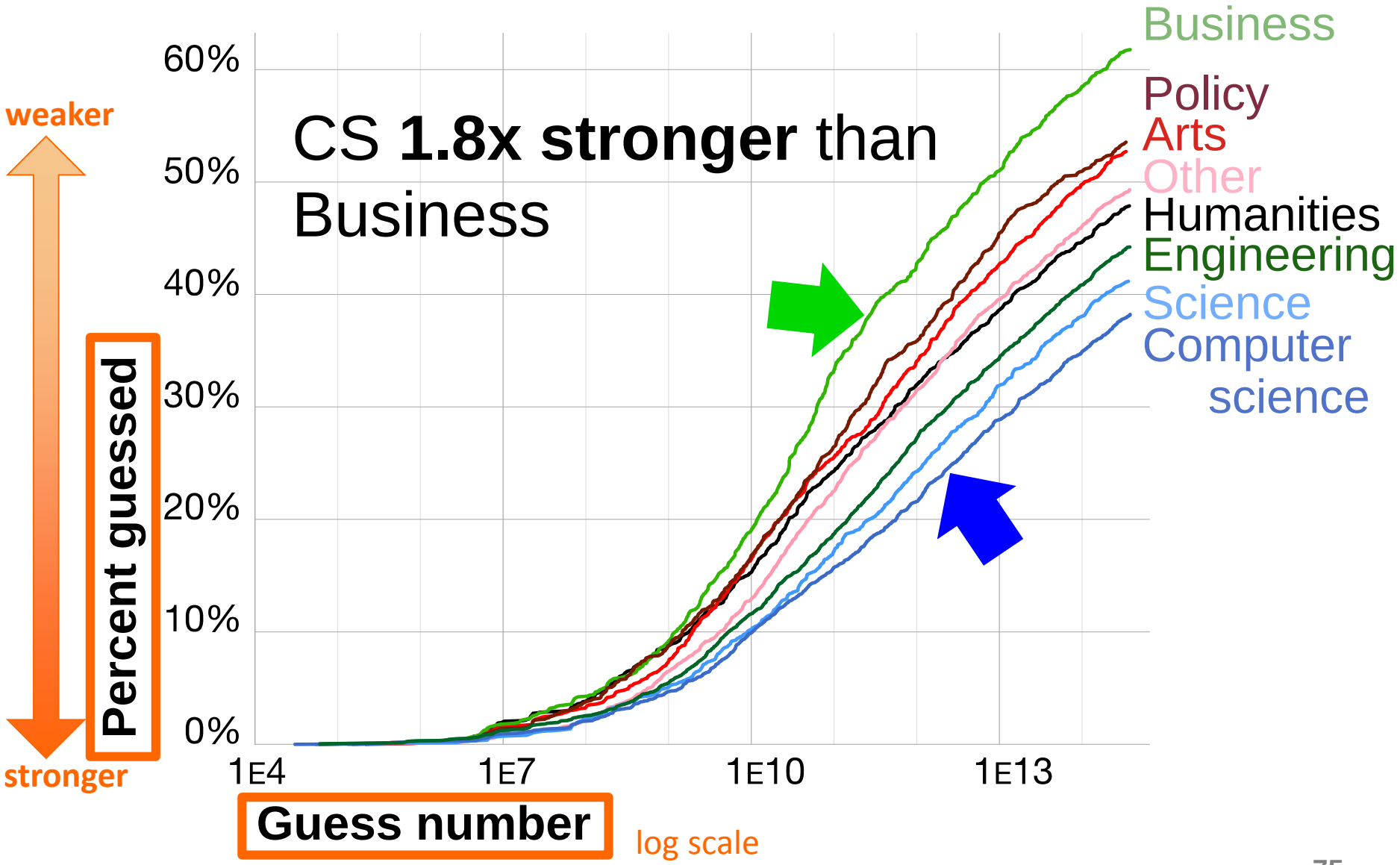
Our guessing configuration

- Modified PCFG algorithm
  - Guesses based on structures, strings in training data
  - Weir et al., S&P 2009; Kelley et al., S&P 2012
- Three **folds** for cross-validation
- Trained on:
  - Inactive CMU passwords
  - Public data (leaks, dictionaries)
  - Other two folds

Results – College affiliation



Results – College affiliation



Conclusions for research

- Study passwords were not a perfect proxy for real, high-value passwords…
- …but, across metrics, they were better than the alternative of leaked passwords

Password Decision-Making

Please create a new password for your news account.

First Trust
National Bank

Please create a new password for your banking account.

SwagMail

Please create a new password for your email account.

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.

Study goal(s):
*Step-by-step, how do users create passwords (and how can we help)?
*How do users value passwords?

Method(s):
*Lab study of 49 participants

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.

password

ilovebillyC$1

ilovebillyC$1

ilovebillyC$1

AfNaHiLoco

AfNaHiLoco

Goals

- Understand precisely how people make passwords
  - In-lab, think-aloud protocol
- How users assign value to accounts
- “Microdecisions” users think add security

Methodology

- 49-participant lab study
- Think aloud while creating 3 passwords:

Qualitative Analysis

- Based on affinity diagramming
- 25 broad themes
  - 122 distinct behaviors

Participants

- 49 participants
  - 21 male
  - 28 female
- Variety of occupations
  - 24 students
  - 16 employed
  - 9 unemployed/retired

Passwords

- Transformed (Fahl et al., SOUPS 2013)
- 6 passwords trivially guessable
  - *gabriel*, *Password1!*
- Half of passwords guessed
  - e.g., *Tyrone1975*, *Gandalf*8*, *Triptrip1963*
- Half of passwords secure
  - e.g., *5cupsoftoys*, *AfNaHiLoco*, *7301Poplarblvd$*

Security Levels

- 21 participants considered sites equal value
- Struggled matching password to security level
  - P6's high-value passwords both guessed

Strategies

Base password on site

- Insecure banking password

```
+Money369
```

Base password on site

- Insecure banking password

+Money369

Base password on site

- Insecure banking password

+Money369

Base password on site

- Secure news password

```
LEFTbrown8!
```

Base password on site

- Secure news password

LEFTbrown8!

Base password on site

- Secure news password

LEFTbrown8!

Base password on site

- Secure news password

LEFTbrown8!

Knew to avoid dictionary words

Knew to avoid dictionary words

- Insecure keyboard patterns

```
1Qazxsw2
```

Knew to avoid dictionary words

- Secure (believed insecure)

`junglesalmon711`

Knew to avoid dictionary words

- Secure (and believed secure)

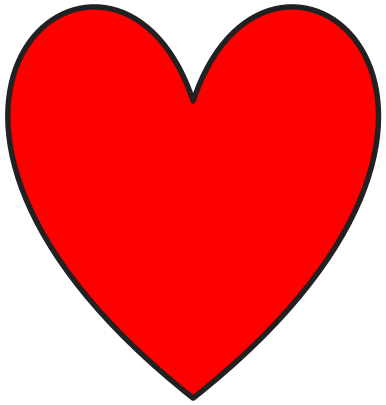
`Rjunglesalmon711@$`

Build password around phrase

Build password around phrase

- Insecure

```
ilove1sttrust!
```



Build password around phrase

- Secure

```
AfNaHiLoco
```

Build password around phrase

- Secure

`AfNaHiLoco`

Afraid of the Native Hipsters
Loopily Coding

Digits and symbols make it secure

- Insecure

Tyrone

Digits and symbols make it secure

- Insecure (believed secure)
  - “Security is required for a bank account” (P37)

`Tyrone1975`

Digits and symbols make it secure

- “I added ‘!’ at the end to make it secure.” (P45)

Misunderstanding attackers

Misunderstanding attackers

- Mahavishnu Orchestra is secure because "this band name is hard to spell" (P2)

Misunderstanding attackers

- Mahavishnu Orchestra is secure because "this band name is hard to spell" (P2)

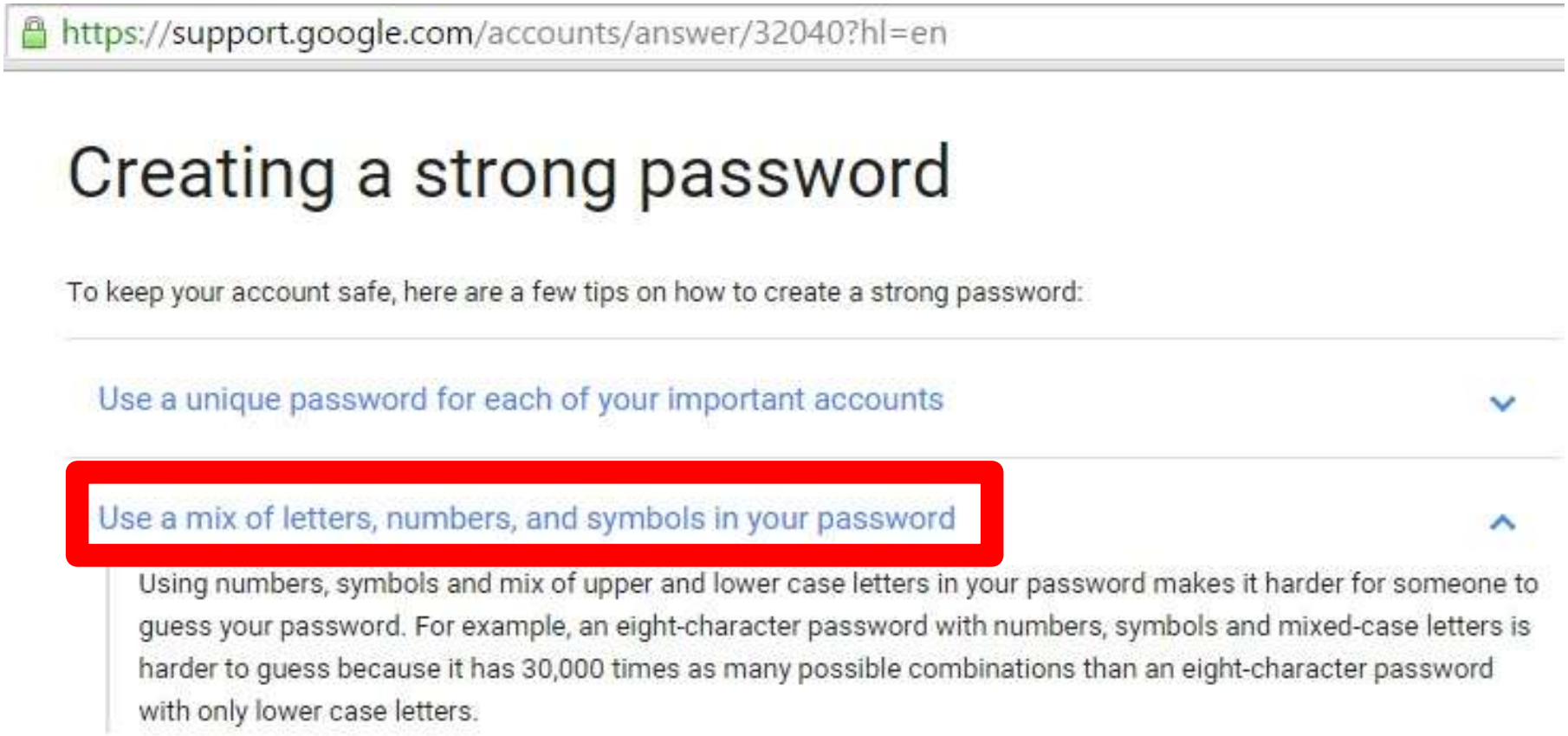
- Goldie: "hackers cannot guess [it] because I have no pictures of him on my Facebook account." (P7)

Conclusions

- Users had process, yet many misconceptions

Conclusions

- Users had process, yet many misconceptions



Conclusions

- Users had process, yet many misconceptions

Cannot Contain:

- known personal information
- last five passwords
- four or more occurrences of same character*
- a Dictionary word* (after removing non-alpha characters)

Conclusions

- Users had process, yet many misconceptions

Cannot Contain:

- known personal information
- last five passwords
- four or more occurrences of same character*
- a Dictionary word* (after removing non-alpha characters)

Retrospective Understanding

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, 2013. Image Creative Commons by Lasya J on Flickr.

Study goal(s):
*Unpack linguistic features
*What structures are common

Method(s):
*Analyze previously created passwords
*MTurk reverse-engineering

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.

Reverse-Engineering Passwords

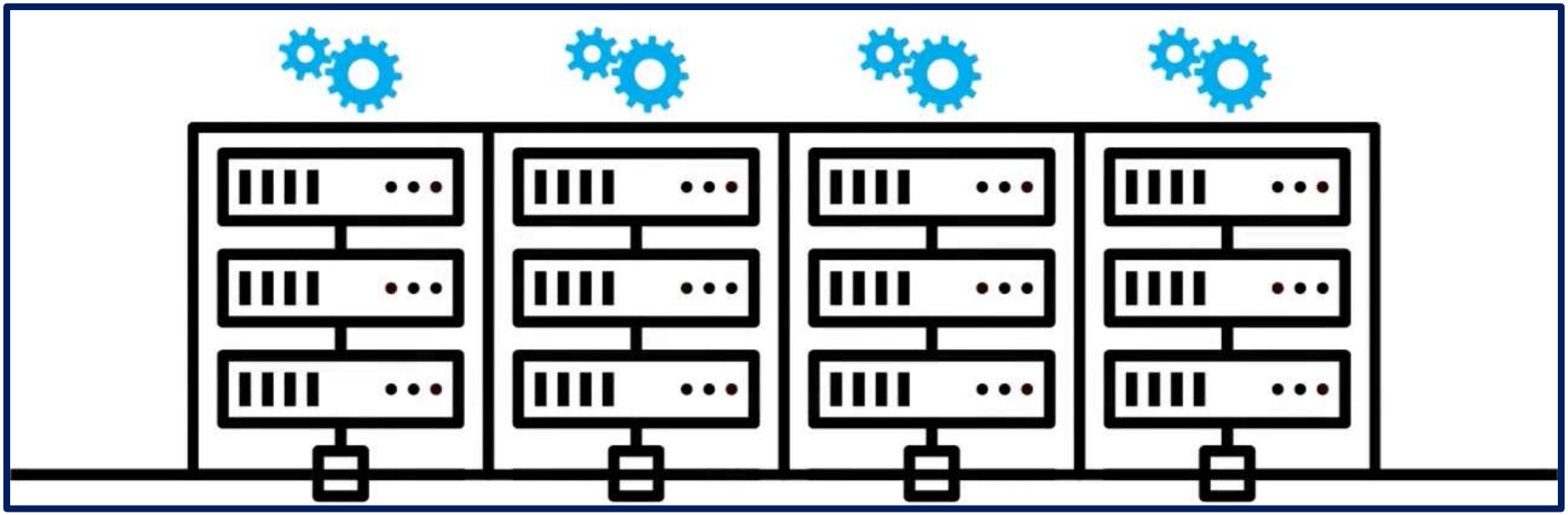
~Cowscomehom3

“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

Modeling Password Cracking



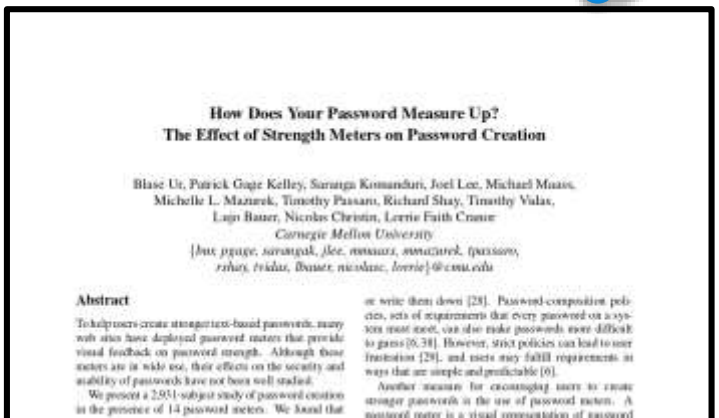
Blase Ur, Sean M. Segreti, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Saranga Komanduri, Darya Kurilova, Michelle L. Mazurek, William Melicher, Richard Shay. Measuring Real-World Accuracies and Biases in Modeling Password Guessability. In *Proc. USENIX Security Symposium*, 2015.

