# Introduction to Password Cracking & Research on Passwords


Michelle Mazurek and Blase Ur

UNIVERSITY OF MARYLAND

Carnegie Mellon

# Introductions

- Your name
- Your position and affiliation (e.g., Ph.D. student at Example University)
- What you'd like to learn in today's tutorial
- Any prior experience (if any) you have researching passwords
- The password for your email account

# Outline

1) 8:30am – 8:40am Intros

2) 8:40am – 8:50am Relevance of passwords

3) 8:50am – 9:05am Password security / threats

4) 9:05am – 9:35am Robust, reliable experiments on passwords

5) 9:35am – 10:00am What we know about passwords

*10:00am – 10:30am Break*

6) 10:30am – 10:45am Approaches to guessing passwords

7) 10:45am – 11:10am Hands-on intro to Hashcat

8) 11:10am – 12:10pm Password-cracking contest

# Why are we still talking about passwords?

# Advantages of Passwords

- Familiar to people
- You can have many different ones
- Difficult to coerce
  - (Disputed) protections from 5th Amendment
- Nothing to carry
- Easy to revoke / replace

Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proc. IEEE S&P*, 2012.

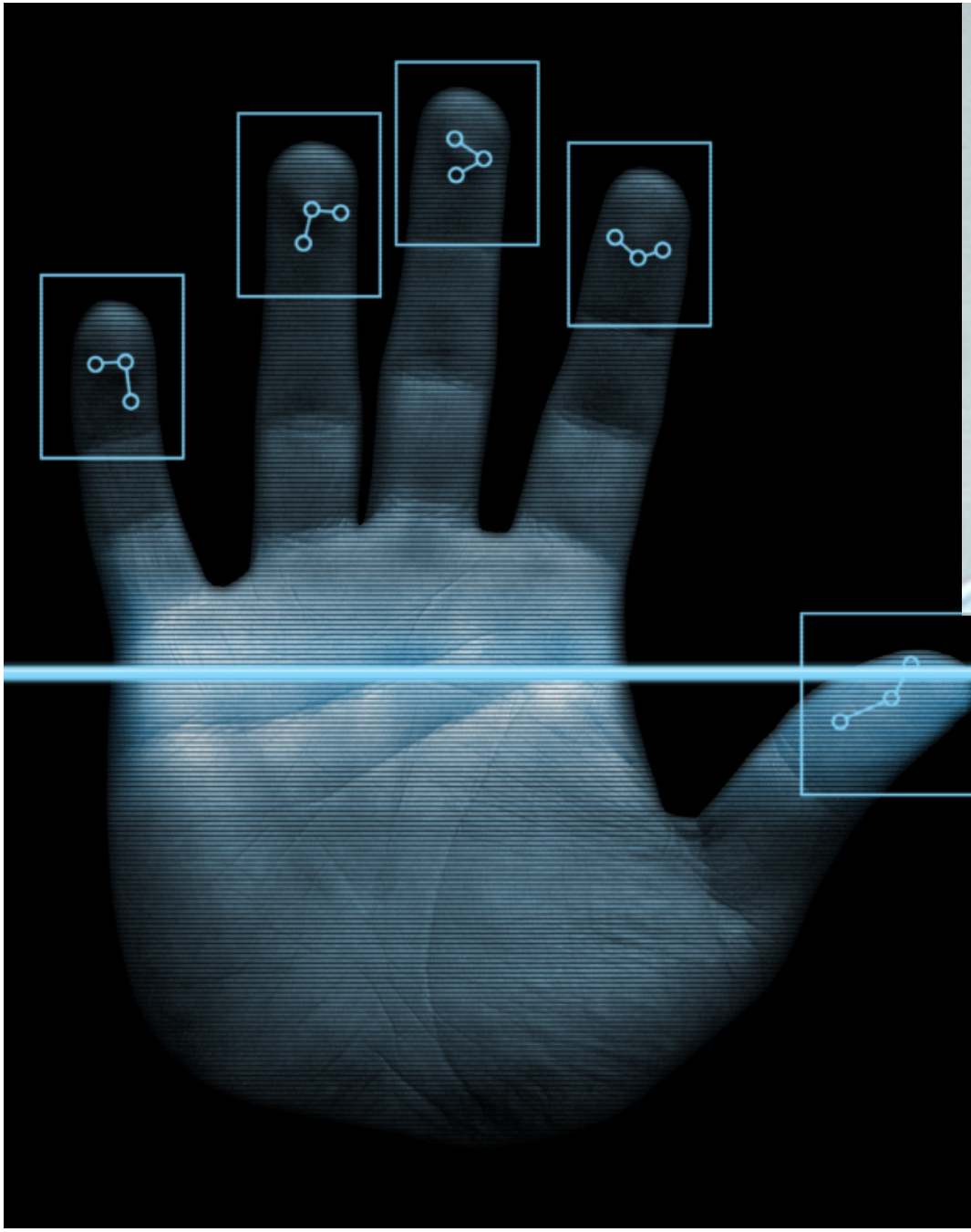
# More Advantages of Passwords

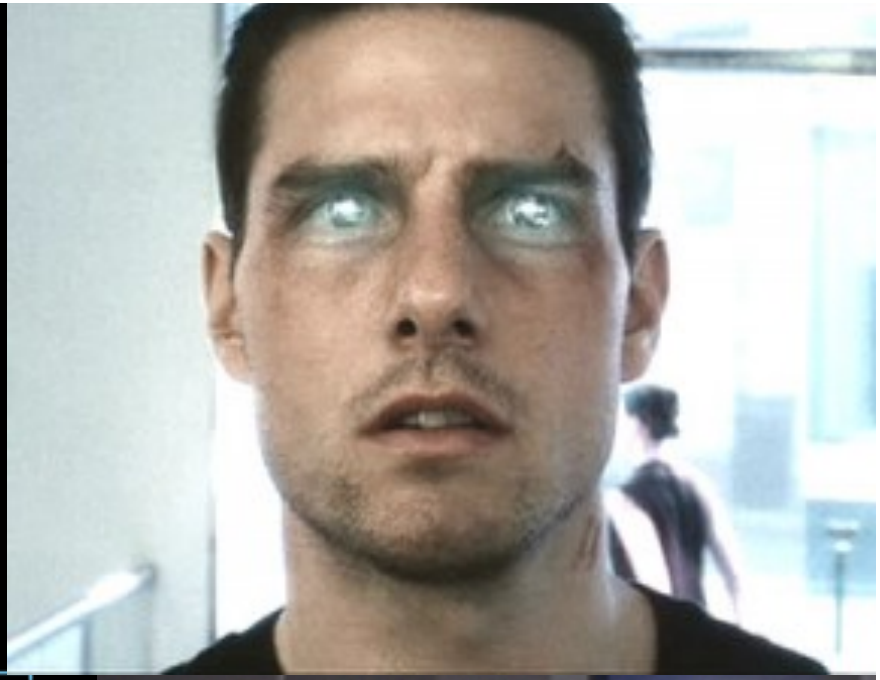
- Accessibility
- Easy to deploy
- Low cost
- No proprietary aspects / patents
- Doesn't require a trusted third party
- Not linked to an individual

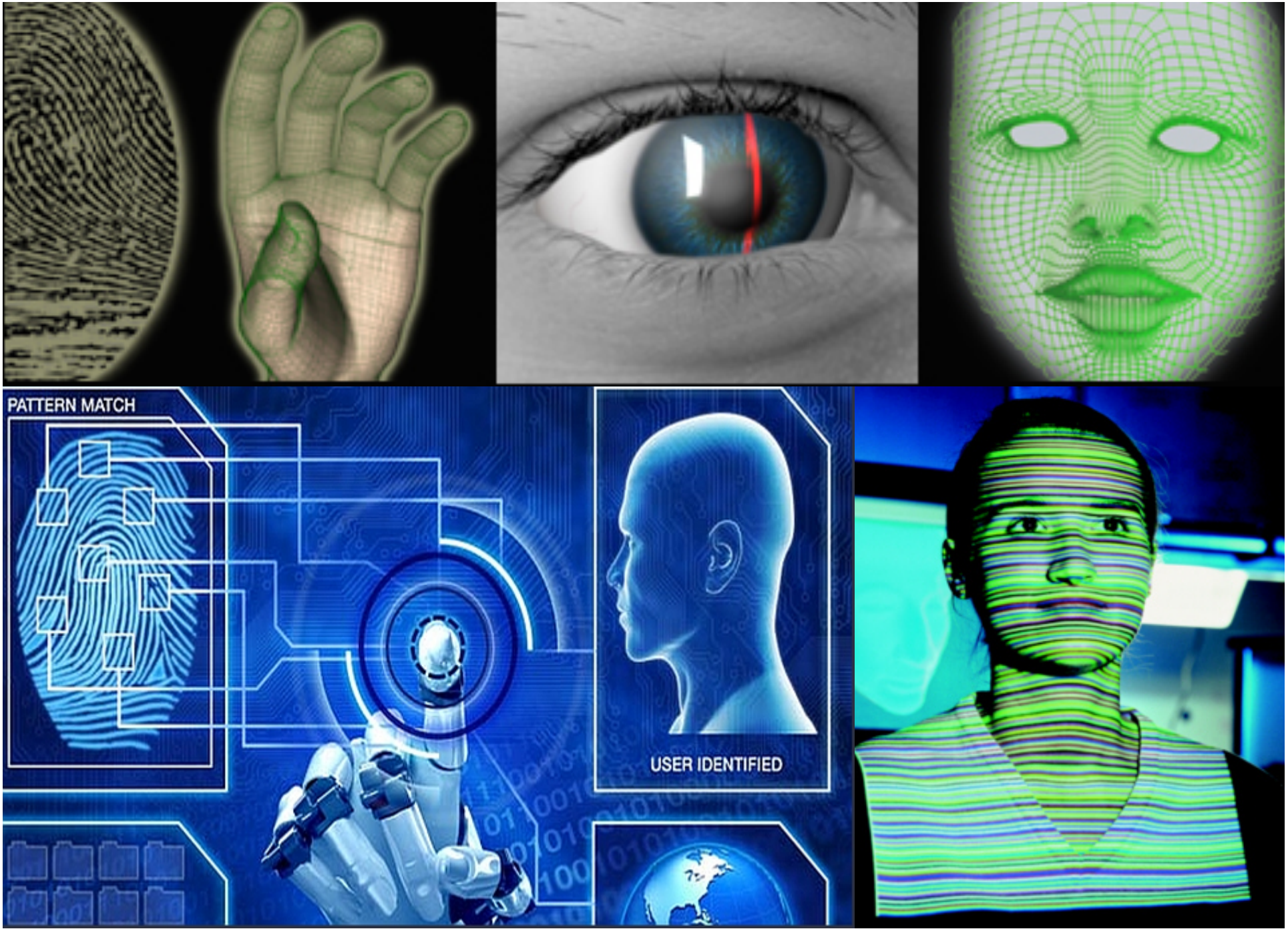
Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proc. IEEE S&P*, 2012.

# What about Biometrics?

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








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

SECTIONS HOME SEARCH

The New York Times

DealB%k WITH FOUNDER ANDREW ROSS SORKIN

# *Goodbye, Password. Banks Opt to Scan Fingers and Faces Instead.*

By MICHAEL CORKERY JUNE 21, 2016

# Biometrics

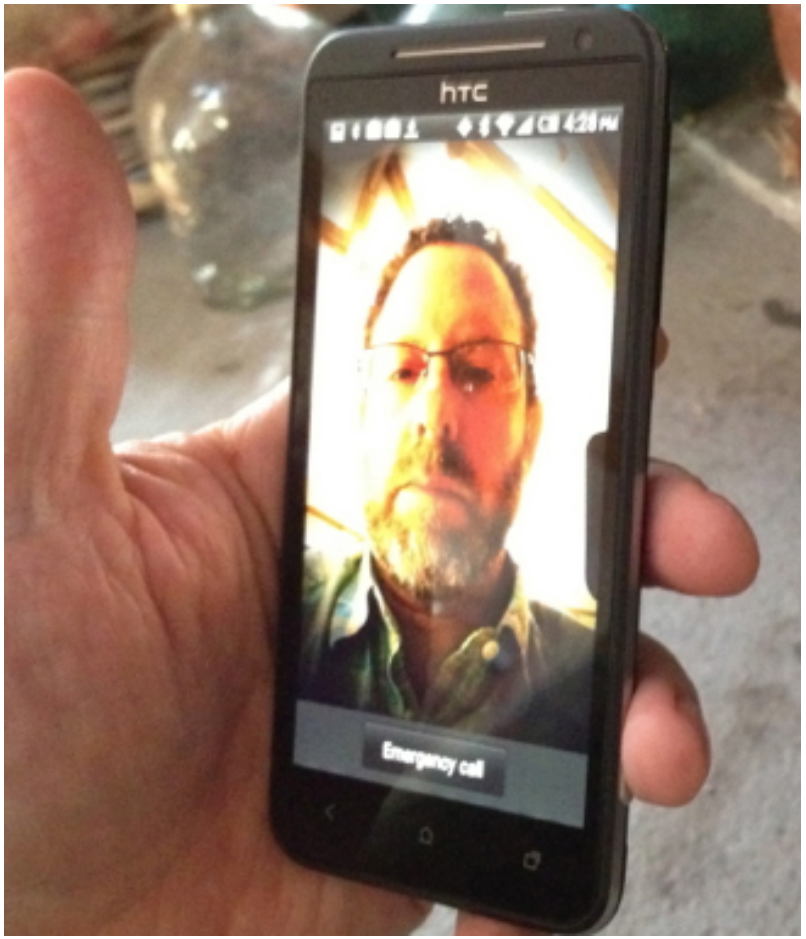
- Fingerprint
- Iris scans or retina scans
- Face recognition
- Finger/hand geometry
- Voice or speech recognition
- The way you type
- (Many others)