Study goal(s):
*How does our choice of password-strength metric impact results?
*Do experts do better?

Method(s):
*Model cracking approaches
*Hire pen-testing firm (& compare)

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.

Guessability in Concept



How Does Your Password Measure Up?
The Effect of Strength Meters on Password Creation

Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass,
Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas,
Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor
Carnegie Mellon University
{*bur, pgage, sarangak, jdlee, mmaass, mmazurek, tpassaro, rshay, tvidas, lbauer, nicolasc, loerie*}*@cmu.edu*

Abstract

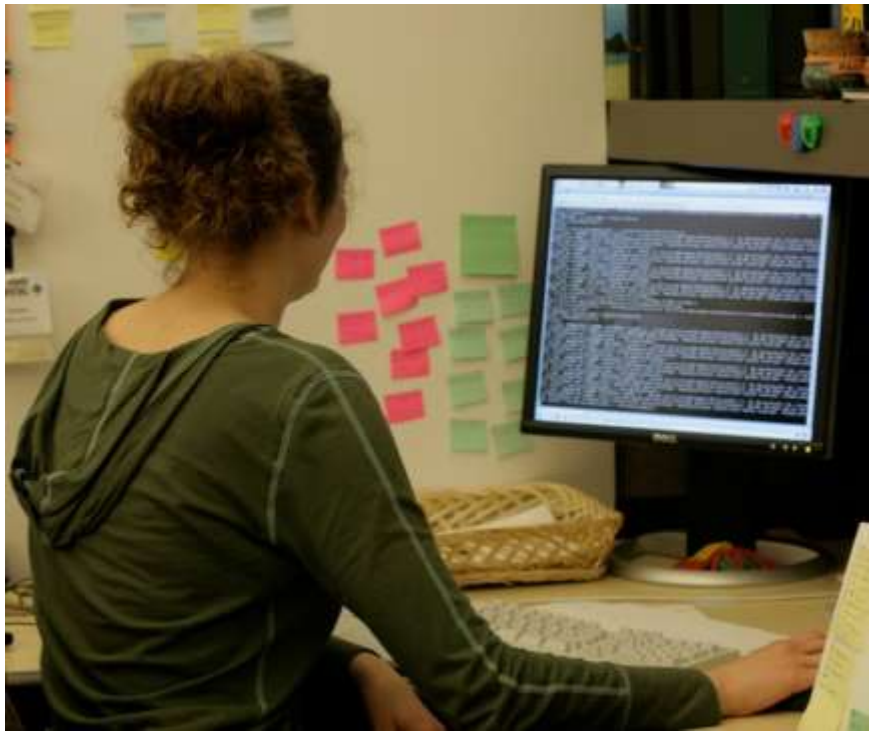
To help users create stronger text-based passwords, many web sites have deployed password meters that provide visual feedback on password strength. Although these meters are in wide use, their effects on the security and usability of passwords have not been well studied.

We present a 2,931-subject study of password creation in the presence of 14 password meters. We found that

or write them down [28]. Password-composition policies, sets of requirements that every password on a system must meet, can also make passwords more difficult to guess [6, 38]. However, strict policies can lead to user frustration [28], and users may fulfill requirements in ways that are simple and predictable [6].

Another measure for encouraging users to create stronger passwords is the use of password meters. A password meter is a visual representation of password

Guessability in Practice



Approach

4 password sets

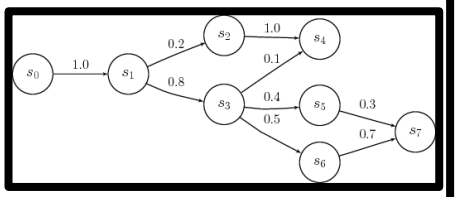
```
password
iloveyou
teamo123
…
```

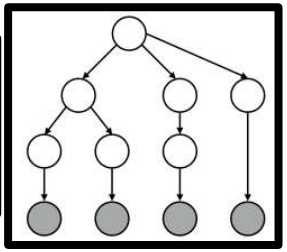
```
passwordpassword
1234567812345678
!1@2#3$4%5^6&7*8
…
```

```
Pa$$w0rd
iLov3you!
1QaZ2W@x
…
```

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

✖ 5 approaches





KoreLogic SECURITY

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

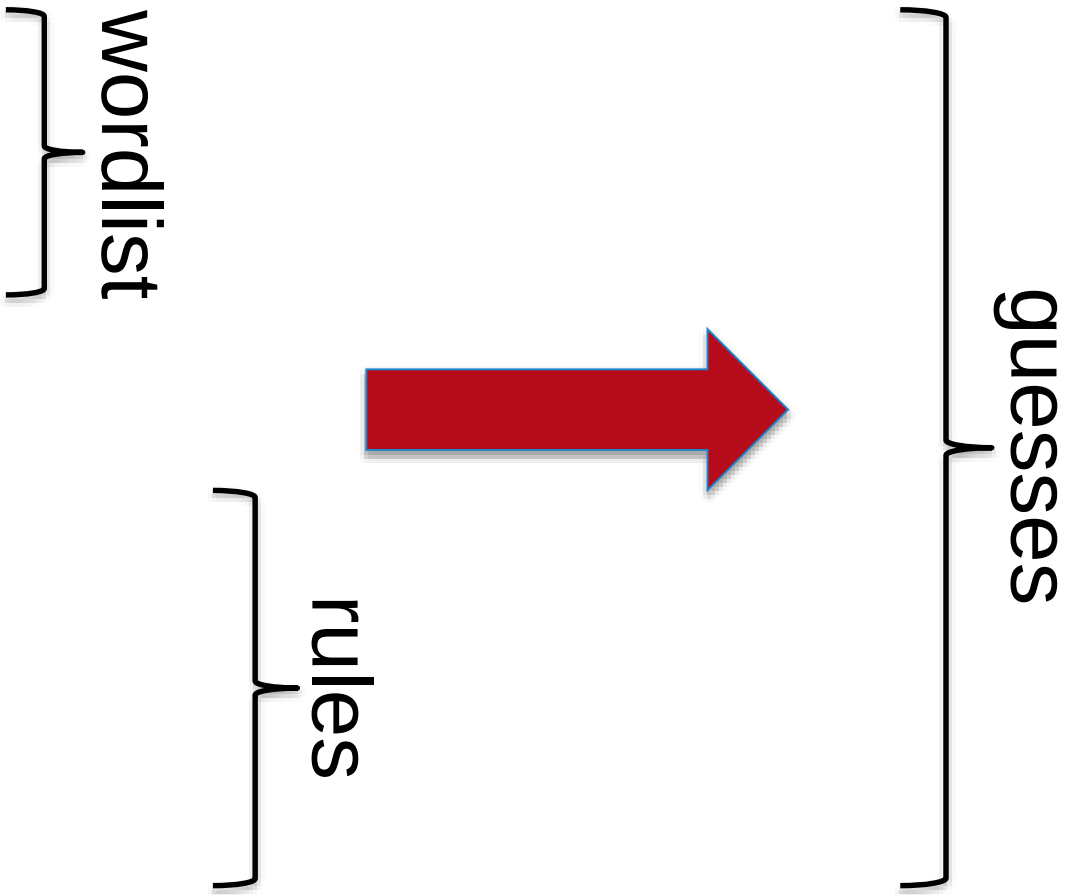
John the Ripper

- 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



John the Ripper

usenix

security

wordlist

rules

guesses

John the Ripper

usenix

security

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

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

John the Ripper

usenix

security

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

usenix

security

usenix1

security1

us3nix

s3curity

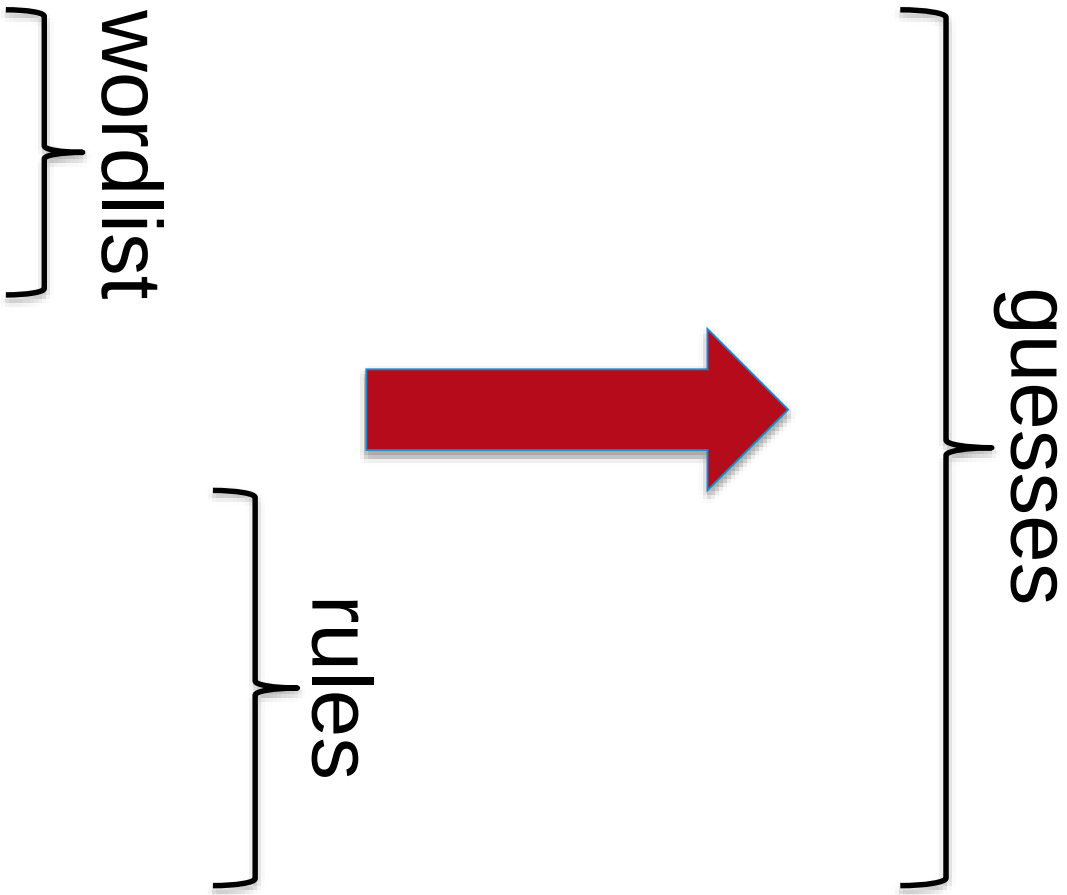
guesses

Hashcat

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

Hashcat


hashcat
advanced
password
recovery


wordlist
rules
guesses

Hashcat

usenix

security

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

guesses

Hashcat

usenix

security

wordlist

usenix

usenix1

us3nix

[ ]

[add 1 at end]

[change e to 3]

rules

security

security1

s3curity

guesses

Hashcat

usenix

security

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

usenix

usenix1

us3nix

security

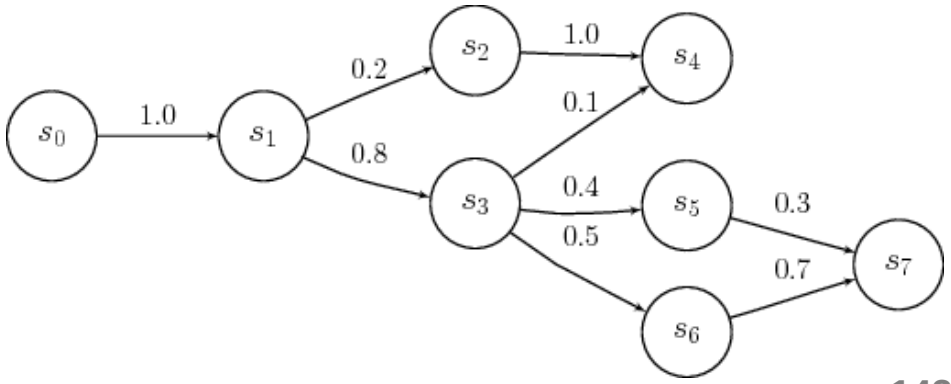
security1

s3curity

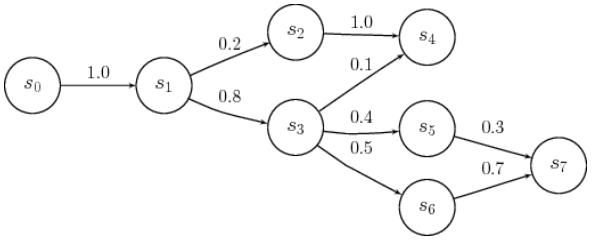
guesses

Markov Models

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

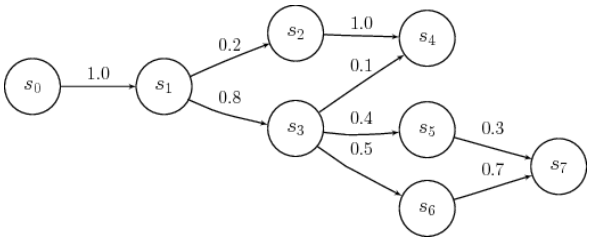


Markov Models



cincinnati

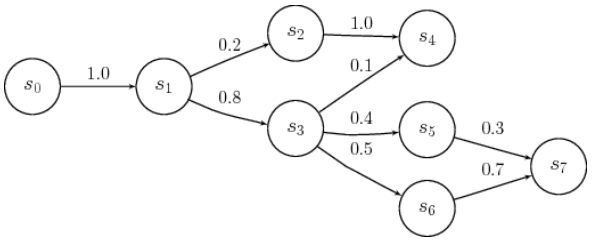
Markov Models



Markov chain of order 3 (4-grams)

___ → c *1.0*

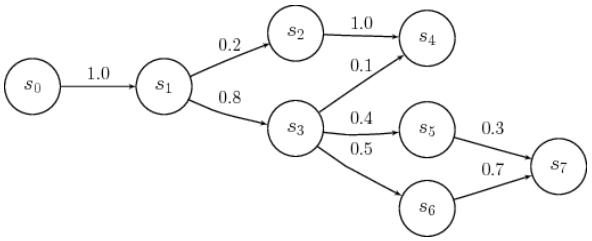
Markov Models



cincinnati

___ → c *1.0*
__c → i *1.0*

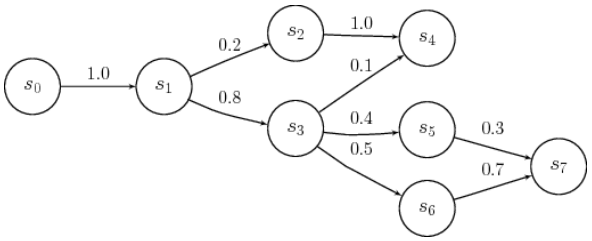
Markov Models



cincinnati

___ → c *1.0*
__c → i *1.0*
_ci → n *1.0*

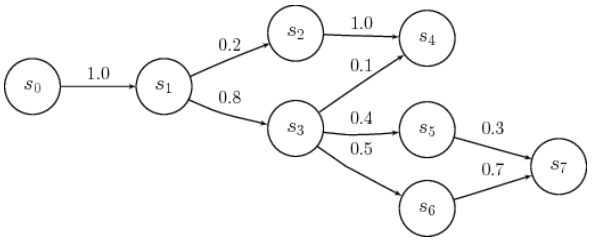
Markov Models



cincinnati

___ → c *1.0*
__c → i *1.0*
_ci → n *1.0*
cin → c *1.0*

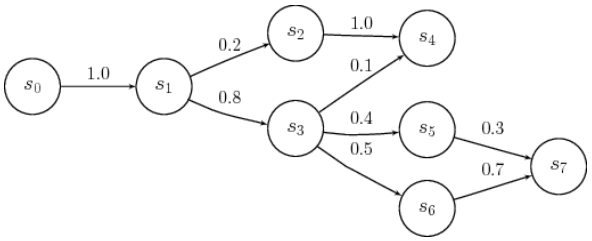
Markov Models



cincinnati

___ → c *1.0*
__c → i *1.0*
_ci → n *1.0*
cin → c *1.0*
inc → i *1.0*

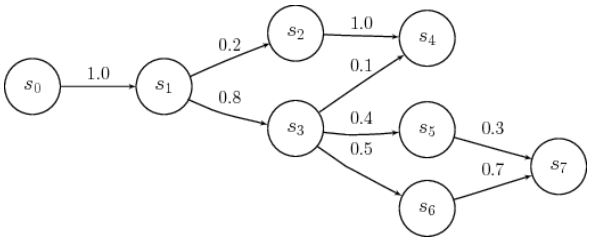
Markov Models



cincinnati

___ → c	*1.0*
__c → i	*1.0*
_ci → n	*1.0*
cin → c	*1.0*
inc → i	*1.0*
nci → n	*1.0*

Markov Models

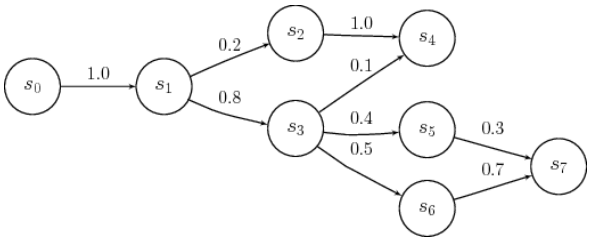


cincinnati

___ → c *1.0*
__c → i *1.0*
_ci → n *1.0*
cin → c *0.5*
cin → n *0.5*
inc → i *1.0*

nci → n *1.0*

Markov Models

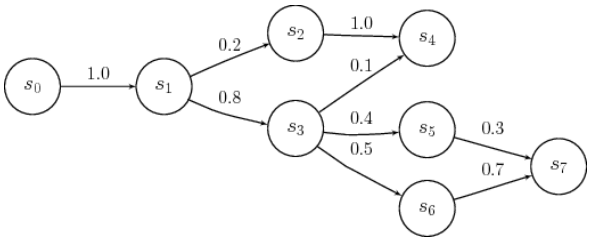


cincinnati

___ → c *1.0*
__c → i *1.0*
_ci → n *1.0*
cin → c *0.5*
cin → n *0.5*
inc → i *1.0*

inn → a *1.0*
nci → n *1.0*

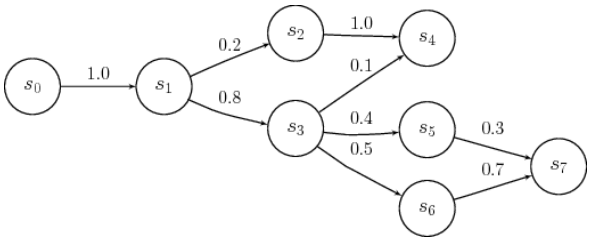
Markov Models



cincinnati

___ → c	*1.0*	inn → a	*1.0*
__c → i	*1.0*	nci → n	*1.0*
_ci → n	*1.0*	nna → t	*1.0*
cin → c	*0.5*		
cin → n	*0.5*		
inc → i	*1.0*		

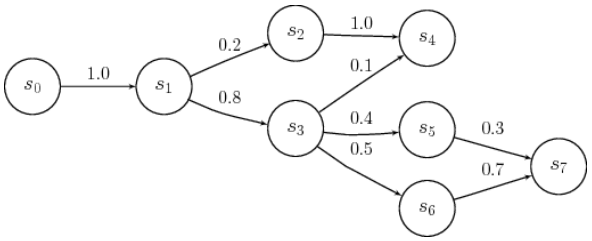
Markov Models



cincinnati

___ → c	*1.0*	inn → a	*1.0*
__c → i	*1.0*	nat → i	*1.0*
_ci → n	*1.0*	nci → n	*1.0*
cin → c	*0.5*	nna → t	*1.0*
cin → n	*0.5*		
inc → i	*1.0*		

Markov Models

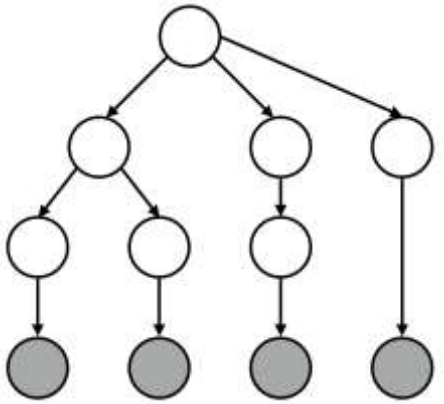


cincinnati

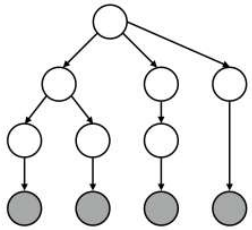
___ → c	*1.0*	inc → i	*1.0*
__c → i	*1.0*	inn → a	*1.0*
_ci → n	*1.0*	nat → i	*1.0*
ati → [end]	*1.0*	nci → n	*1.0*
cin → c	*0.5*	nna → t	*1.0*
cin → n	*0.5*		

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

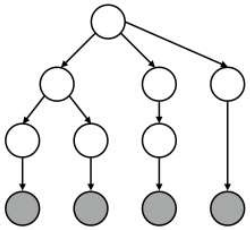
usenix3

5ecurity

iloveyou

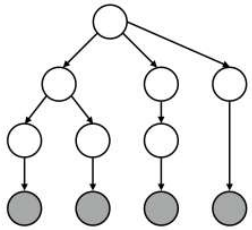
nirvana123

PCFG



passwordpassword	L_{16}	1/6
password123	$L_8 D_3$	1/6
usenix3	$L_6 D_1$	1/6
5ecurity	$D_1 L_7$	1/6
iloveyou	L_8	1/6
nirvana123	$L_7 D_3$	1/6

PCFG



passwordpassword

password123

usenix3

5ecurity

iloveyou

nirvana123

D_3

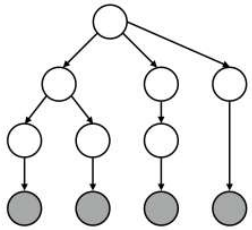
123: *1.0 probability*

D_1:

3: *0.50 probability*

5: *0.50 probability*

PCFG



passwordpassword

password123

usenix3

5ecurity

iloveyou

nirvana123

L_8

password: *0.5*

iloveyou: *0.5*

L_7

ecurity: *0.5*

nirvana: *0.5*

etc.

Key Results

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

Per-Password Highly Impacted

P@ssw0rd!

Per-Password Highly Impacted

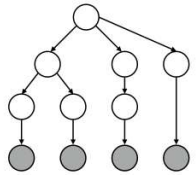
- JTR guess # 801 


```
P@ssw0rd!
```

Per-Password Highly Impacted

- JTR guess # 801

- Not guessed in 10^{14} PCFG guesses

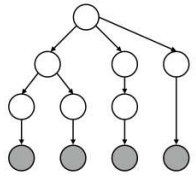


P@ssw0rd!

Per-Password Highly Impacted

- JTR guess # 801

- Not guessed in 10^{14} PCFG guesses



P@ssw0rd!

Password Guessability Service (PGS)

- Guessability of plaintext passwords

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

https://pgs.ece.cmu.edu


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

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.

Study goal(s):
*Do users have misconceptions about passwords?
*(Future) fix these misconceptions

Method(s):
*Online survey of 165 MTurkers

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

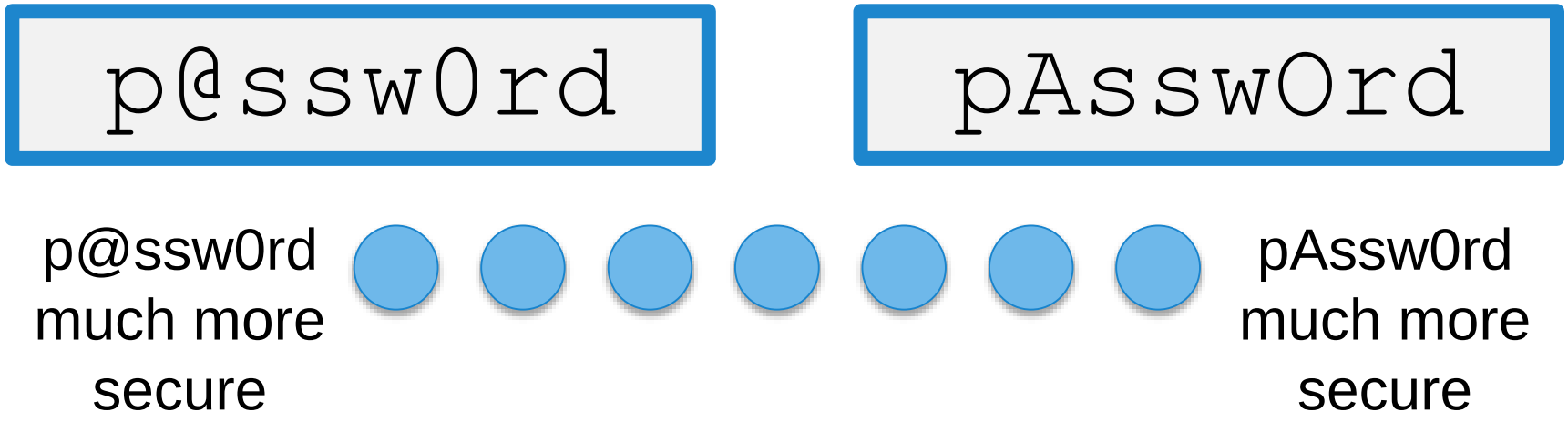
Compare actual strength of passwords to users' perceptions

Study Tasks

1. Evaluating password pairs

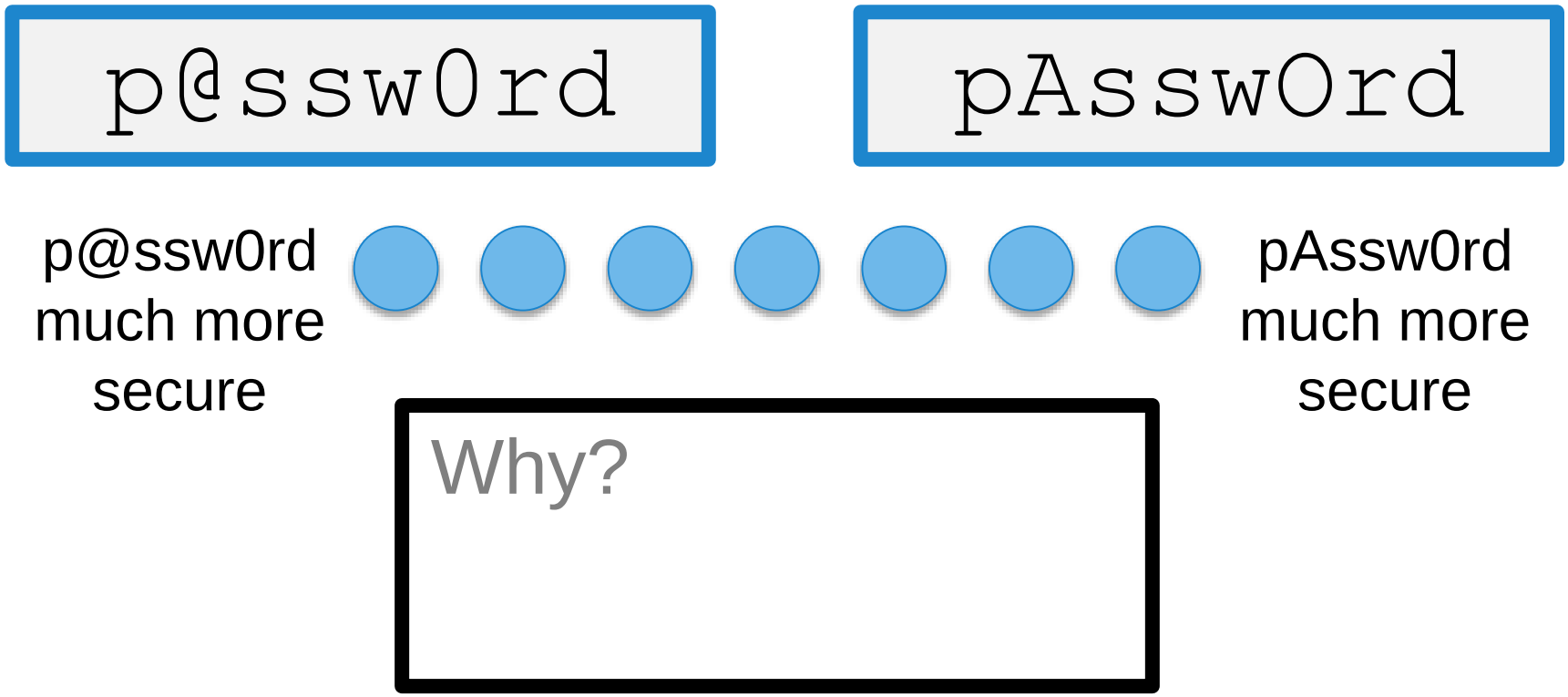
Study Tasks

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
- 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

Evaluating Password Pairs

`iloveyou88`

`ieatkale88`

Evaluating Password Pairs

`iloveyou88`

`ieatkale88`

Evaluating Password Pairs

`iloveyou88`

`ieatkale88`

4,000,000,000 × more secure!