# 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

# Means of Authentication (1/2)

- Something you know
  - Password or PIN
- 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)

# Means of Authentication (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
  - PKI Certificate Authorities

# Disadvantages of Passwords

- Predictability
- Interference between multiple passwords
  - Limits of human memory
- Requiring a large portfolio of passwords
- Easy to deploy incorrectly / naively
  - System administrators
  - Users

# Outline

1) 8:30am – 8:40am Intros

2) 8:40am – 8:50am Relevance of passwords

3) 8:50am – 9:05am Password security / threats

4) 9:05am – 9:35am Robust, reliable experiments on passwords

5) 9:35am – 10:00am What we know about passwords

*10:00am – 10:30am Break*

6) 10:30am – 10:45am Approaches to guessing passwords

7) 10:45am – 11:10am Hands-on intro to Hashcat

8) 11:10am – 12:10pm Password-cracking contest

# Deploying Passwords

- Logging into an online or local account
  - /etc/shadow
  - Hashed passwords
- Encrypting a local file using a password
  - Password-Based Key Derivation Functions
  - Key used to encrypt data often stored in file

# Best Practices for Storing Passwords

- Hash function: one-way function
  - Designed for efficiency (e.g., MD5)
  - Password-specific hash functions (e.g., bcrypt, scrypt, PBKDF2, Argon2)
- hash("Blase") =

```
$2a
$04$iHdEgkI681VdDMc3f7edau9phRwOR
vhYjqWAIb7hb4B5uFJO1g4zi
```

# Best Practices for Storing Passwords

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

# Threats to Password Security

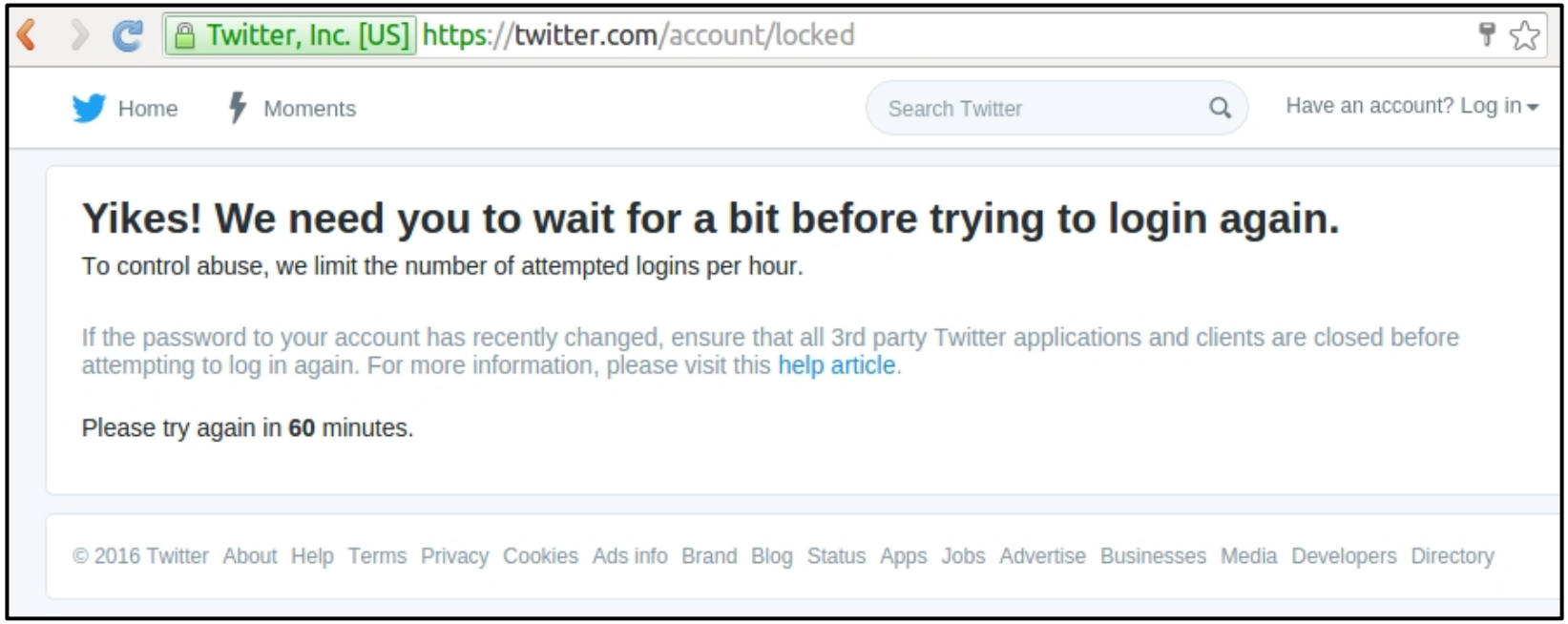
- Phishing attacks
- Shoulder surfing (observation)
- Poor implementation / deployment

# 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

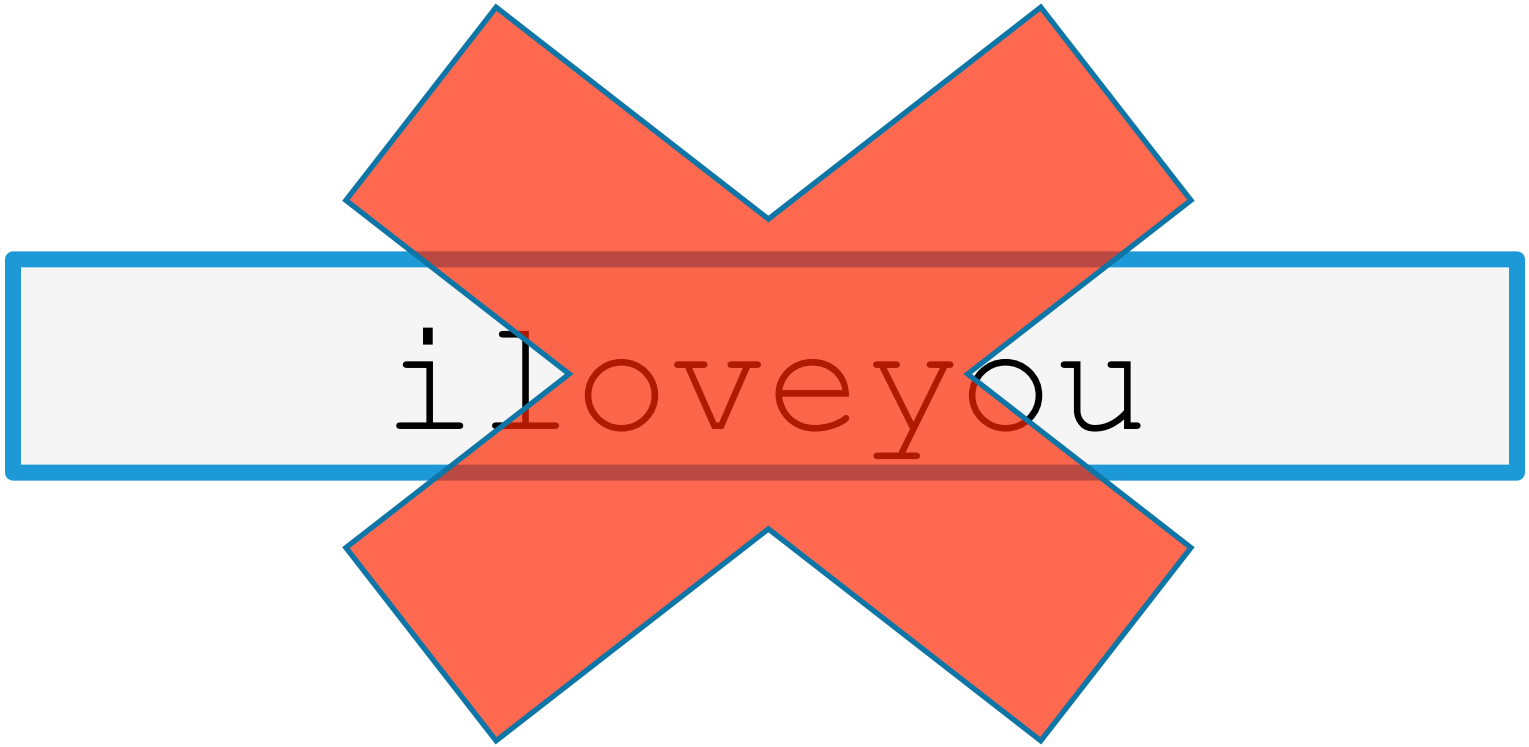
- Attacker compromises database
- Attacker makes and hashes guesses
- Finds match → try on other sites
  - Password reuse is a key problem


# How strong is a particular password?

# Why Measure Password Strength?

- Eliminate bad passwords
  - Organizational password audits
- Help users make better passwords
  - Determine if interventions are effective
  - Provide users feedback

```
iloveyou
```


iloveyou

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

j@mesb0nd007!

# Outline

1) 8:30am – 8:40am Intros

2) 8:40am – 8:50am Relevance of passwords

3) 8:50am – 9:05am Password security / threats

4) 9:05am – 9:35am Robust, reliable experiments on passwords

5) 9:35am – 10:00am What we know about passwords

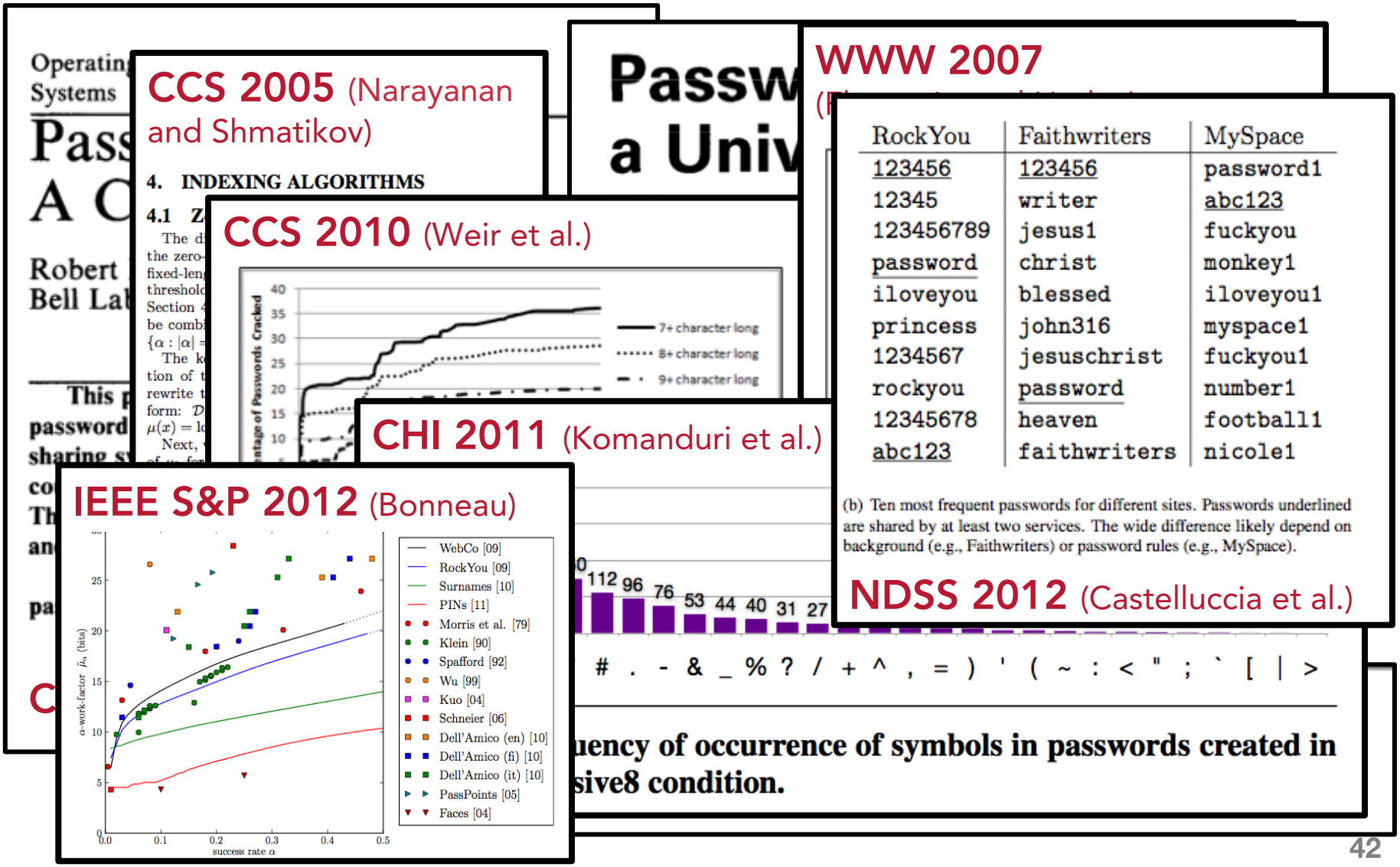
*10:00am – 10:30am Break*

6) 10:30am – 10:45am Approaches to guessing passwords

7) 10:45am – 11:10am Hands-on intro to Hashcat

8) 11:10am – 12:10pm Password-cracking contest

# Passwords research is everywhere



# … but is it reliable?

- How are strength, usability measured?
- How good is the data source?