Evaluating Password Pairs

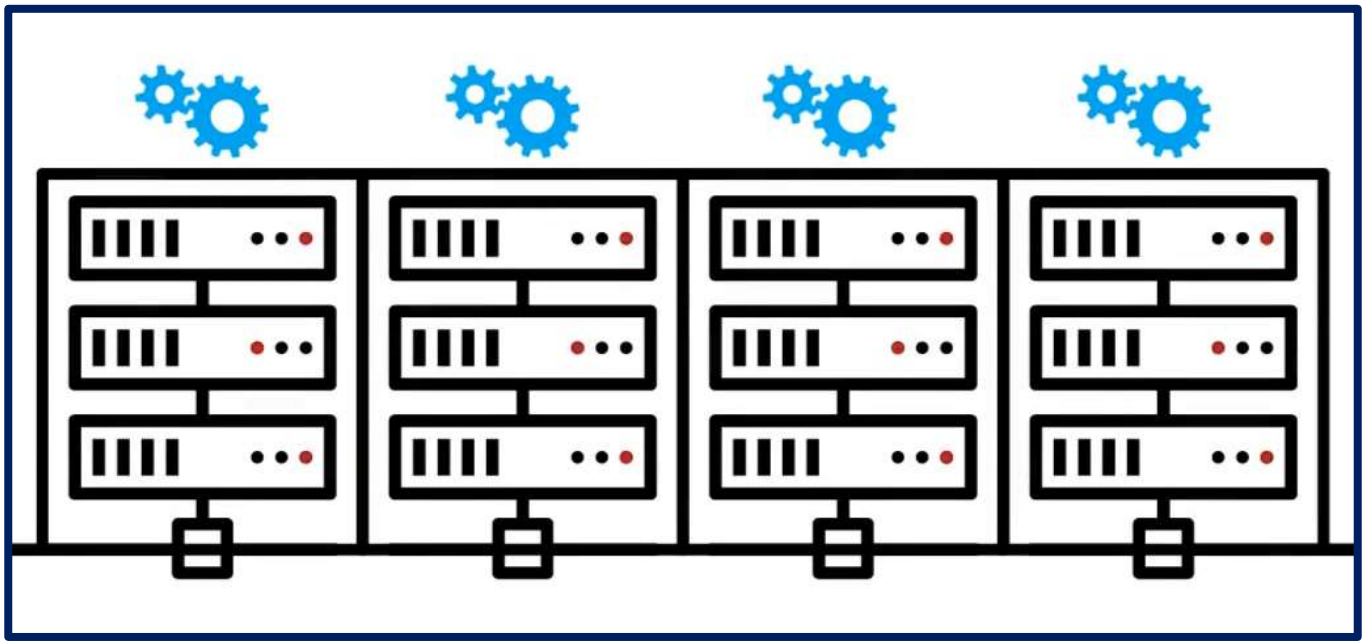
`iloveyou88`

`ieatkale88`

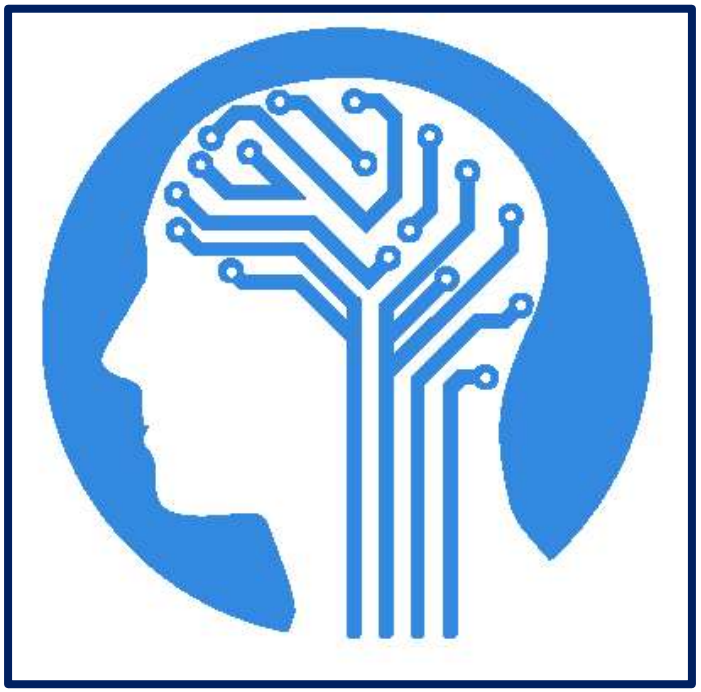
Weren’t we supposed to be helping people make better* passwords?

Better Password Scoring

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



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.

Study goal(s):
*Can we guess passwords better?
*Can we do so client-side?

Method(s):
*Write software
*Comparatively evaluate NN configurations

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.

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

“”

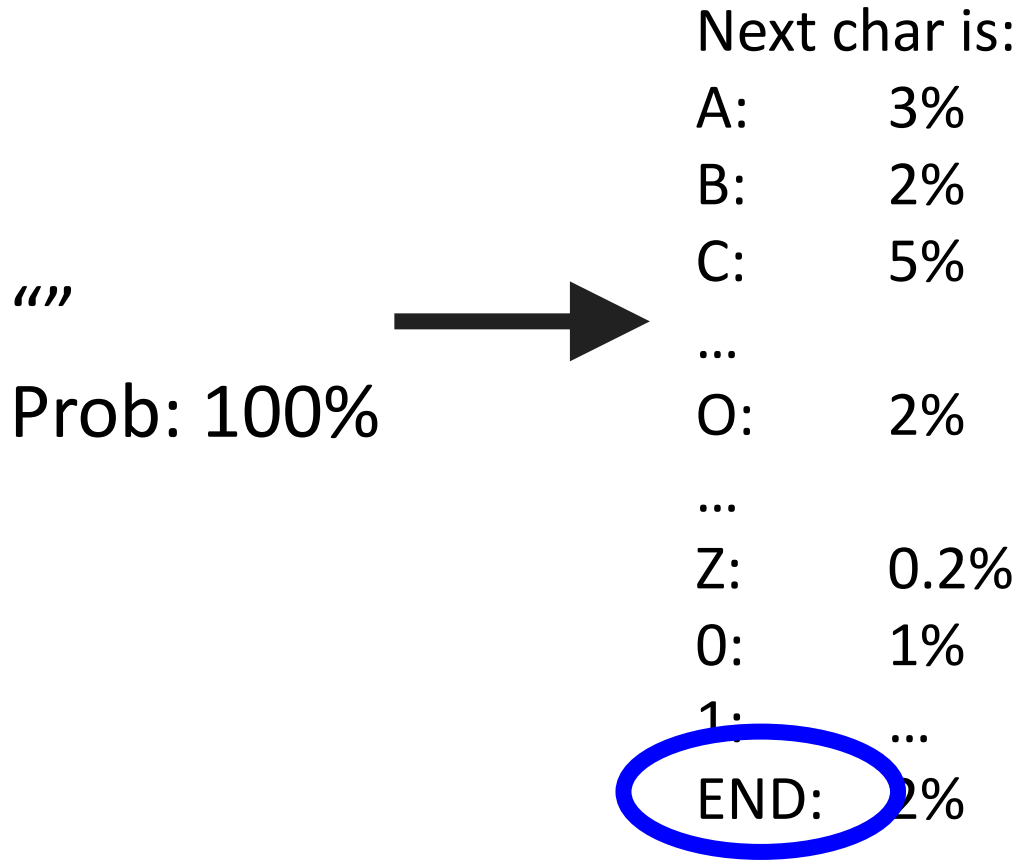
Prob: 100%

Next char is:

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

190

Generating Passwords



191

Generating Passwords

“”

Prob: 100%

Next char is:

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

192

Generating Passwords

“C”

Prob: 5%

193

Generating Passwords

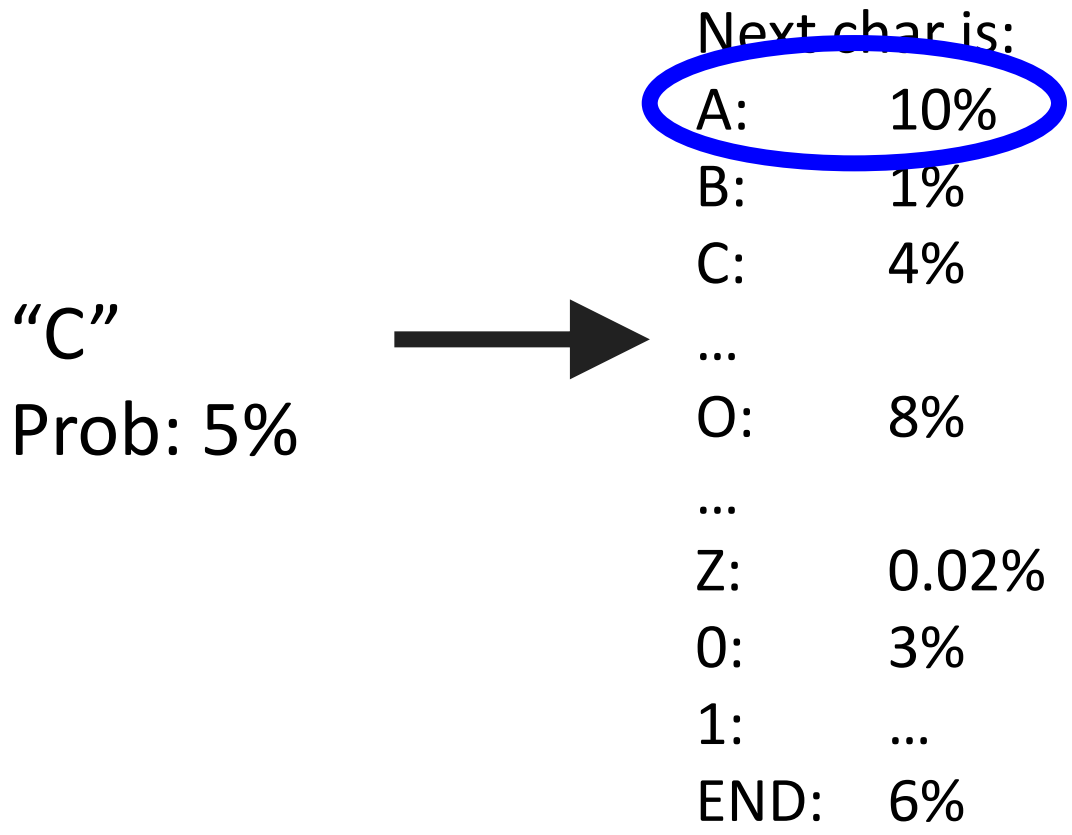
“C”
Prob: 5%

Next char is:

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

194

Generating Passwords



195

Generating Passwords

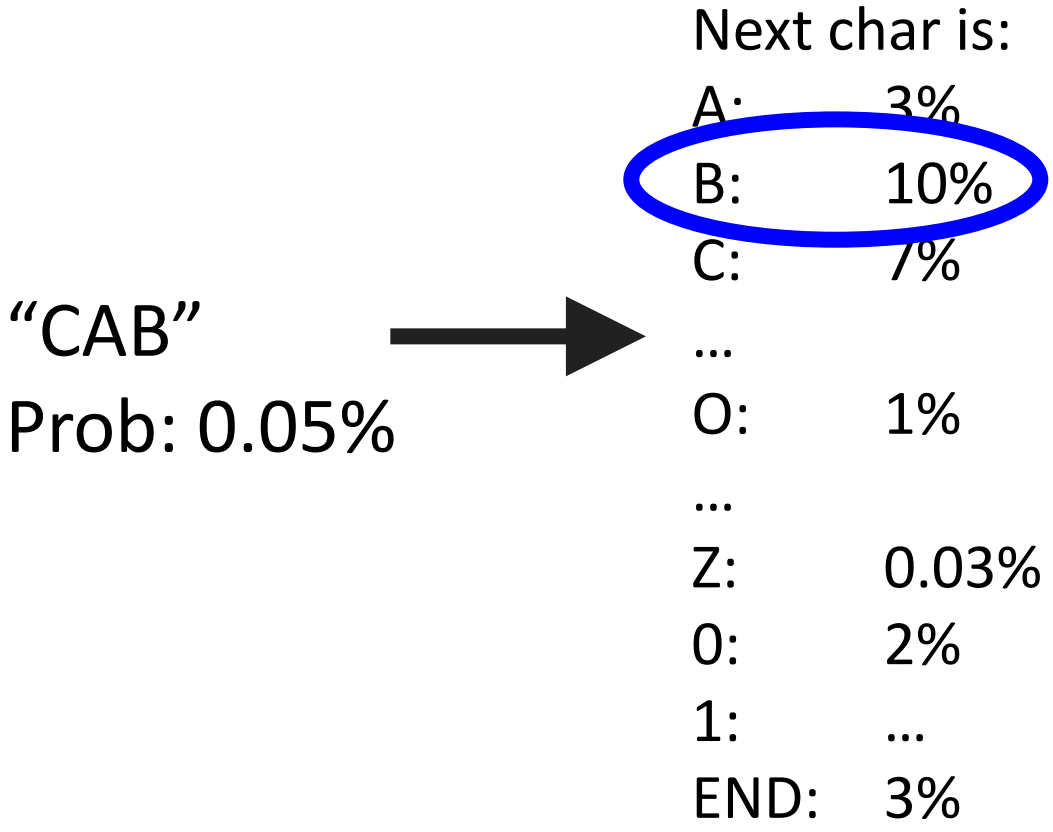
"CA"
Prob: 0.5%

Next char is:

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

196

Generating Passwords



197

Generating Passwords

"CAB"

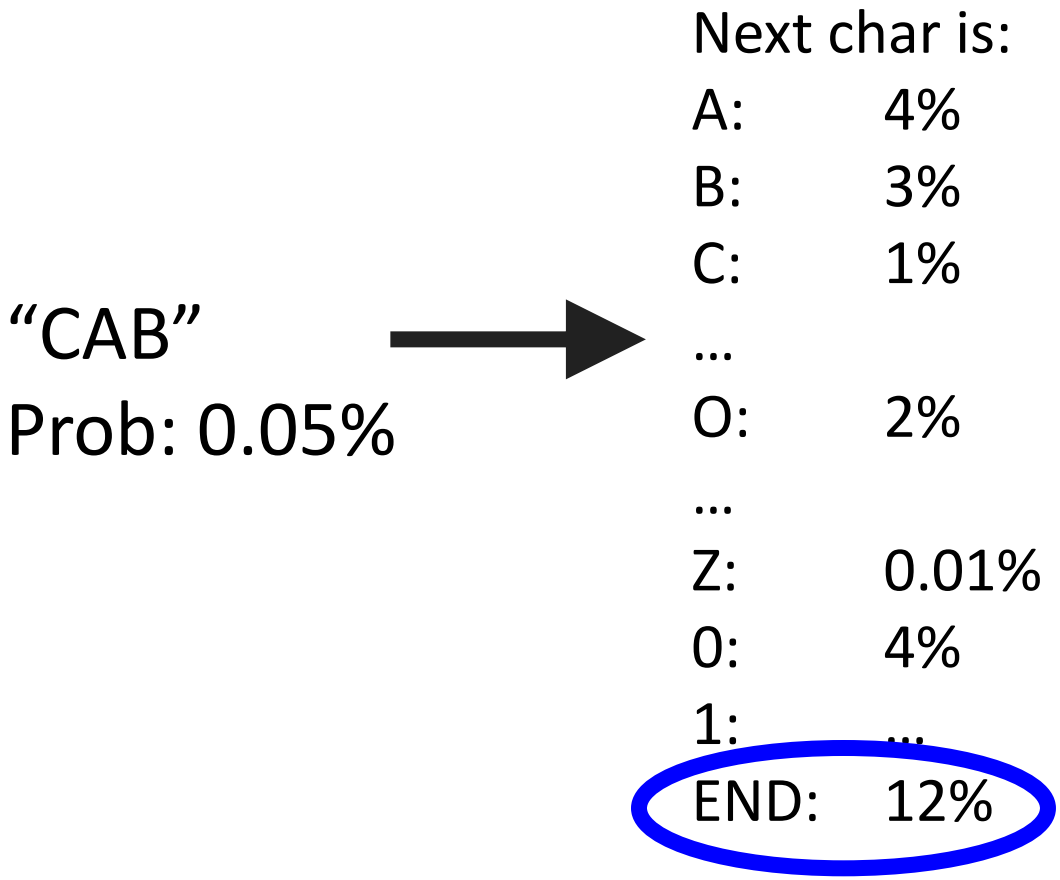
Prob: 0.05%

Next char is:

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

198

Generating Passwords



199

Generating Passwords

“CAB”

Prob: 0.006%

200

Generating Passwords

CAB - 0.006%

CAC - 0.0042%

ADD1 - 0.002%

CODE - 0.0013%

…

201

Generating Passwords

CAR - 0.006%

CAC - 0.0042%

ADD1 - 0.002%

CODE - 0.0013%

...

Must be longer than 3 characters

202

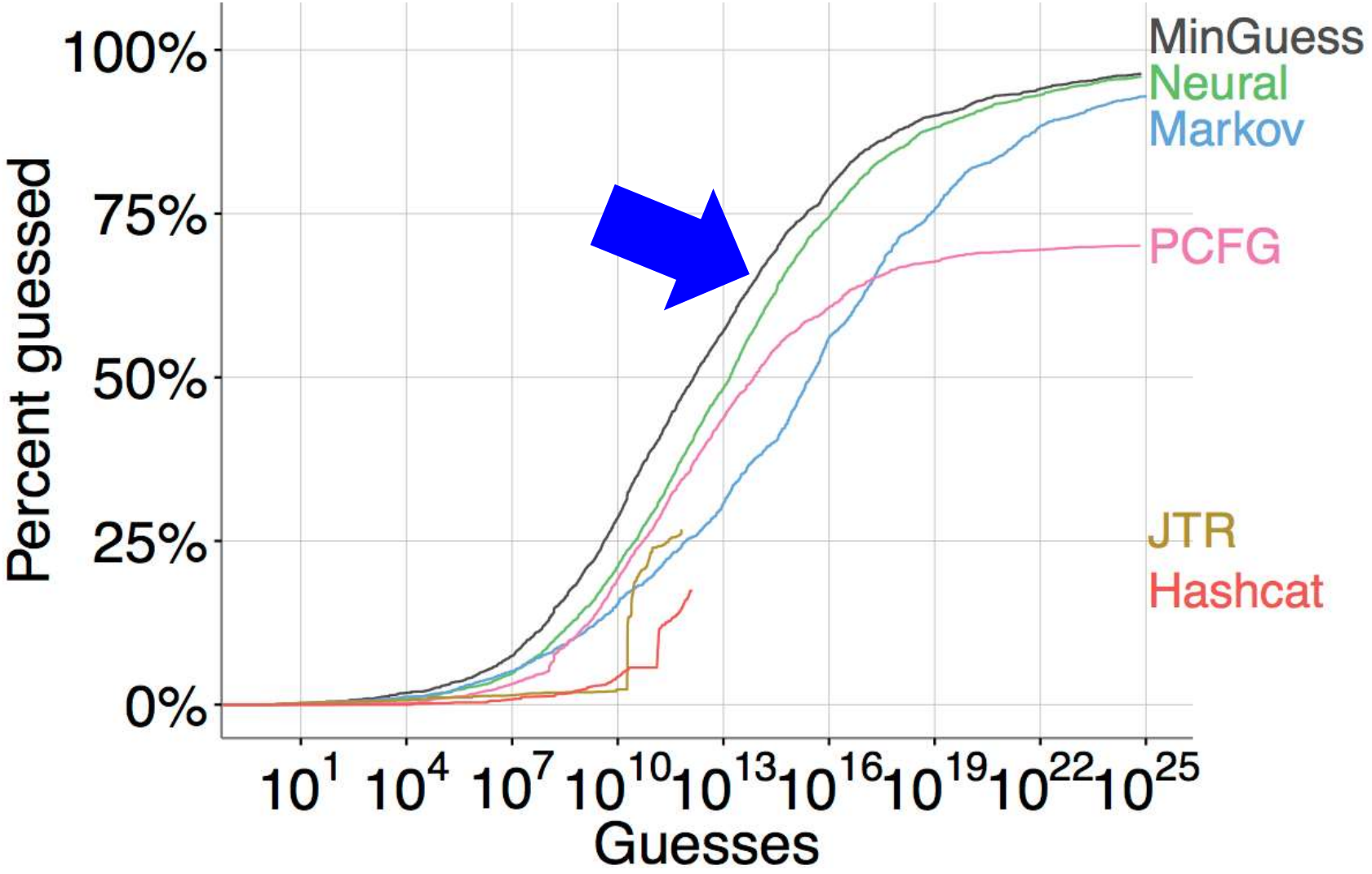
Design Space

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

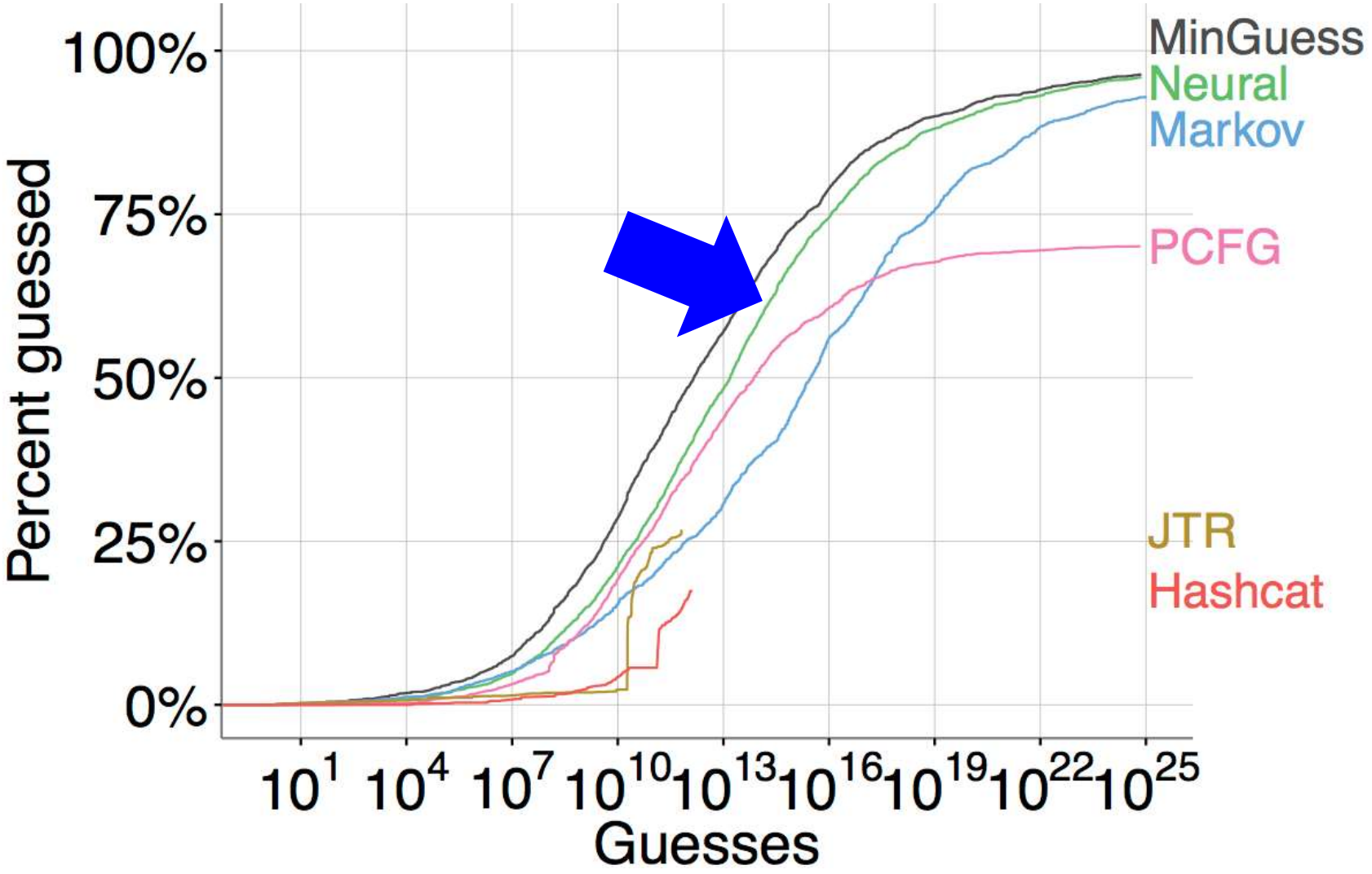
Method

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

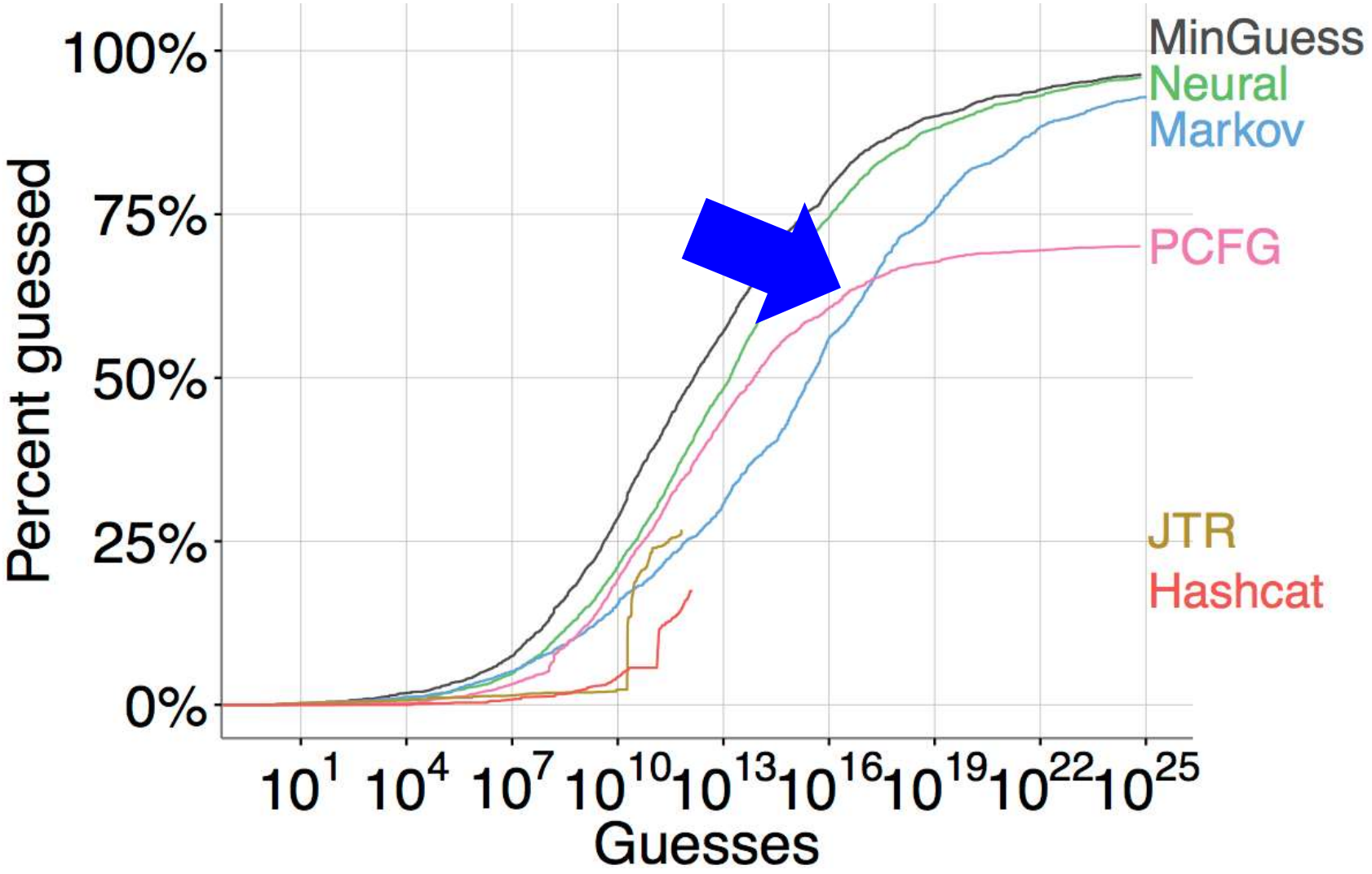
Neural Networks Guess Better



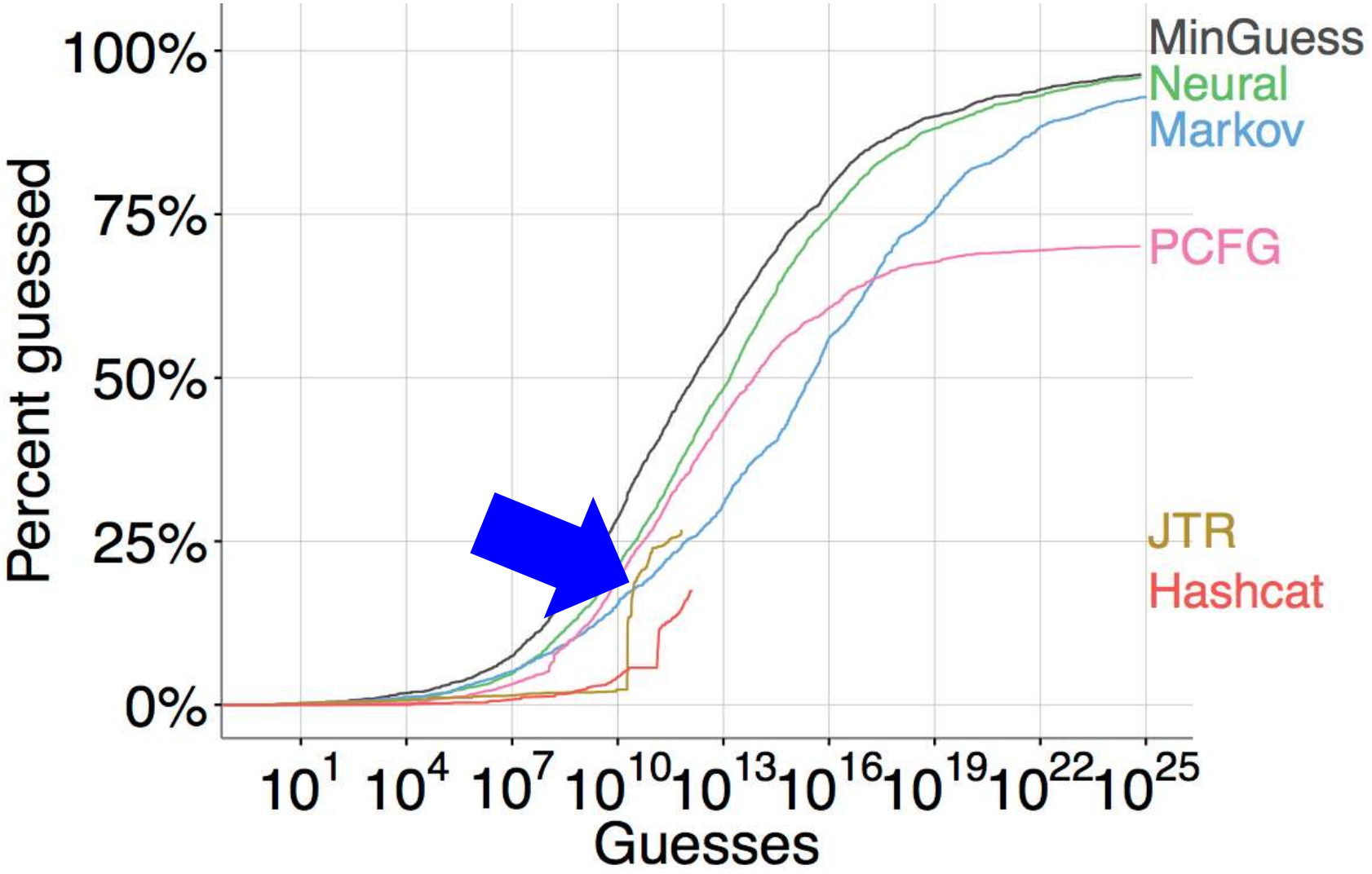
Neural Networks Guess Better



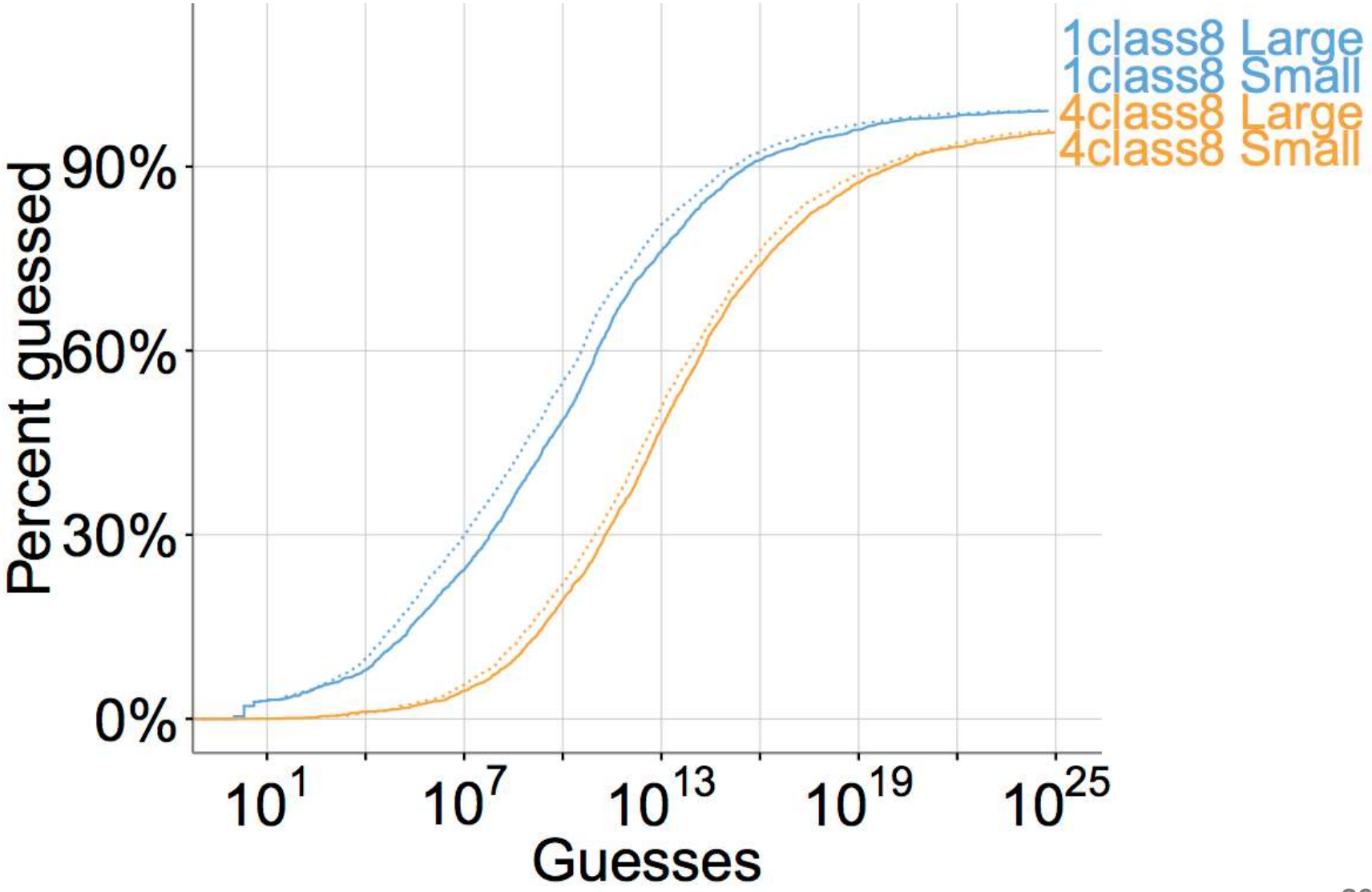
Neural Networks Guess Better



Neural Networks Guess Better



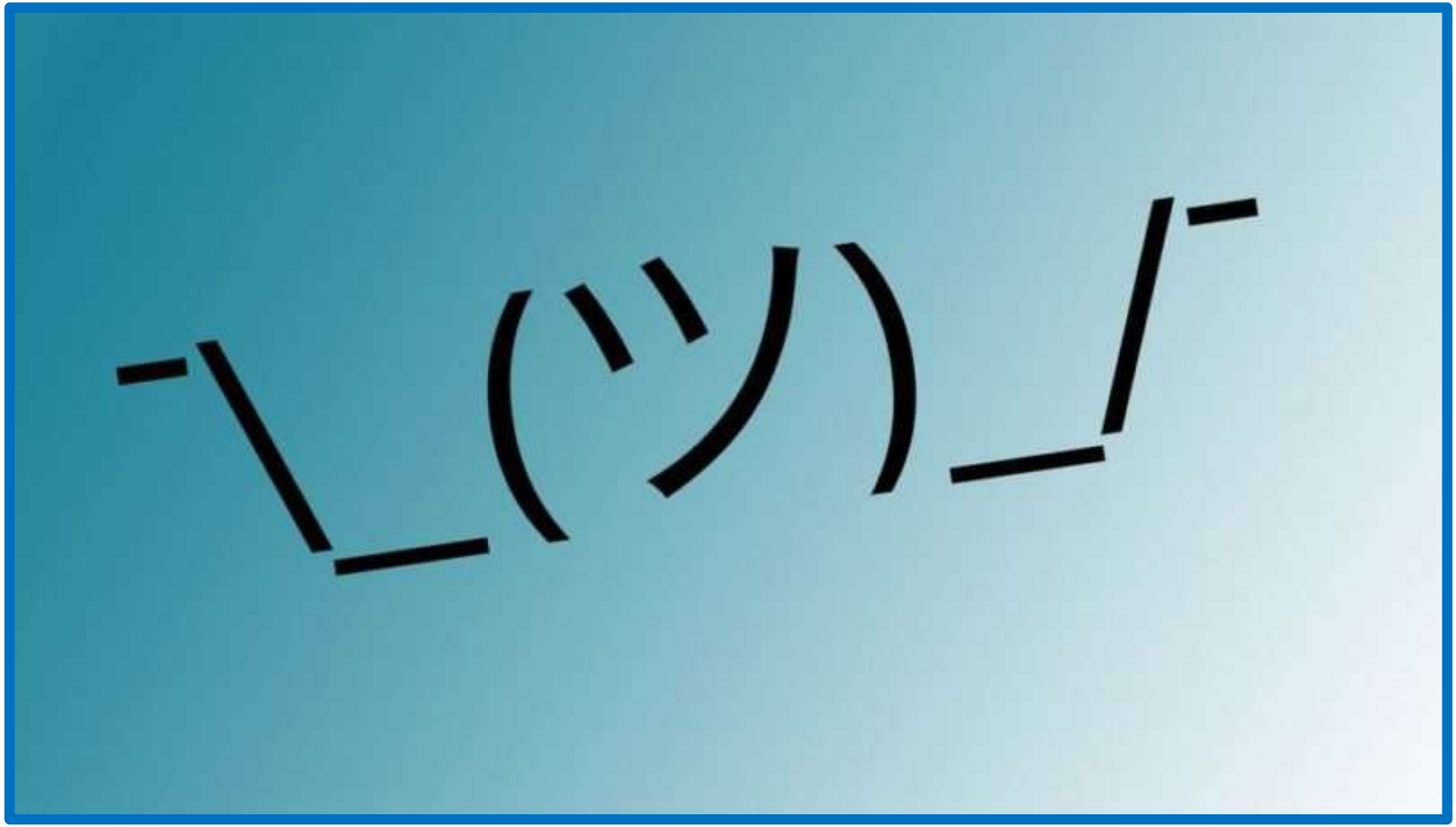
Larger Model Not a Major Advantage



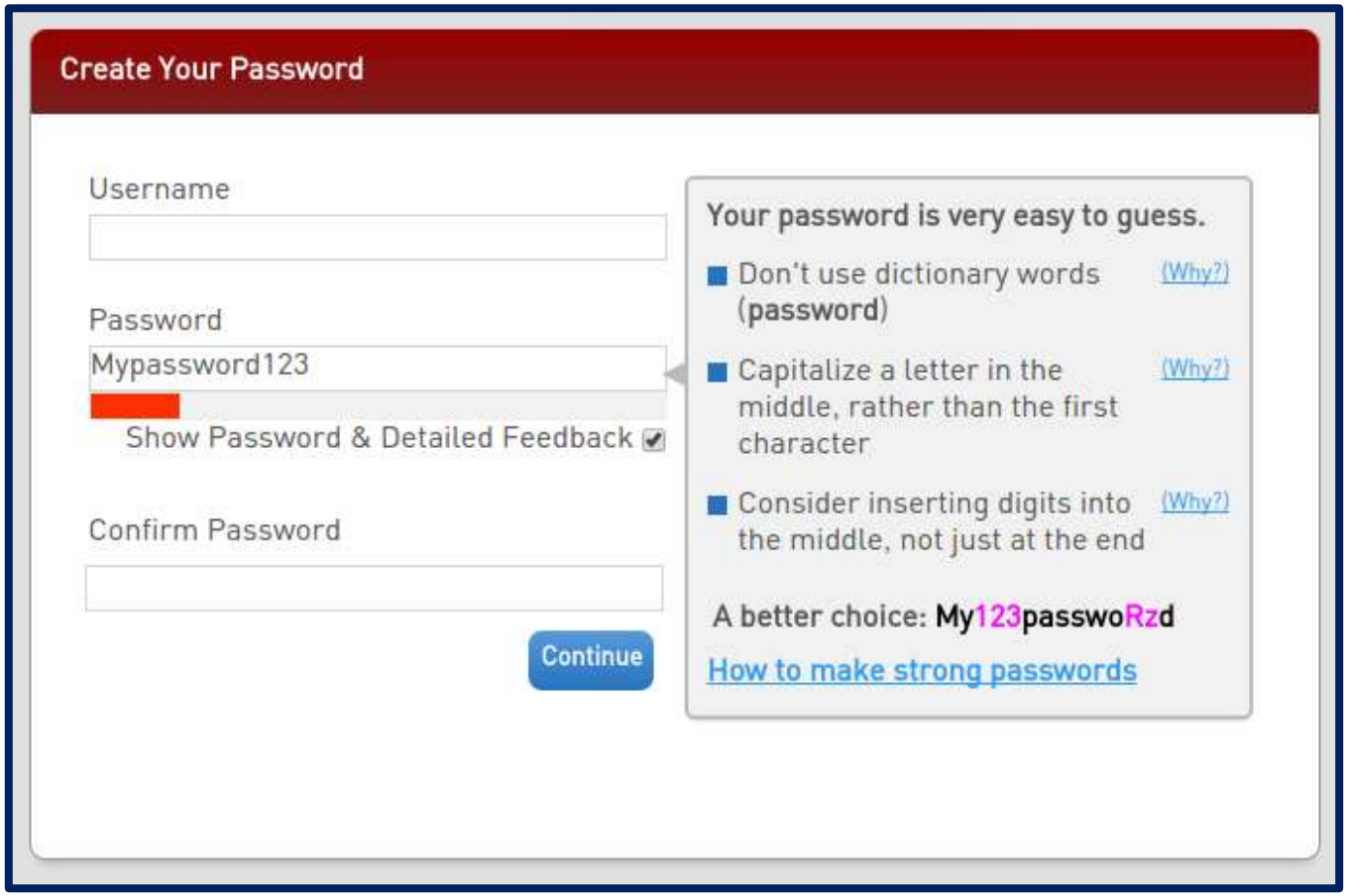