- Recently, significant progress in both areas


http://adamwarrock.com/

# MEASURING PASSWORDS

# Strength is hard to measure

- Number of character classes?
- Shannon entropy?
- α-guesswork?
- John the Ripper?

**How do we know if a password (or a set of passwords) is secure?**

# Old metric: Entropy

- Calculated based on input symbol size (many)
  - Doesn't account for human patterns
- NIST back-of-envelope estimate (NIST 2006)
  - Vague, not empirical
- Estimated Shannon entropy (Shay 2010)
  - Requires big sample sizes, underestimates
- Average, doesn't tell you about your weak links

# Better 1: Statistical guesswork

- Alpha guesswork: Expected #/guesses per account to guess fraction alpha
- Assumes knowledge of underlying distribution
  - Sample = systematic underestimate
  - Requires enormous sample sizes
- Extrapolate via Poisson distribution

Joseph Bonneau. The science of guessing: Analyzing an anonymized corpus of 70 million passwords. IEEE S&P 2012.

# Better 2: Parameterized guessability

- How many guesses to reach password?
  - Subject to guessing algorithm, training data
  - Calculate quickly via lookup algorithm
- Result: guess number or beyond cutoff

Example:

| Password | Guess number |
|---|---|
| 12345678 | 4 |
| Password178 | $1.4 \times 10^6$ |
| jn%fKXsl!8@Df | Beyond cutoff |

Patrick Gage Kelley et al. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. IEEE S&P 2012.

# Guesswork vs. guessability

- Optimal attacker
- Depends only on data set
- Can use hashes
- Describe entire set in one stat
- Sample size: enormous

- Model real attacker
- Depends on algorithm, training
- Requires plaintext
- Per-password estimates
- Sample size: large

# Range of usability metrics

- Memorability
  - Realism? Time, frequency, interference
- Creation time, attempts
- Login time
- Storage
- Self-reported sentiment
- False rejects (where applicable)

# SOURCING QUALITY DATA

# Problems with password data

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

**Are the results generalizable?**

# Lab vs. online vs. real

- Anonymized plaintext dump of thousands of university students' passwords
- Online and lab studies, (no) priming
  - Same pool of students as plaintext dump
- Manual analysis for similarity
- 583 online, 63 lab participants

Sascha Fahl et al. On The Ecological Validity of a Password Study. SOUPS 2013.

# Results: Validity

| % | Online | Lab | Priming | Non | Total |
|---|---|---|---|---|---|
| Highly valid | 46 | 49 | 47 | 44 | **46** |
| Somewhat valid | 23 | 32 | 24 | 24 | **24** |
| Invalid | 31 | 18 | 29 | 32 | **30** |

- Overall, experimental data can be useful
  - Self-reporting of realistic behavior can help
- No significant difference from priming
- Lab slightly but significantly better than online

# CMU password set

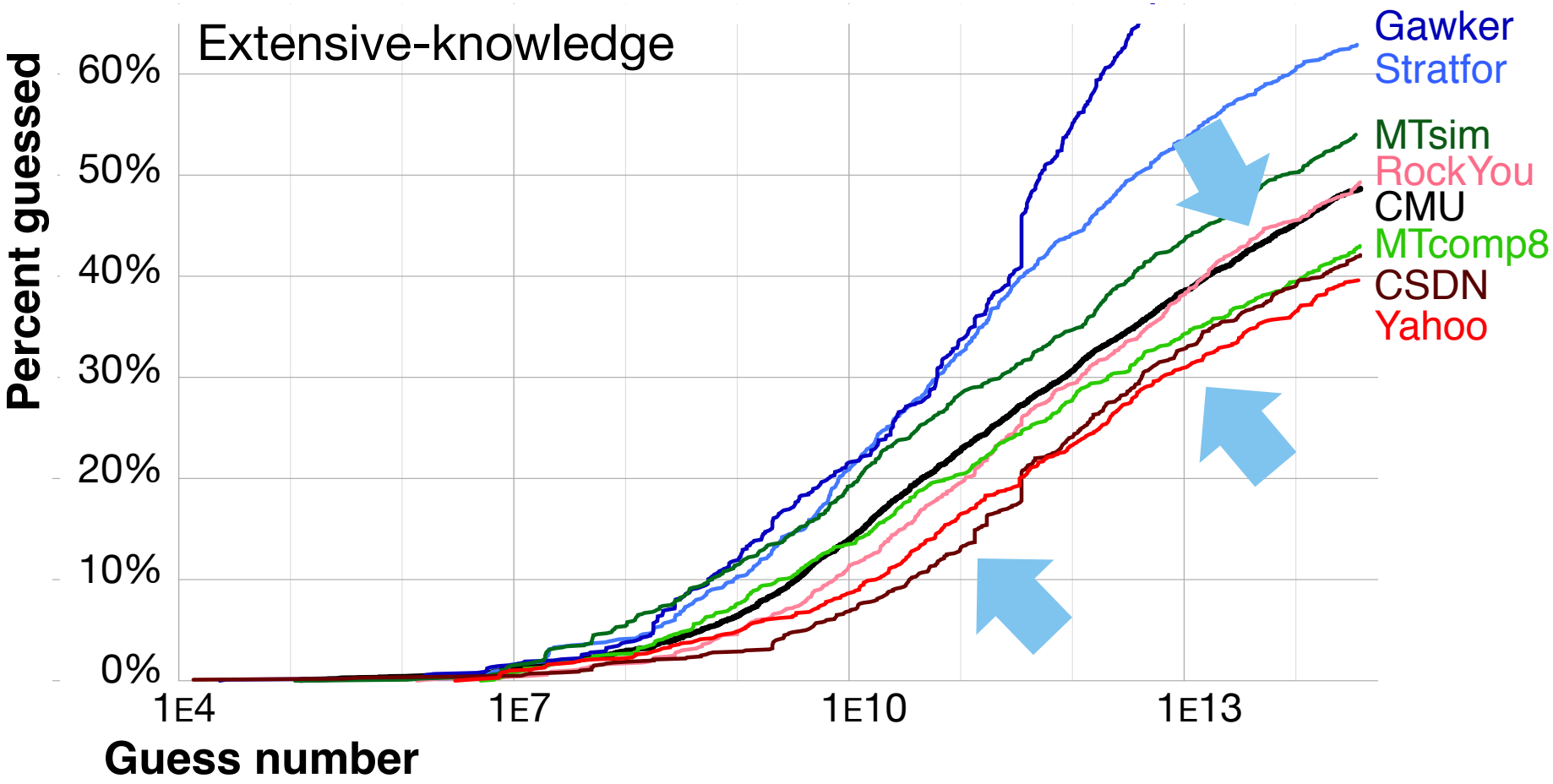
- 25,000 **real, high-value** CMU passwords
  - 8 char, 4 class, dictionary check
  - Email, financial, grades, taxes, health, etc.
- Use **conforming subset** for all leaked data
- Associated servers logs, personnel records
- Complex process for safe handling

Michelle Mazurek et al. Measuring password guessability for an entire university. CCS 2013.

# Real vs. online vs. leaked

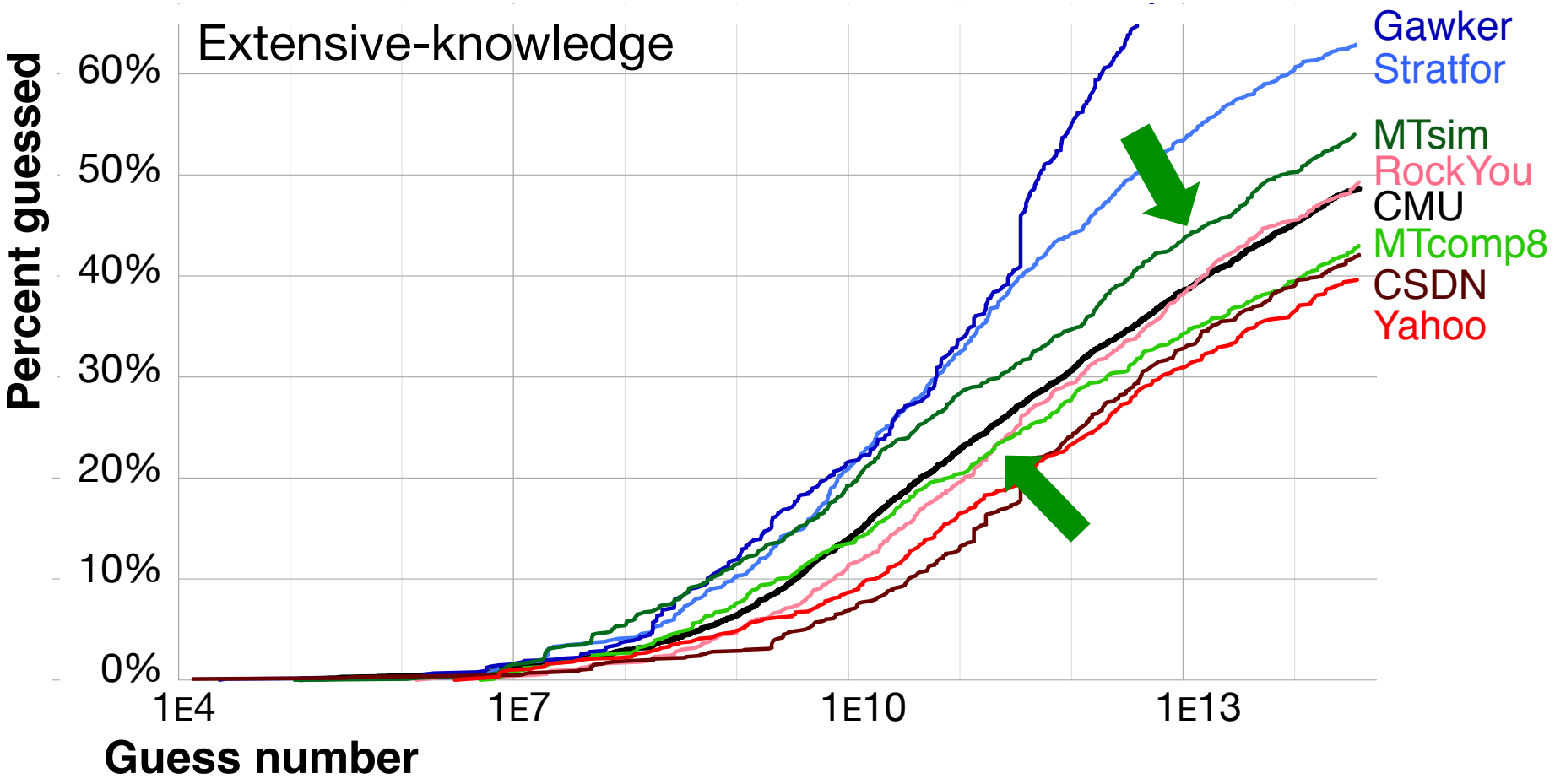
- Real CMU passwords
- Online studies
  - MTsim: Closest match to real CMU experience
  - MTcomp8: Similar password requirements
- Leaked: plaintext
  - RockYou, Yahoo!, CSDN
- Leaked: hashed and cracked
  - Gawker, StratFor