Browser Implementation

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

Intelligibility



Building a Data-Driven Meter



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.

Study goal(s):
*Does data-driven feedback help?
*What feedback features matter?

Method(s):
*Write software
*Online study (task + survey) for 4,509 MTurkers

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.

Main Screen (Password Shown)

Main Screen (Password Shown)

Main Screen (Password Shown)

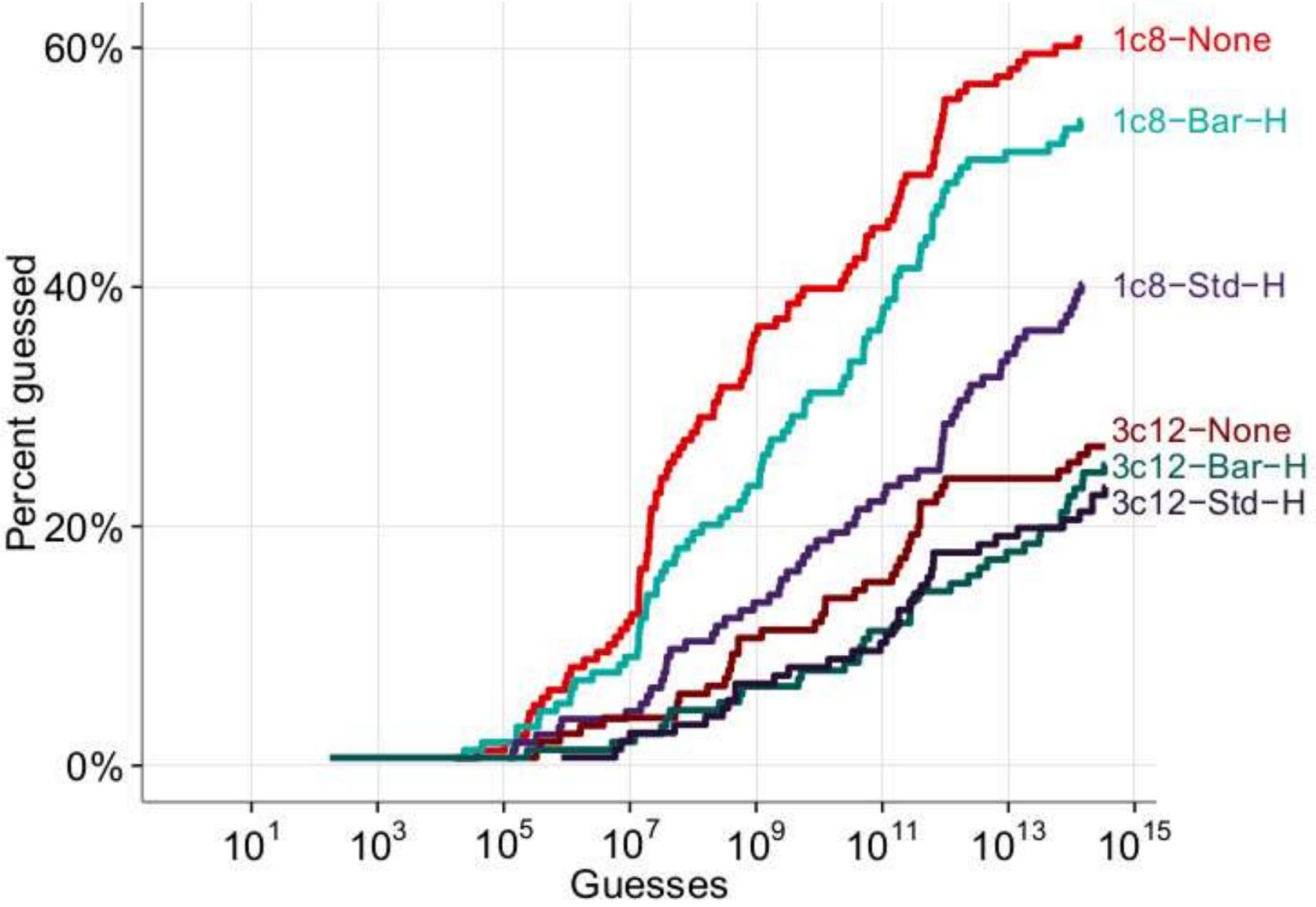
Main Screen (Password Shown)

Main Screen (Password Shown)