# Comparing sets – Guessability



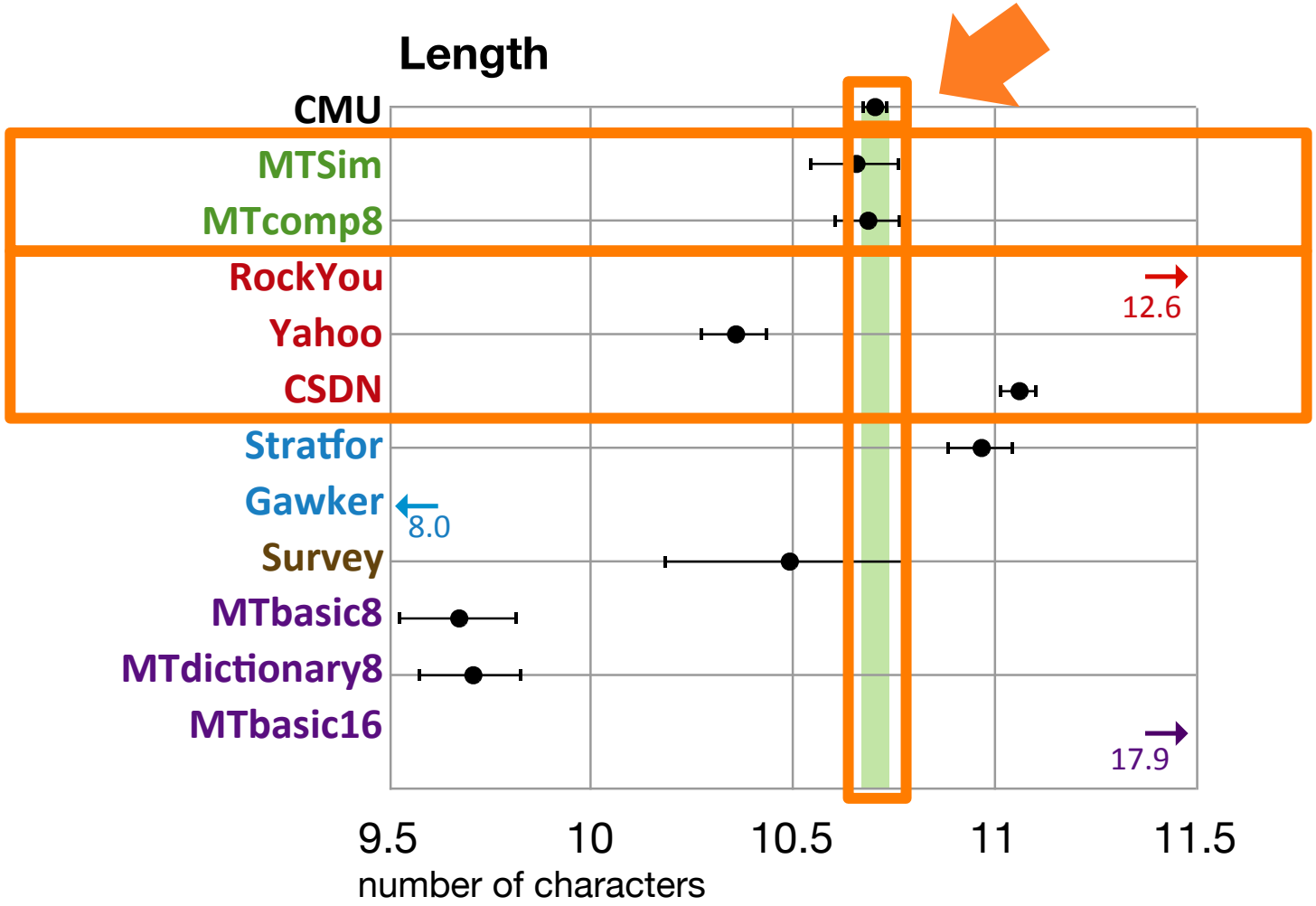

Leaked plaintext: RockYou close, others much tougher

# Comparing sets – Guessability




Online studies: Both close, MTcomp8 closer

# Comparing sets – Length




Overall: **Online studies closest** across metrics

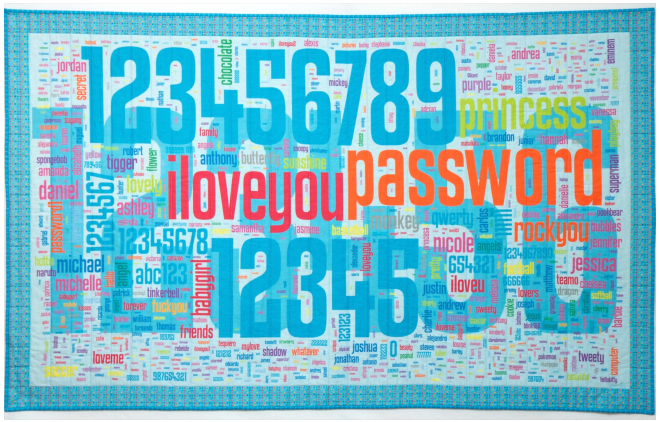
# Choosing a data source

- Lab: Higher quality data, deeper insights
  - Slow, small samples, expensive
- Online: Large samples, controlled experiments, fast
  - Specific samples, limited oversight
- Real: Most ecologically valid
  - Requires relationships, likely no experiments

# PASSWORD STUDY BEST PRACTICES

# Best practices: General

- Use a motivating scenario
- Ask whether behavior was realistic
- Use multiple usability metrics
- Require return for recall



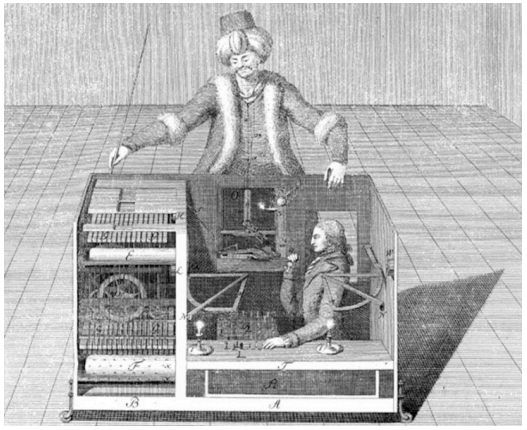
# Best practices: Lab studies

- Practice new schemes (graphical, gestures)
- Distraction tasks


usertesting.com

# Best practices: Online studies

- Ask about storage (and measure pasting)
- Offer a “show my password” option
- Control for language / geography
- Don’t ask for multiple passwords



siliconangle.com

# Reliable passwords research

- Carefully acquired experimental data is good
  - Real data is still better when possible
- Guesswork and guessability both reasonable
  - Depends on your specific context
  - Configure guessability effectively (or use PGS!)
- Good passwords research is expensive
  - Requires large samples
  - Can be computationally intensive

# Open questions

- What other metrics do we need?
  - Shoulder-surfing resistance
  - Resistance to online guessing
  - Resistance to targeted/insider attack
- How can we improve experimental validity?
  - In lab, online
  - Controlled experiments in the field?
  - Other security data beyond passwords

# Outline

1) 8:30am – 8:40am Intros

2) 8:40am – 8:50am Relevance of passwords

3) 8:50am – 9:10am Password security (threats, metrics)

4) 9:10am – 9:35am Robust, reliable experiments on passwords

5) 9:35am – 10:00am What we know about passwords

*10:00am – 10:30am Break*

6) 10:30am – 10:45am Approaches to guessing passwords

7) 10:45am – 11:10am Hands-on intro to Hashcat

8) 11:10am – 12:10pm Password-cracking contest

# Summary of What We Already Know

- Purpose: highlight bodies of knowledge
  - Impossible to be comprehensive
  - Please speak up to fill in missing work
  - Discuss interesting / uninteresting directions
- Lots of interesting work out of scope
  - Graphical passwords (Robert Biddle et al. Graphical passwords: Learning from the first twelve years. CSUR 2012)
  - Android gestures
  - Phone locking / unlocking

# People Can Make Bad Passwords

- Robert Morris and Ken Thompson. Password security: A case history. CACM 22, 11 (1979).
- Moshe Zviran and William J. Haga. Password security: an empirical study. J. Mgt. Info. Sys., 15(4), 1999.
- Joseph Bonneau. The science of guessing: Analyzing an anonymized corpus of 70 million passwords. IEEE S&P 2012.
- Matteo Dell'Amico et al. Password strength: An empirical analysis. INFOCOM 2010.
- Many analyses of leaked/stolen passwords

# How People Make Passwords

- Markus Jakobsson and Mayank Dhiman. The Benefits of Understanding Passwords. HotSec 2012.
- Joseph Bonneau and Ekaterina Shutova. Linguistic properties of multi-word passphrases. USEC 2012.
- Rafael Veras et al. Visualizing semantics in passwords: The role of dates. VizSec 2012.
- Cynthia Kuo et al. Human selection of mnemonic phrase-based passwords. SOUPS 2006.
- Blase Ur et al. "I added '!' at the end to make it secure": Observing password creation in the lab. SOUPS 2015.

# There May be Cultural Dimensions

- Zhigong Li et al. A Large-Scale Empirical Analysis of Chinese Web Passwords. USENIX Security 2014.
- Joseph Bonneau and Rubin Xu. Of contraseñas, סיסמאות and 密码: Character encoding issues for web passwords. W2SP 2012.

# Password-Composition Policies

- Philip Inglesant and M. Angela Sasse. The true cost of unusable password policies: Password use in the wild. CHI 2010.
- Saranga Komanduri et al. Of passwords and people: Measuring the effect of password-composition policies. CHI 2011.
- Richard Shay et al. Can long passwords be secure and usable? CHI 2014.

# Mobile Passwords are Different

- Florian Schaub et al. Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms. MUM 2012.
- Yulong Yang et al. Text entry method affects password security. LASER 2014.
- Emmanuel von Zezschwitz et al. Honey, I shrunk the keys: influences of mobile devices on password composition and authentication performance. NordiCHI 2014.
- William Melicher et al. Usability and security of text passwords on mobile devices. CHI 2016.

# Mental Models & Perceptions Matter

- Rick Wash. Folk models of home computer security. SOUPS 2010.
- L. Jean Camp. Mental models of privacy and security. IEEE T&S 2009.
- Adam J. Aviv and Dane Fichter. Understanding visual perceptions of usability and security of Android's graphical password pattern. ACSAC 2014.
- Blase Ur et al. Do Users' Perceptions of Password Security Match Reality? CHI 2016.
- Serge Egelman et al. Behavior Ever Follows Intention?: A Validation of the Security Behavior Intentions Scale (SeBIS). CHI 2016.
- Iulia Ion et al. "...no one can hack my mind": Comparing Expert and Non-Expert Security Practices. SOUPS 2015.

# Think About the Overall Ecosystem

- Anne Adams and M. Angela Sasse. Users are not the enemy. CACM, 42(12):40{46, 1999.
- Joseph Bonneau et al. The quest to replace passwords: A framework for comparative evaluation of Web authentication schemes. IEEE S&P 2012.
- Sonia Chiasson et al. Multiple password interference in text passwords and click-based graphical passwords. CCS 2009.
- Supriya Singh et al. Password sharing: Implications for security design based on social practice. CHI 2007.

# Password Management is Crucial

- Beate Grawemeyer and Hilary Johnson. Using and managing multiple passwords: A week to a view. Interacting with Computers, 23(3), June 2011.
- Shirley Gaw and Edward W. Felten. Password management strategies for online accounts. SOUPS 2006.
- Elizabeth Stobert and Robert Biddle. The password life cycle: User behaviour in managing passwords. SOUPS 2014.
- Elizabeth Stobert and Robert Biddle. Expert Password Management. Passwords 2016.

# Rethink Password Expiration

- Yinqian Zhang et al. The security of modern password expiration: An algorithmic framework and empirical analysis. CCS 2010.
- Sonia Chiasson and Paul C. van Oorschot. Quantifying the Security Advantage of Password Expiration Policies. DCC 2015.

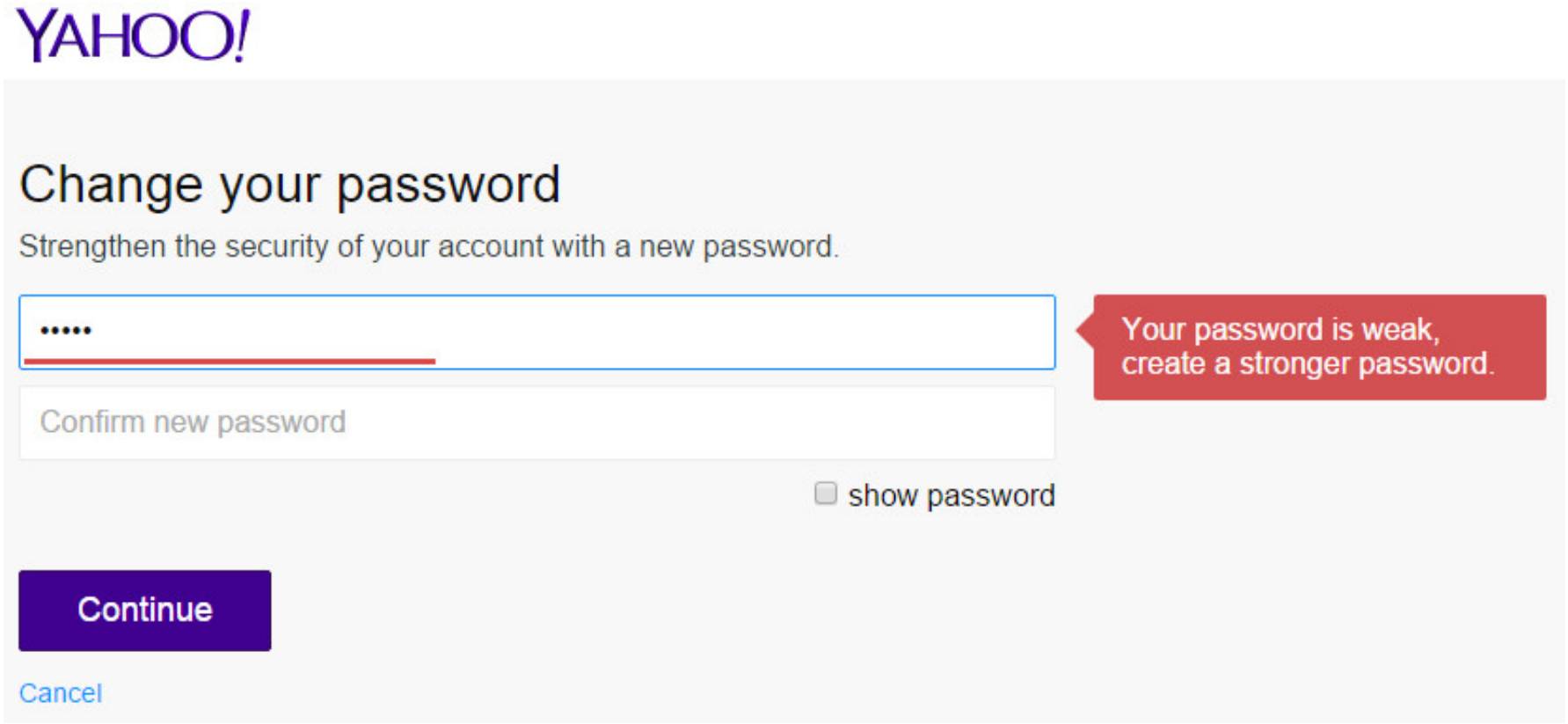
# People Reuse Passwords

- Dinei Florencio and Cormac Herley. A large-scale study of web password habits. WWW 2007.
- Anupam Das et al. The tangled web of password reuse. NDSS 2014.
- Rishab Nithyanand and Rob Johnson. The password allocation problem: Strategies for reusing passwords effectively. WPES 2013.
- Dinei Florencio et al. Password portfolios and the finite effort user: Sustainably managing large numbers of accounts. USENIX Security 2014.

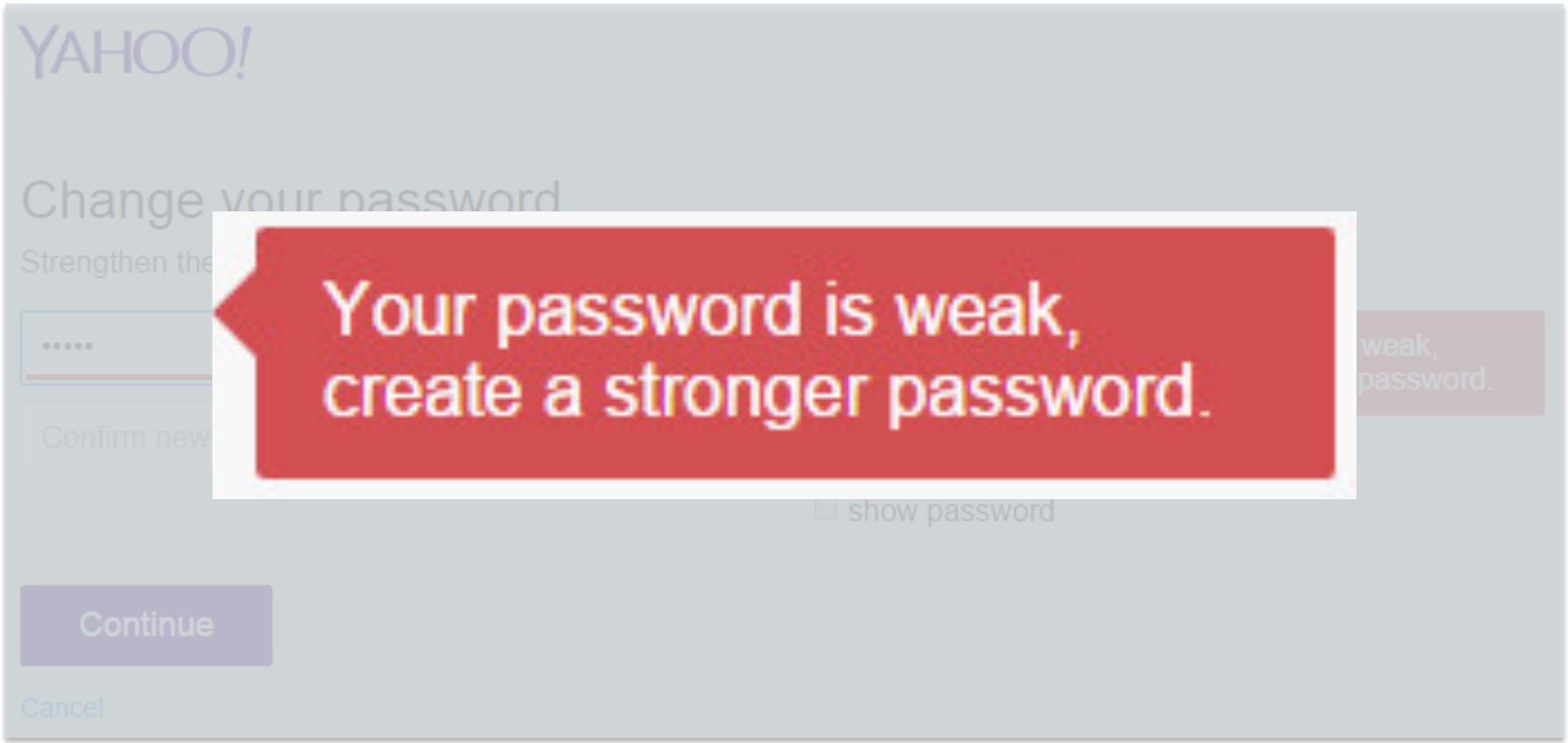
# Proactive Checking & Meters Matter

- Matt Bishop and Daniel V. Klein. Improving system security via proactive password checking. Computers & Security, 14(3): 233-249, 1995.
- Francesco Bergadano et al. Proactive password checking with decision trees. CCS 1997.
- Stuart Schechter et al. Popularity is everything: A new approach to protecting passwords from statistical-guessing attacks. HotSec 2010.
- Blase Ur et al. How does your password measure up? The effect of strength meters on password creation. USENIX Security 2012.
- Serge Egelman et al. Does my password go up to eleven? The impact of password meters on password selection. CHI 2013.

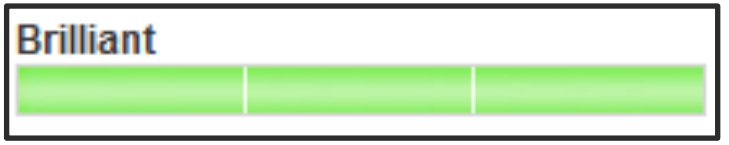
# Current User Feedback Insufficient



# Current User Feedback Insufficient



# Build Better Meters




- Xavier de Carne de Carnavalet and Mohammad Mannan. From very weak to very strong: Analyzing password-strength meters. NDSS 2014.
- Steven Acker et al. Password meters and generators on the web: From large-scale empirical study to getting it right. CODASPY 2015.
- Claude Castellucia et al. Adaptive password-strength meters from Markov models. NDSS 2012.
- Saranga Komanduri et al. Telepathwords: Preventing weak passwords by reading users' minds. USENIX Security 2014.
- Dan Wheeler. zxcvbn: Low-Budget Password Strength Estimation. USENIX Security 2016.

# One Can Nudge Users

- Alain Forget et al. Improving text passwords through persuasion. SOUPS 2008.
- Leah Zhang-Kennedy, S. Chiasson, and R. Biddle. Password advice shouldn't be boring: Visualizing password guessing attacks. eCRS, 2013.
- Andreas Sotirakopoulos et al. Motivating users to choose better passwords through peer pressure. SOUPS 2011 Poster.

# Take Into Account Human Memory

- Joseph Bonneau and Stuart Schechter. Towards reliable storage of 56-bit secrets in human memory. USENIX Security 2014.
- Manuel Blum and Santosh Vempala. Publishable Humanly Usable Secure Password Creation Schemas. HComp 2015.
- Jeremiah Blocki et al. Naturally Rehearsing Passwords. ASIACRYPT 2013.
- L. Jean Camp and Jacob Abbott. CPasswords: Leveraging Episodic Memory and Human-Centered Design for Better Authentication. HICSS 2016.
- Richard Shay et al. Correct horse battery staple: Exploring the usability of system-assigned passphrases. SOUPS 2012.
- Andreas Gutmann et al. ZETA - Zero-Trust Authentication: Relying on Innate Human Ability, not Technology. Euro S&P 2016.

# Store Passwords Smartly

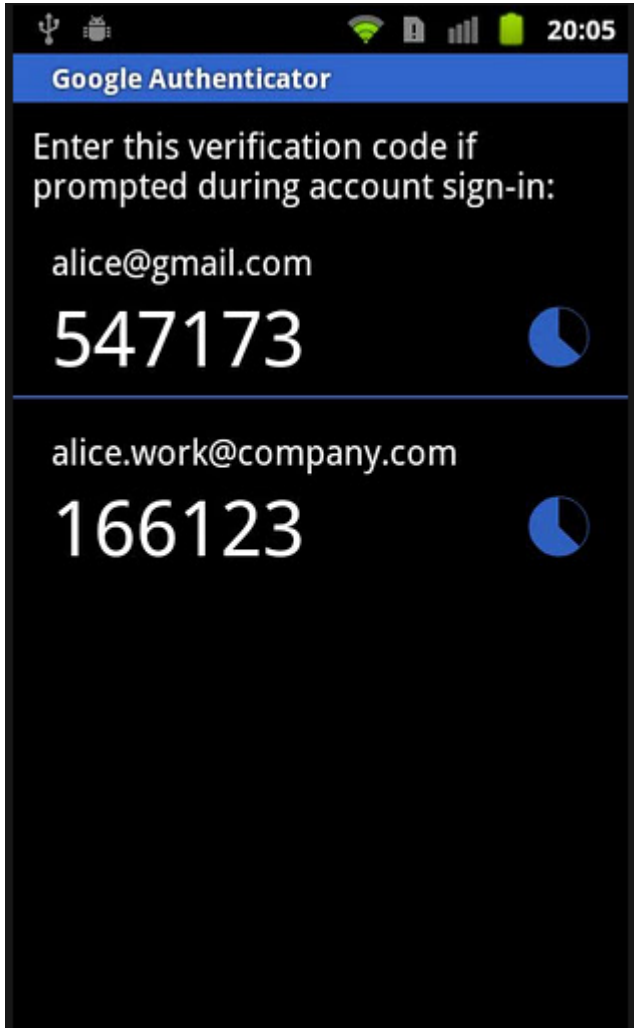
- Niels Provos and David Mazieres. A future-adaptable password scheme. In Proc. USENIX ATC 1999.
- Alex Biryukov et al. Fast and Tradeo -Resilient Memory-Hard Functions for Cryptocurrencies and Password Hashing. IACR Pre-print.
- Ari Juels and Ronald L. Rivest. Honeywords: Making password-cracking detectable. CCS, 2013.
- Rahul Chatterjee et al. Cracking-Resistant Password Vaults Using Natural Language Encoders. IEEE S&P 2015.
- Dinei Florencio et al. An administrator's guide to internet password research. LISA 2014.

# Single Sign-On


# Single Sign-On / Other Alternatives

- San-Tsai Sun et al. What Makes Users Refuse Web Single Sign-On? An Empirical Investigation of OpenID. SOUPS 2011.
- Lujo Bauer et al. A comparison of users' perceptions of and willingness to use Google, Facebook, and Google+ single-sign-on functionality. DIM 2013.
- Frank Stajano. Pico: No more passwords! SPW 2011.

# Two-Factor Auth



# Password Managers

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


1Password

# Improving Password Managers

- Daniel McCarney et al. Tapas: design, implementation, and usability evaluation of a password manager. ACSAC 2012.
- Zhiwei Li et al. The Emperor's New Password Manager: Security Analysis of Web-based Password Managers. USENIX Security 2014.
- Hristo Bojinov et al. Kamouflage: Loss-Resistant Password Management. ESORICS 2010.
- Ambarish Karole et al. A comparative usability evaluation of traditional password managers. ISC 2010.