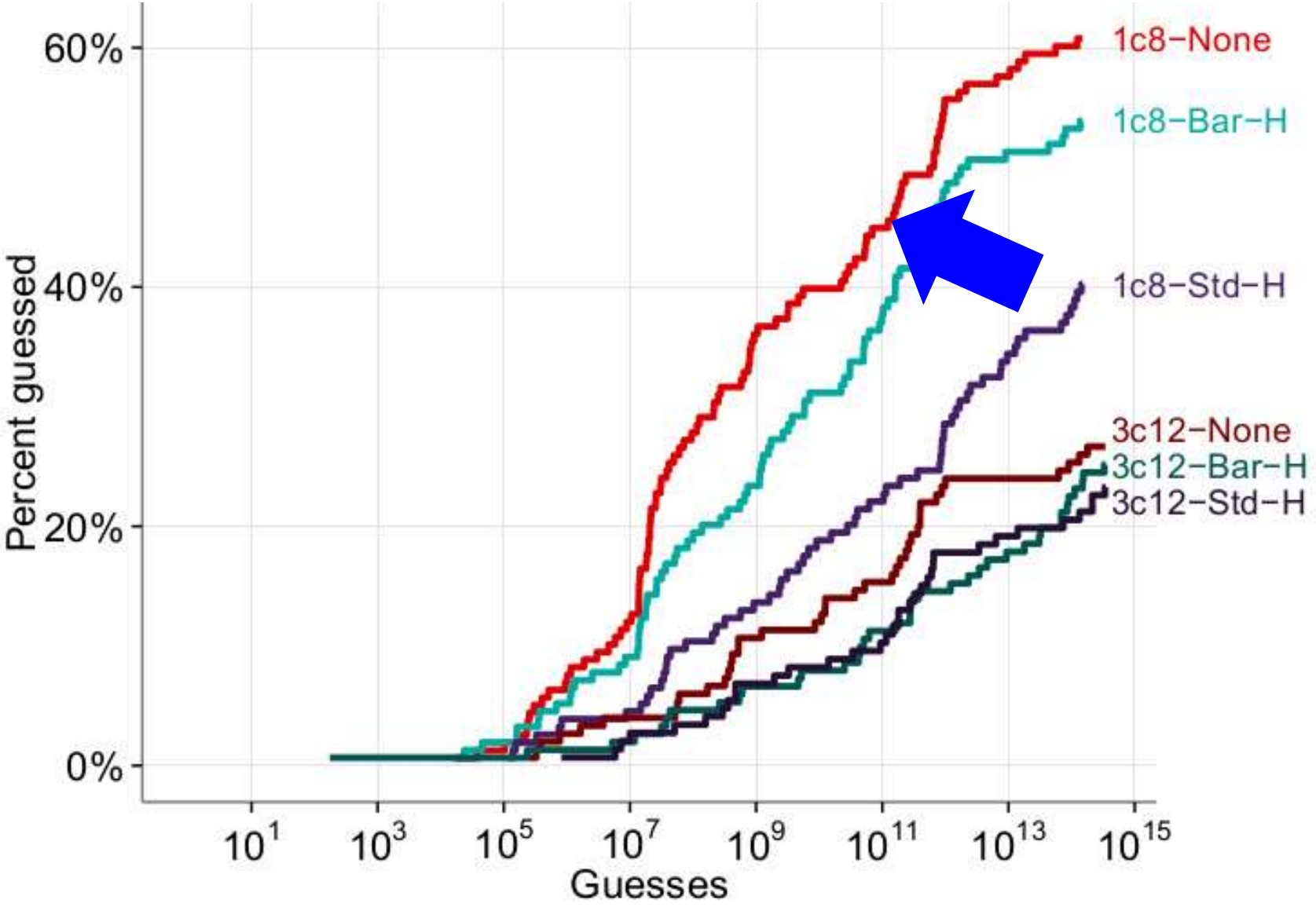
Method

- 4,509-participant online study
- Full-factorial design
  - Password-composition policy
  - Amount of feedback
  - Scoring stringency
- Many security and usability metrics