# Outline

1) 8:30am – 8:40am Intros

2) 8:40am – 8:50am Relevance of passwords

3) 8:50am – 9:10am Password security (threats, metrics)

4) 9:10am – 9:35am Robust, reliable experiments on passwords

5) 9:35am – 10:00am What we know about passwords

*10:00am – 10:30am Break*

6) 10:30am – 10:45am Approaches to guessing passwords

7) 10:45am – 11:10am Hands-on intro to Hashcat

8) 11:10am – 12:10pm Password-cracking contest

# Outline

1) 8:30am – 8:40am Intros

2) 8:40am – 8:50am Relevance of passwords

3) 8:50am – 9:10am Password security (threats, metrics)

4) 9:10am – 9:35am Robust, reliable experiments on passwords

5) 9:35am – 10:00am What we know about passwords

*10:00am – 10:30am Break*

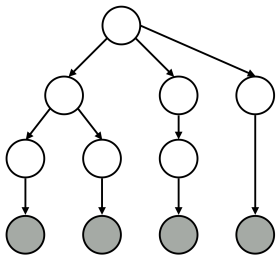
6) 10:30am – 10:45am Approaches to guessing passwords

7) 10:45am – 11:10am Hands-on intro to Hashcat

8) 11:10am – 12:10pm Password-cracking contest

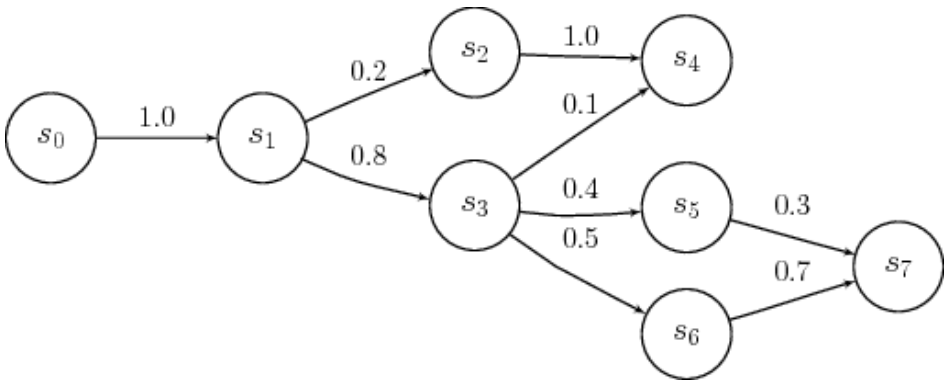
# Password-Guessing Attacks

- Guessing attacks are data-driven
  - Previously stolen passwords
  - Natural-language corpora
- Array of tools
  - Cracking software
  - Academic algorithms



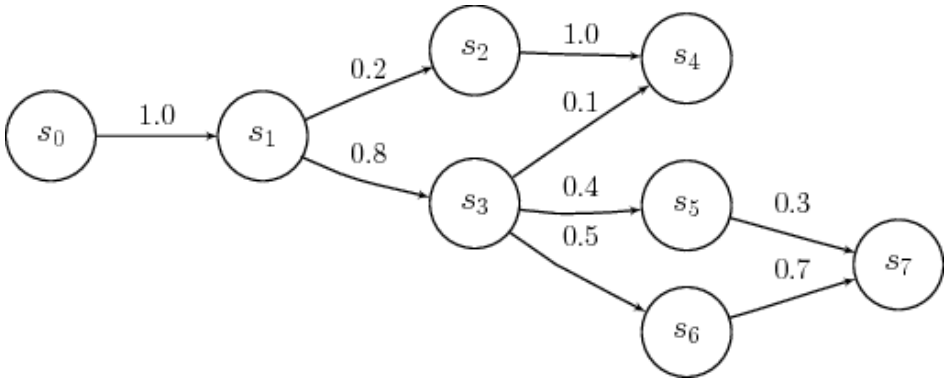

# Markov Models

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

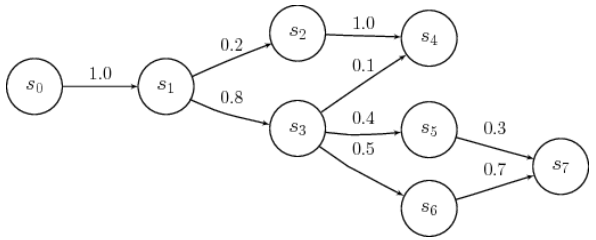


# Markov Models

- Arvind Narayanan and Vitaly Shmatikov. Fast dictionary attacks on passwords using time-space tradeoff. CCS 2005.
- Jerry Ma et al. A study of probabilistic password models. IEEE S&P 2014.
- Markus Durmuth et al. OMEN: Faster password guessing using an ordered markov enumerator. ESSoS 2015.
- Matteo Dell'Amico and Maurizio Filippone. Monte Carlo strength evaluation: Fast and reliable password checking. CCS 2015.

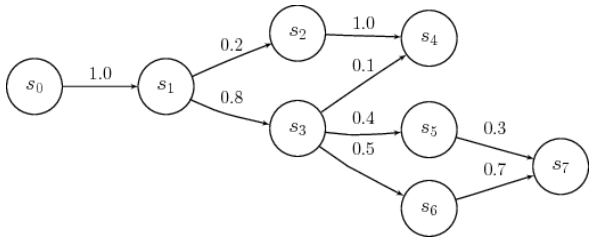


# Markov Models



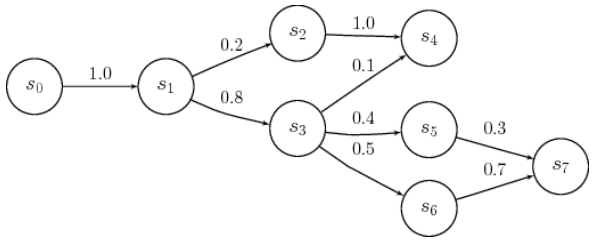

usenixsecurity

# Markov Models



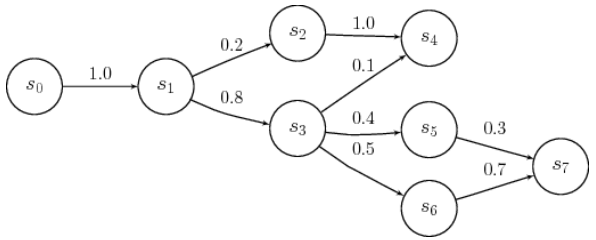

usenixsecurity

# Markov Models



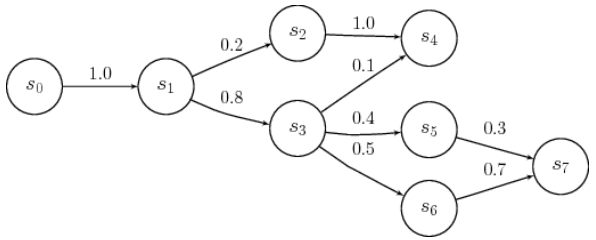

usenixsecurity

# Markov Models




usenixsecurity

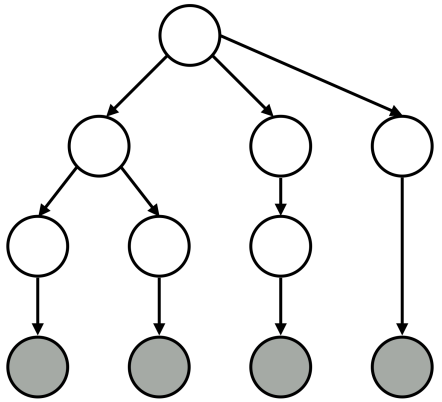
# Markov Models




usenixsecurity

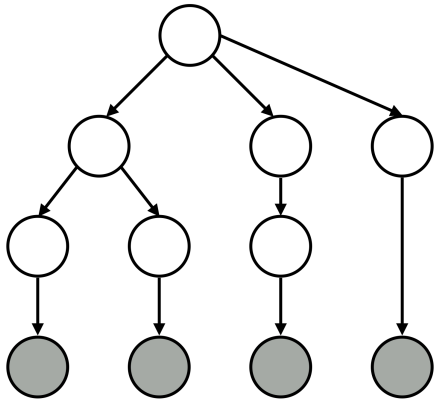
# Probabilistic Context-Free Grammars

- Generate password grammar
  - Structures
  - Terminals



# Probabilistic Context-Free Grammars

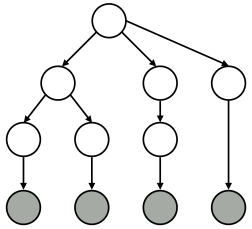
- Generate password grammar
  - Structures
  - Terminals



# Probabilistic Context-Free Grammars

- Matt Weir et al. Password cracking using probabilistic context-free grammars. IEEE S&P 2009.
- Patrick Gage Kelley et al. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. IEEE S&P 2012.
- Rafael Veras et al. On the semantic patterns of passwords and their security impact. NDSS 2014.
- Saranga Komanduri. Modeling the adversary to evaluate password strength with limited samples. PhD thesis, CMU, 2015.

# PCFG



*passwordpassword*

*password123*

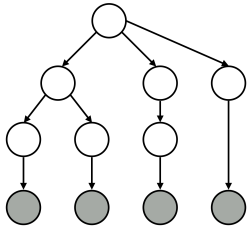
*usenix3*

*5ecurity*

*iloveyou*

*nirvana123*

# PCFG



*passwordpassword*

*password123*

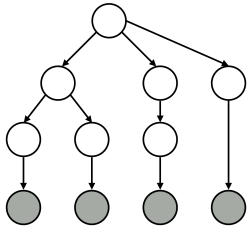
*usenix3*

*5ecurity*

*iloveyou*

*nirvana123*

# PCFG



*passwordpassword*

*password123*

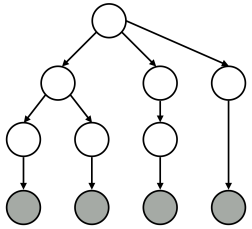
*usenix3*

*5ecurity*

*iloveyou*

*nirvana123*

# PCFG



*passwordpassword*

*password123*

*usenix3*

*5ecurity*

*iloveyou*

*nirvana123*

# Neural Networks (Preview)

- William Melicher et al. Fast, lean, and accurate: modeling password guessability using neural networks. USENIX Security 2016.

# Wordlist tools

- John the Ripper, Hashcat

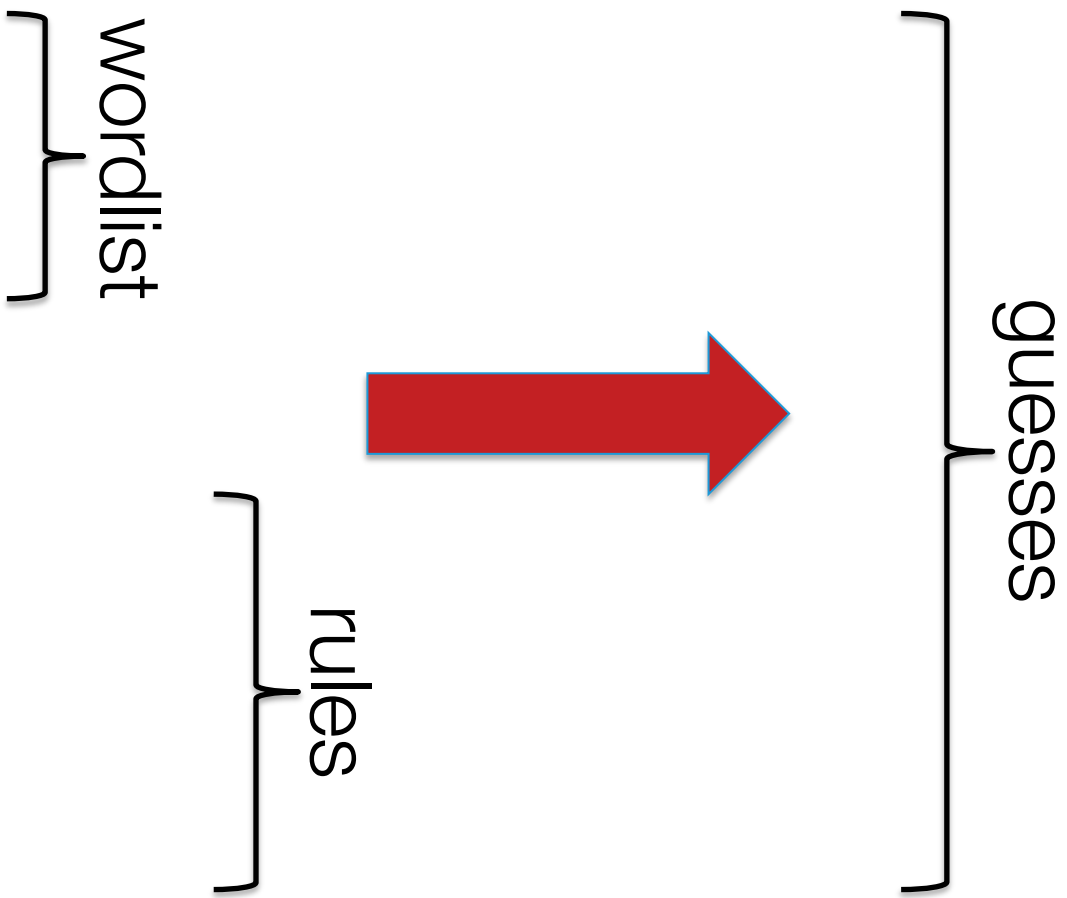

# Wordlist tools

- John the Ripper, Hashcat
- Guess variants of input wordlist


# Wordlist tools

- John the Ripper, Hashcat
- Guess variants of input wordlist
- Wordlist mode requires:
  - Wordlist (passwords and dictionary entries)
  - Mangling rules


# John the Ripper



# John the Ripper


*blase*

*carnegie*

wordlist

rules

guesses

# John the Ripper


*blase*

*carnegie*

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

guesses

# John the Ripper


*blase*

*carnegie*

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

blase

carnegie

blase1

carnegie1

blas3

carn3gi3

guesses

# John the Ripper


*blase*

*carnegie*

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

blase

carnegie

blase1

carnegie1

blas3

carn3gi3

guesses

# John the Ripper


*blase*

*carnegie*

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

blase

carnegie

blase1

carnegie1

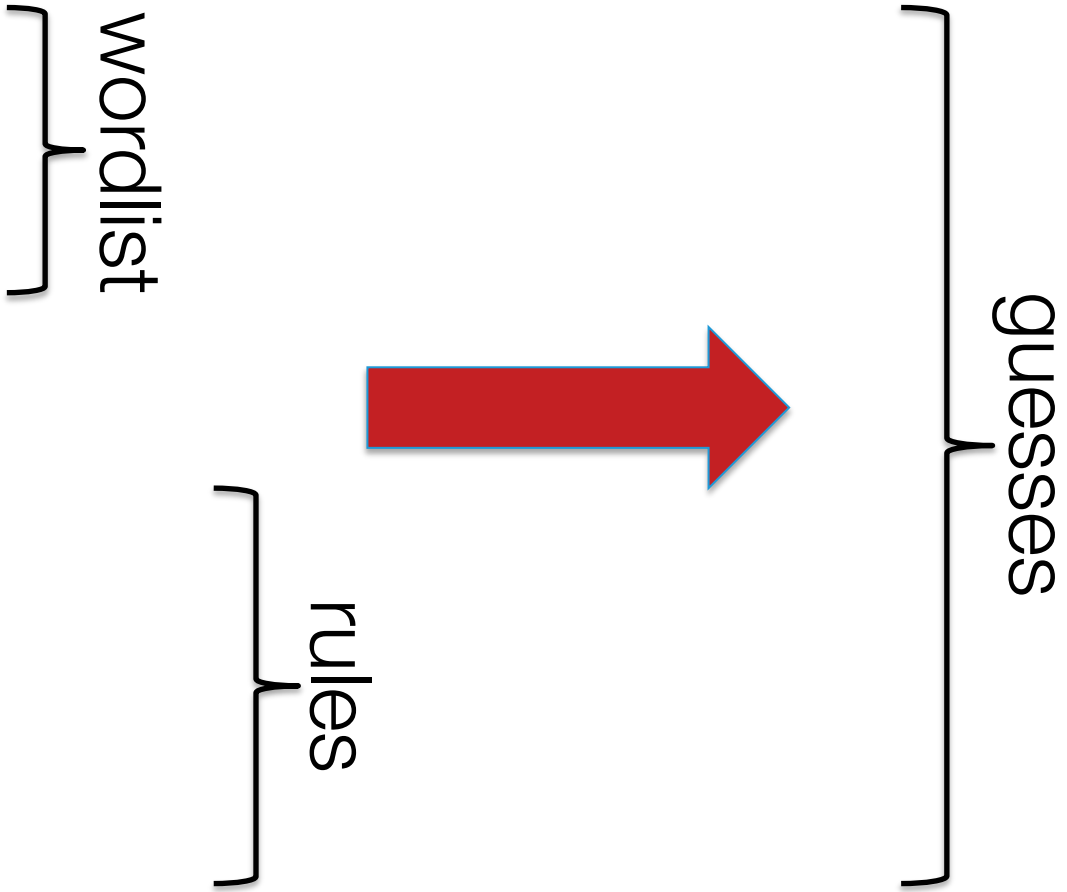
blas3

carn3gi3

guesses

# Hashcat


hashcat
advanced
password
recovery


wordlist
rules
guesses

# Hashcat


*blase*

*carnegie*

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

guesses

# Hashcat


*blase*

*carnegie*

wordlist

blase

blase1

blas3

[ ]

[add 1 at end]

[change e to 3]

rules

carnegie

carnegie1

carn3gi3

guesses

# Hashcat


*blase*

*carnegie*

wordlist

[ ]

[add 1 at end]

[change e to 3]

rules

blase

blase1

blas3

carnegie

carnegie1

carn3gi3

guesses

# Other Work on Password Guessing

- Markus Durmuth et al. When privacy meets security: Leveraging personal information for password cracking. CoRR 2013.
- Joseph Bonneau. Statistical metrics for individual password strength. WPS 2012.
- Matt Weir et al. Testing metrics for password creation policies by attacking large sets of revealed passwords. CCS 2010.
- Yiannis Chrysanthou. Modern password cracking: A hands-on approach to creating an optimised and versatile attack. Master's thesis, Royal Holloway, University of London, 2013.
- http://arstechnica.com/security/2012/08/passwords-under-assault/
- AbdelRahman Abdou et al. What Lies Beneath? Analyzing Automated SSH Bruteforce Attacks. Passwords 2016.

# Recall: Advantages of Guessability

- Straightforward
- Models an attacker
- Per-password strength estimates

Blase Ur et al. Measuring real-world accuracies and biases in modeling password guessability. USENIX Security 2015.

# Guessability in Practice

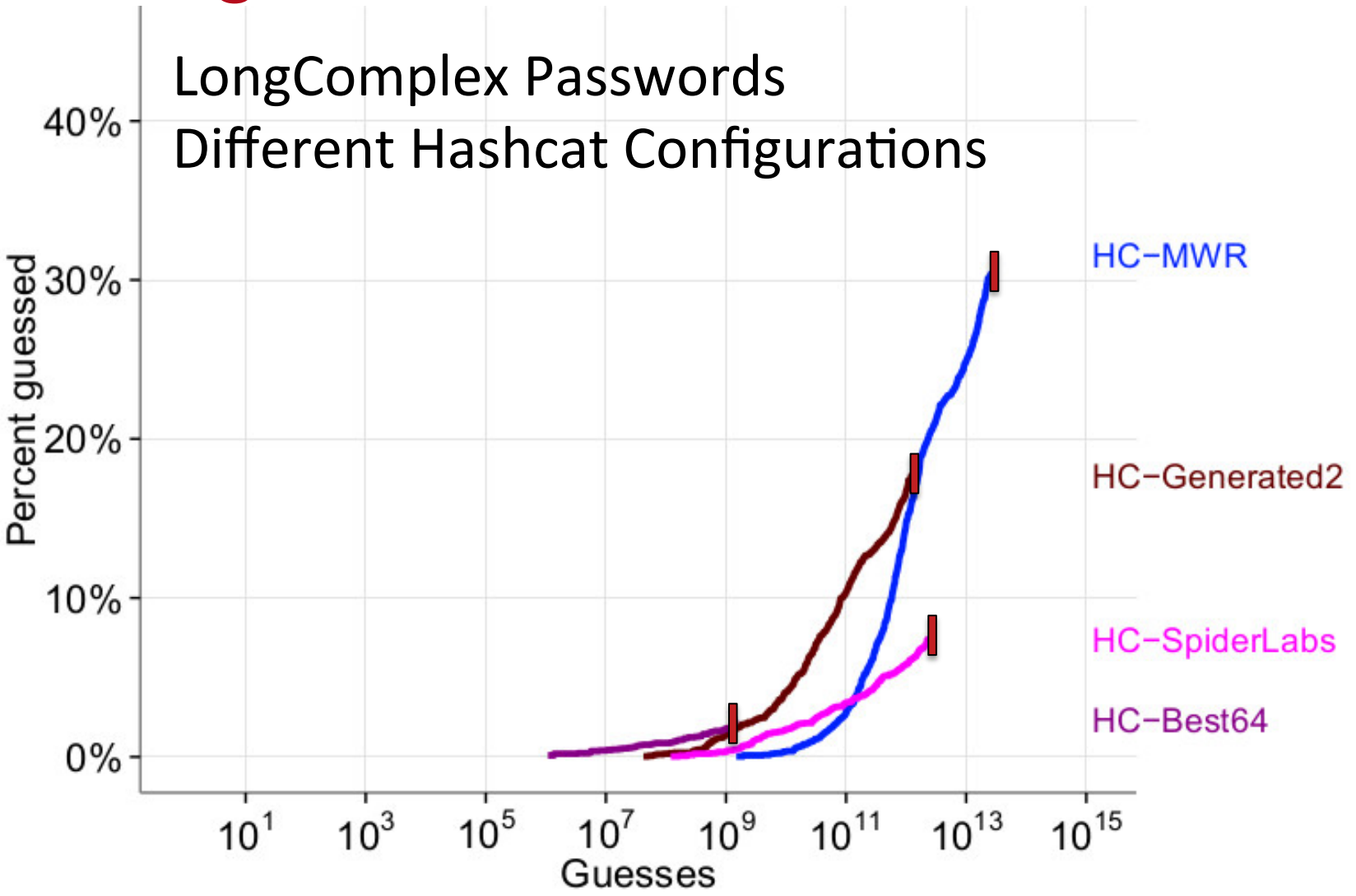
- Default (inexpert) configurations
- Single guessing approach

# Guessability in Practice

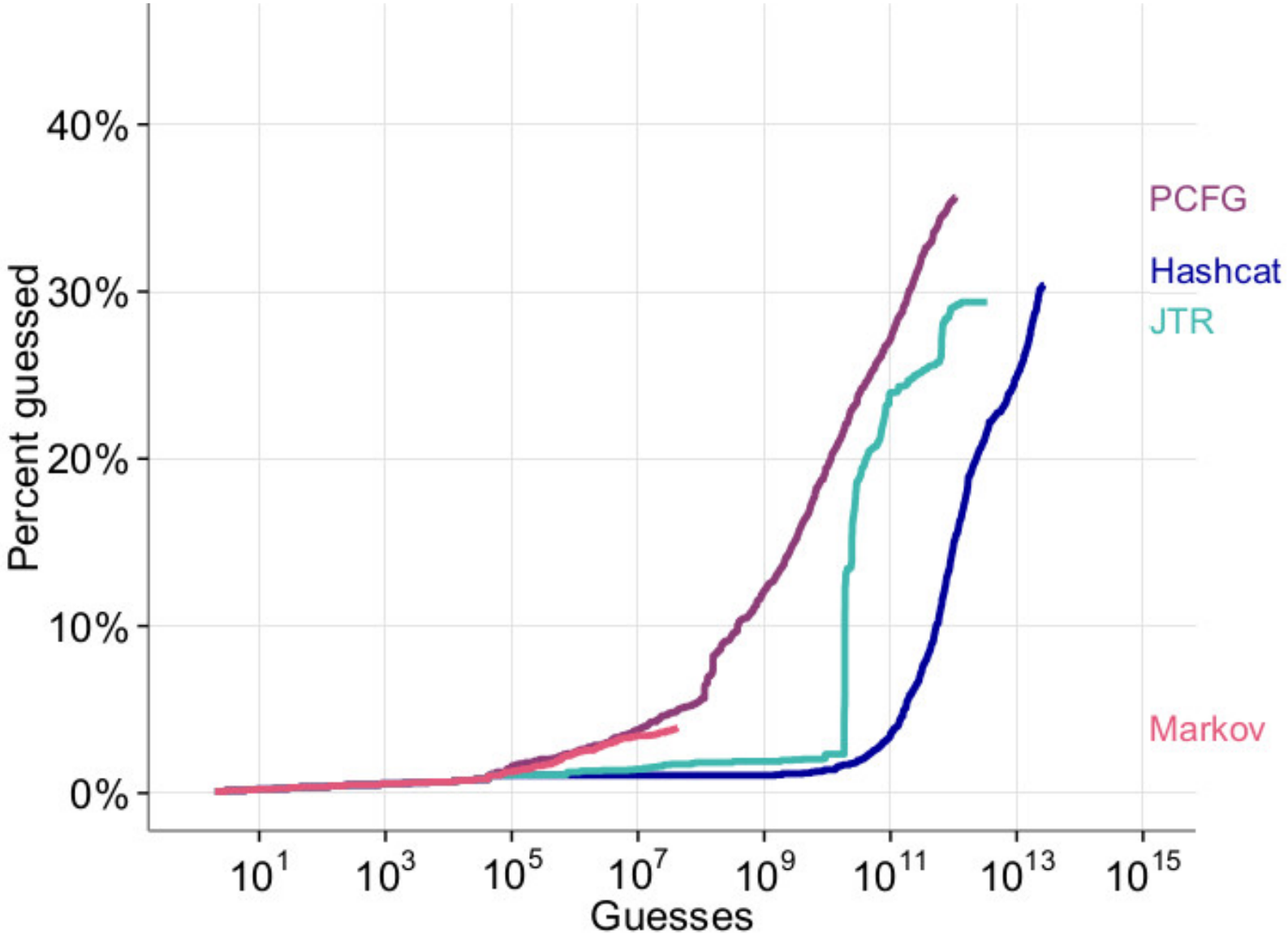
- Default (inexpert) configurations
- Single guessing approach

- How does this compare to professionals?
- How does it impact research results?