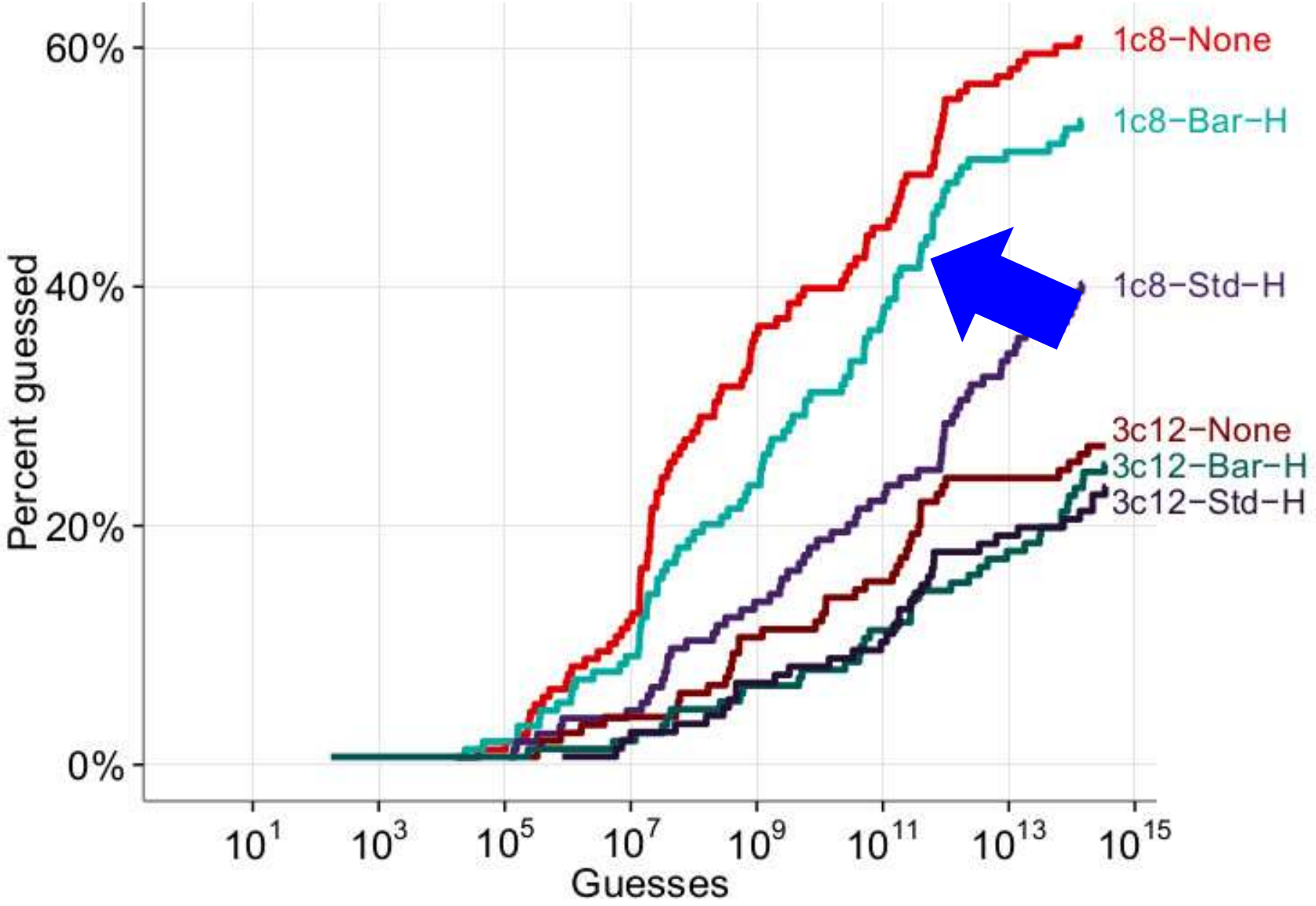
Feedback Major Factor



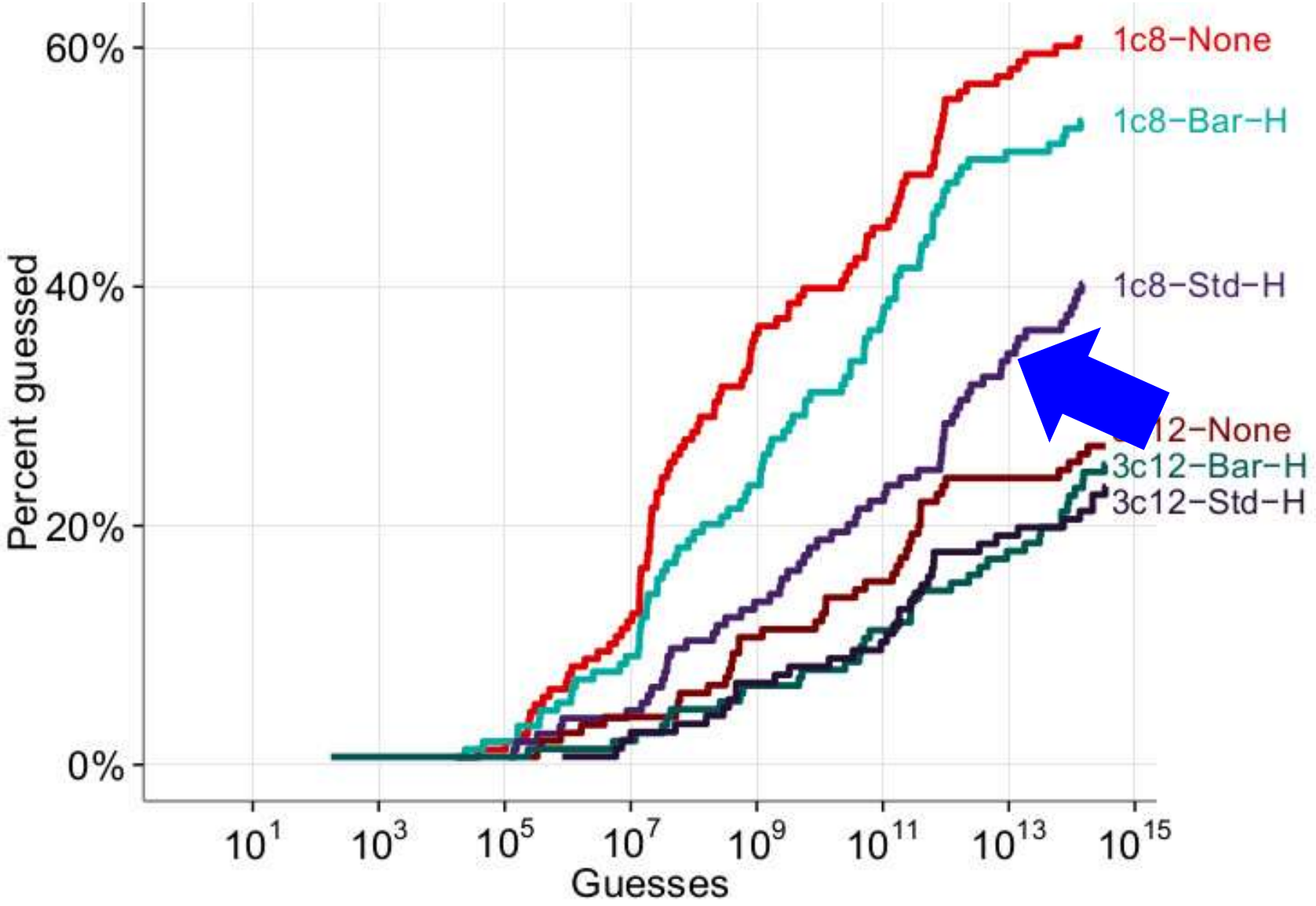
Feedback Major Factor



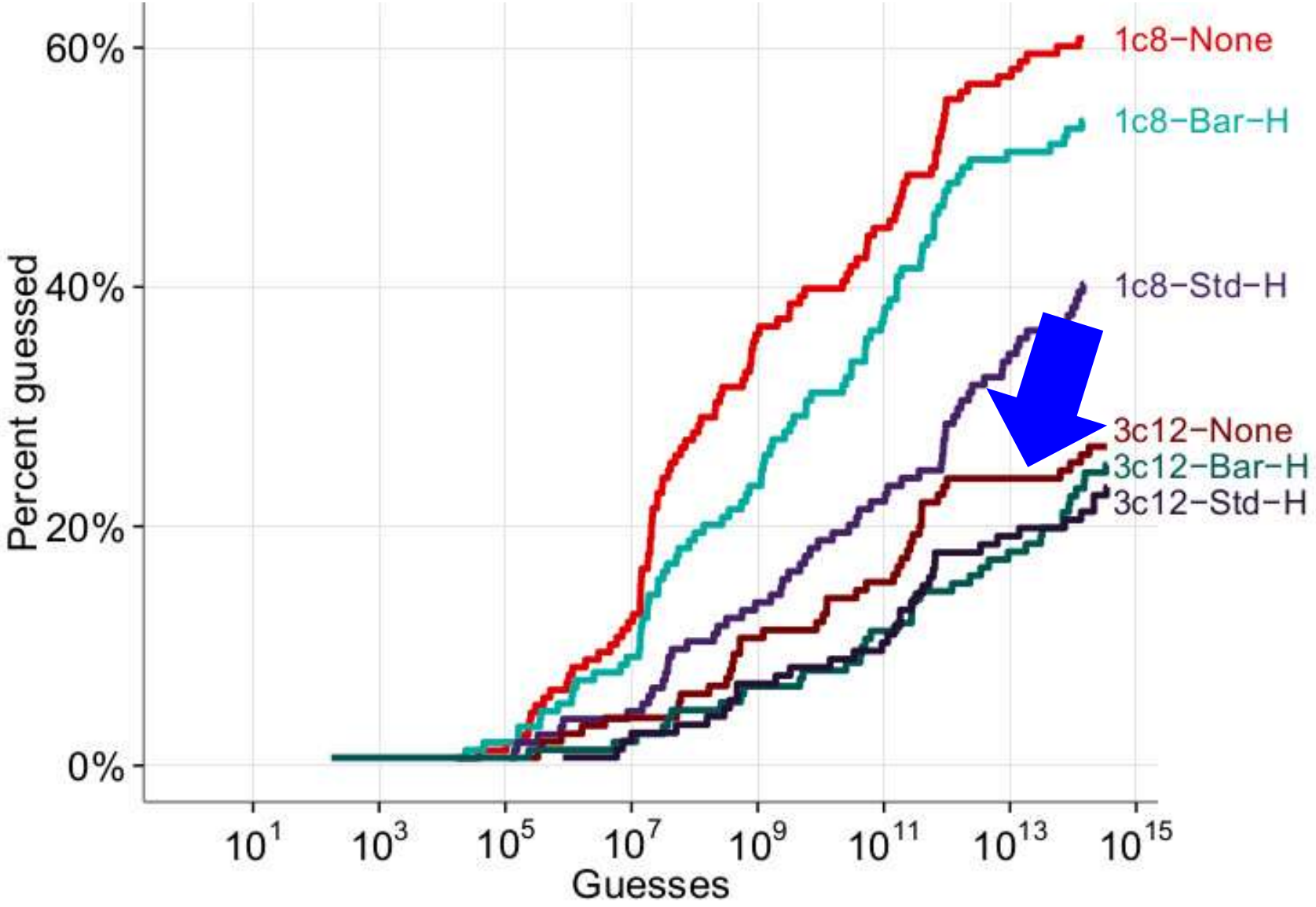
Feedback Major Factor



Feedback Major Factor



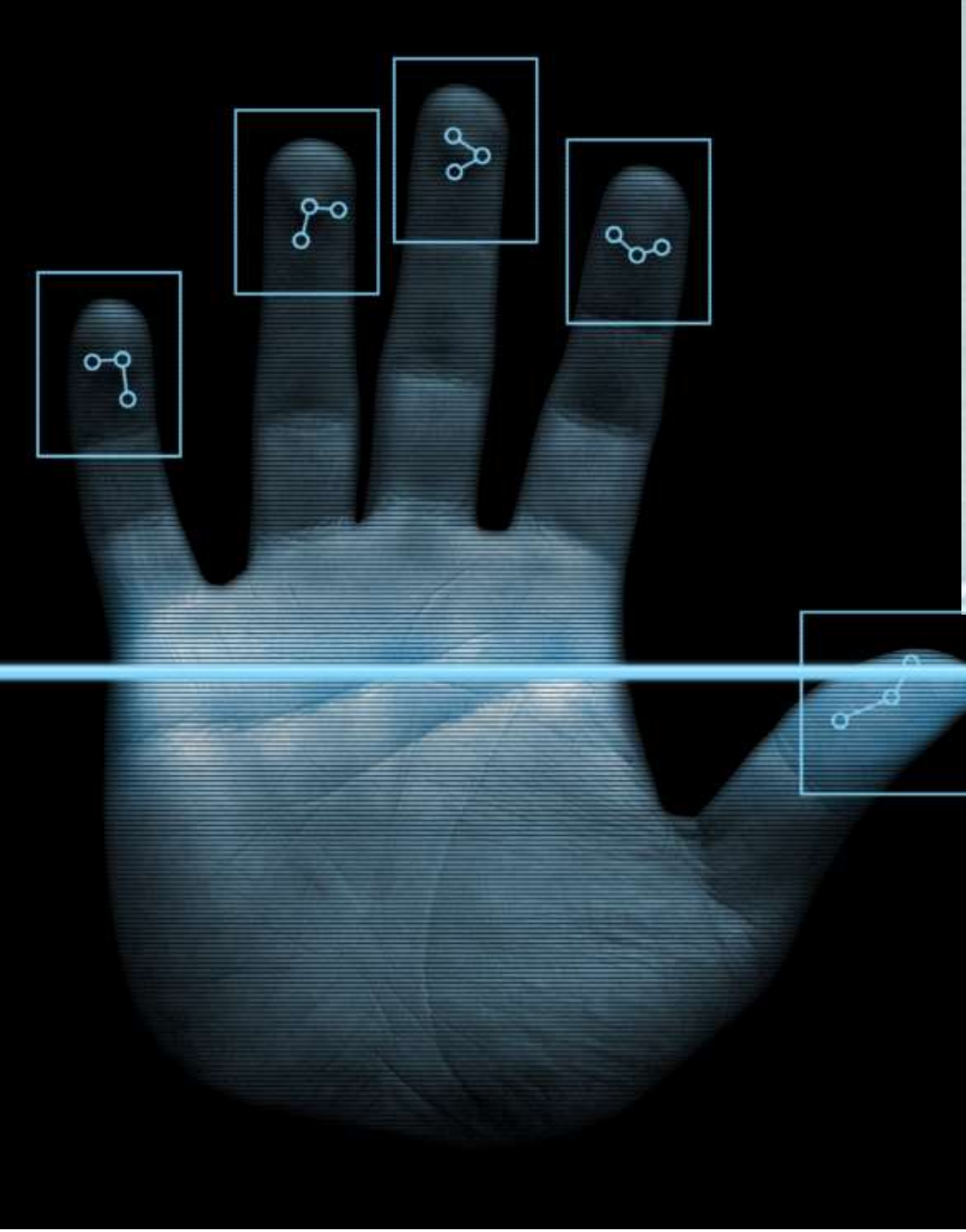
Feedback Major Factor

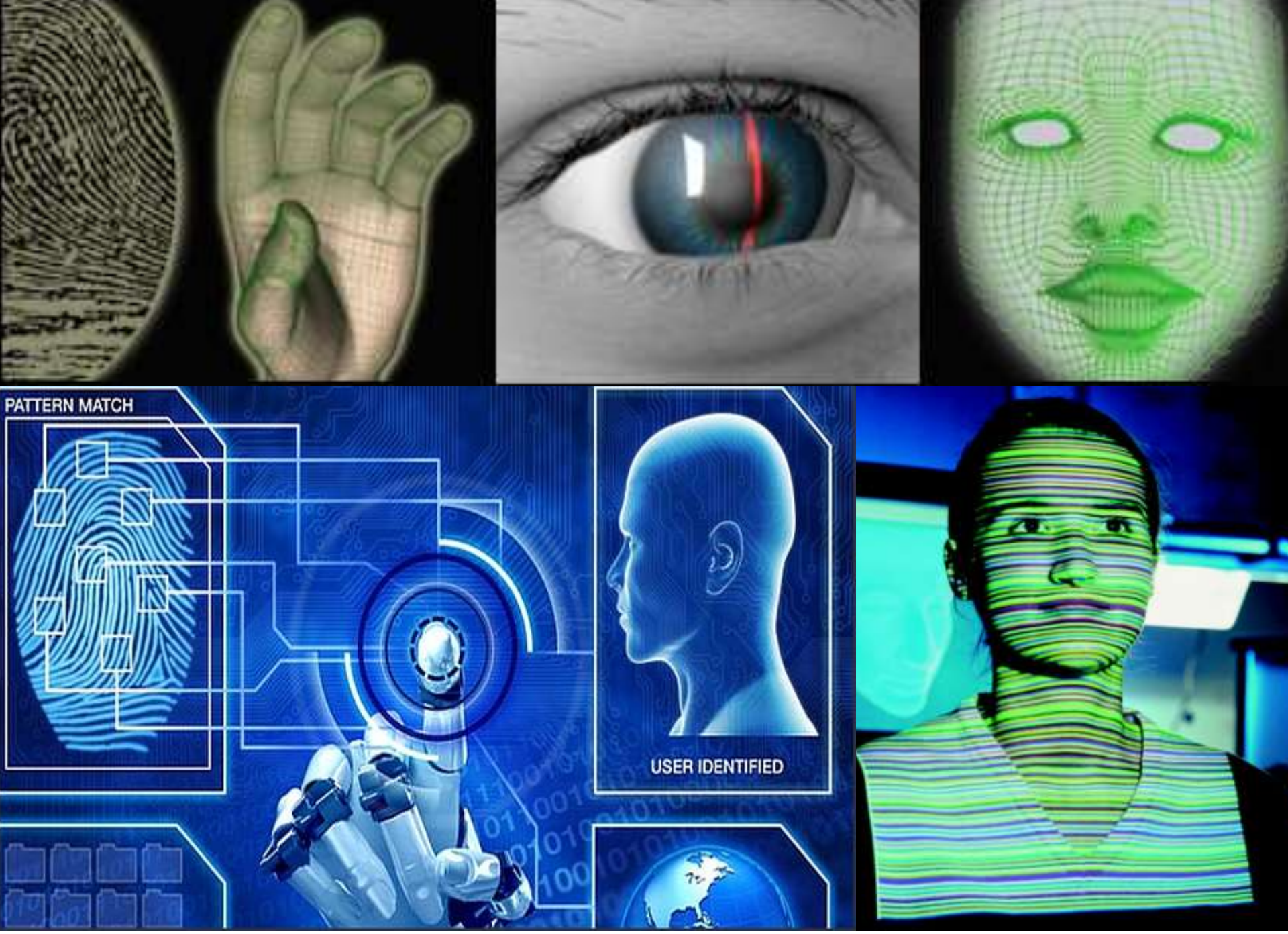


What about Biometrics?

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

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





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

Android 4.0 Face Unlock

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

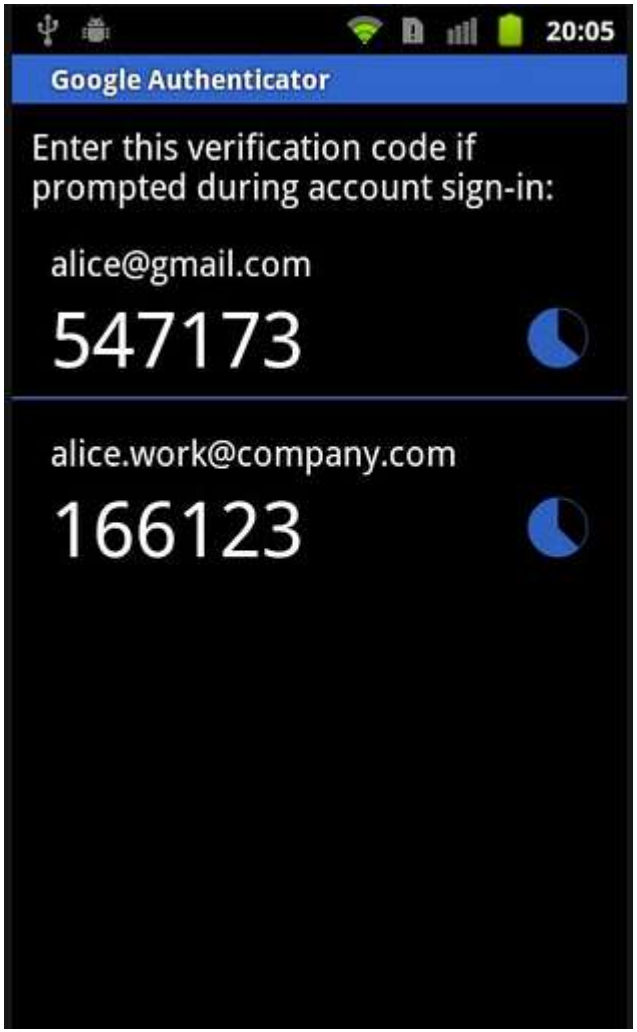
Smartphone Biometrics

- 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

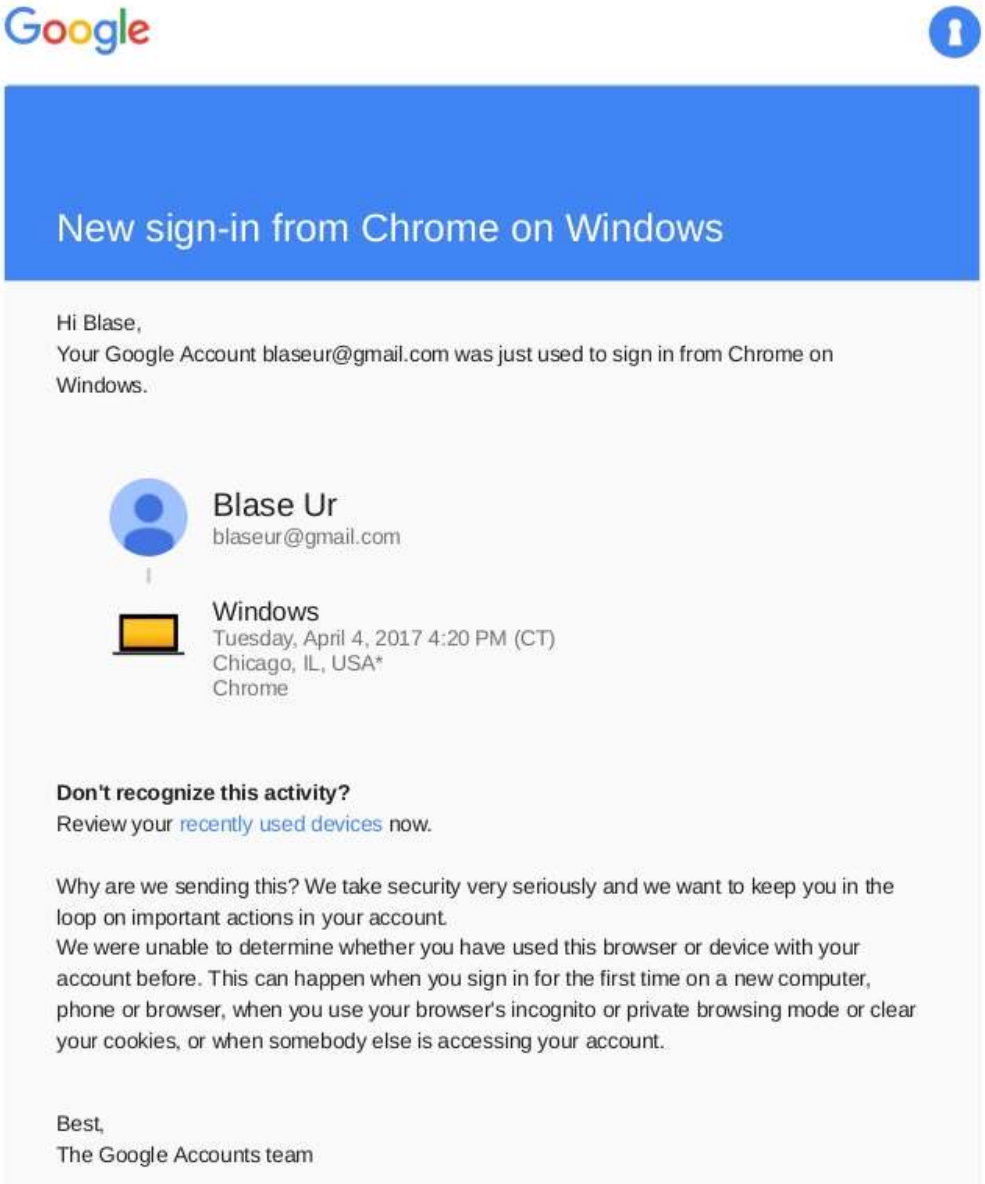
Practical Authentication

Single Sign-On

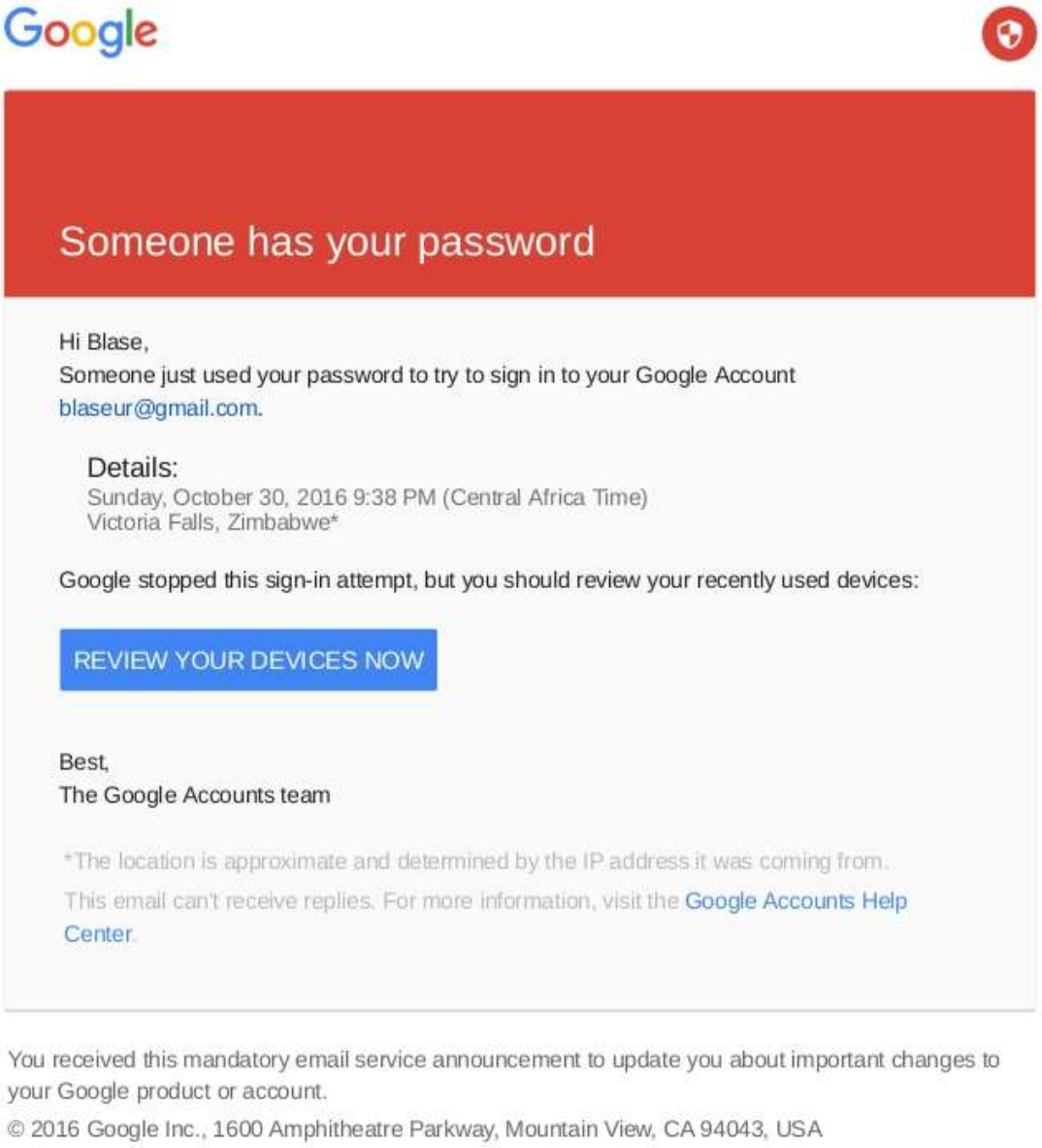
Two-Factor Auth



Context-Sensitive Factors



Context-Sensitive Factors



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

1Password

Conclusions

- Authentication is really hard!
  - Hard for system administrators
  - Hard for users
- Unfortunately, authentication is necessary
- **Different study designs can help you understand a problem from different perspectives**