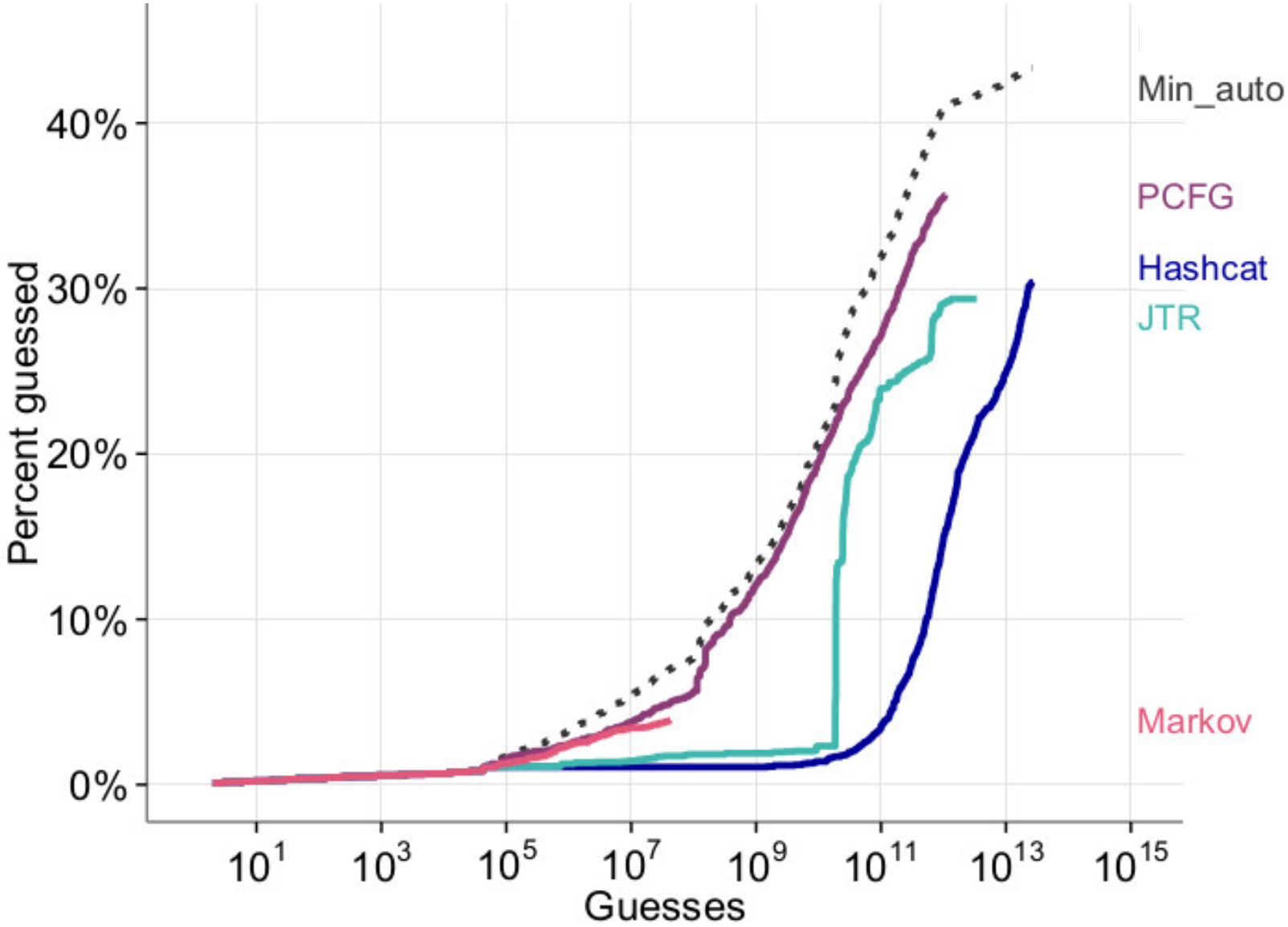
# Configuration Is Crucial



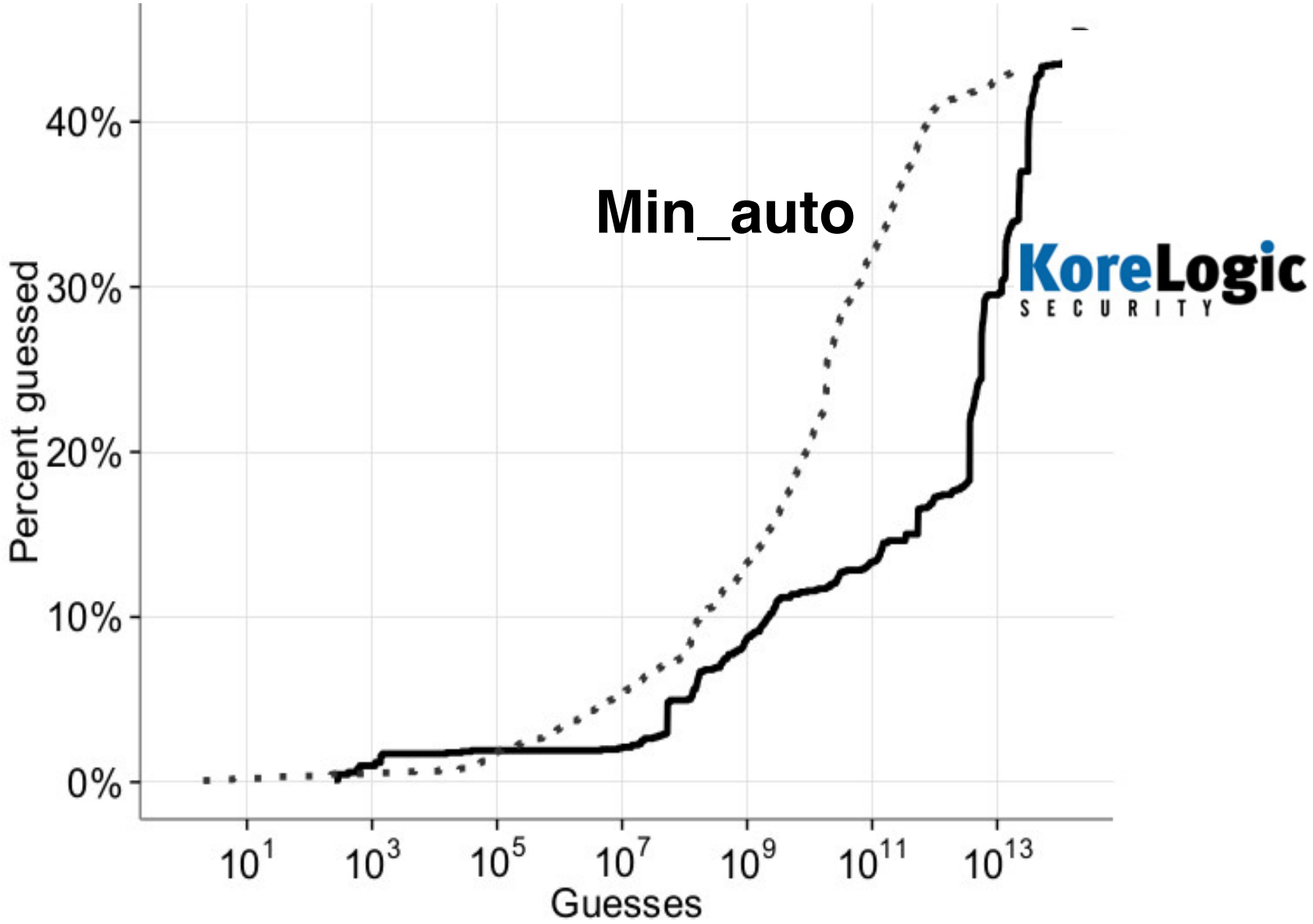
# Comparison for Complex Passwords



# Comparison for Complex Passwords



# Min_auto Conservative Proxy for Pros



# Per-Password Highly Impacted

```
P@ssw0rd!
```

# Per-Password Highly Impacted

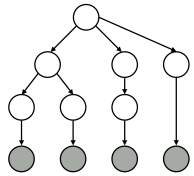
- JTR guess # 801


```
P@ssw0rd!
```

# Per-Password Highly Impacted

- JTR guess # 801


- Not guessed in $10^{14}$ PCFG guesses

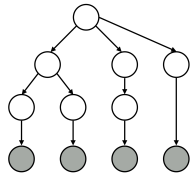


`P@ssw0rd!`

# Per-Password Highly Impacted

- JTR guess # 801


- Not guessed in $10^{14}$ PCFG guesses



P@ssw0rd!

# Conclusions

- Running a single approach is insufficient
  - Especially out of the box
- Multiple approaches proxy for pros

# Password Guessability Service (PGS)

- Guessability of plaintext passwords

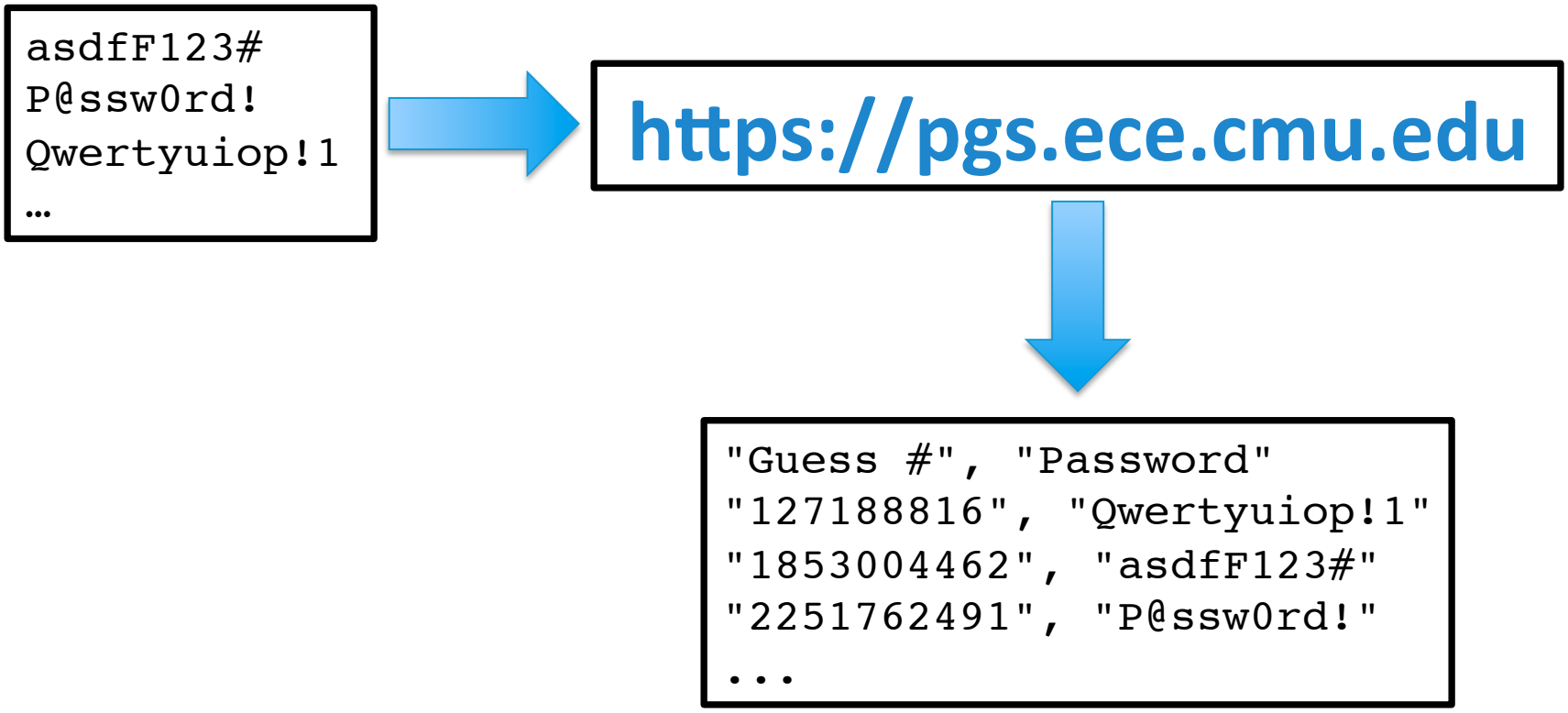
**https://pgs.ece.cmu.edu**

# Password Guessability Service (PGS)

- Guessability of plaintext passwords

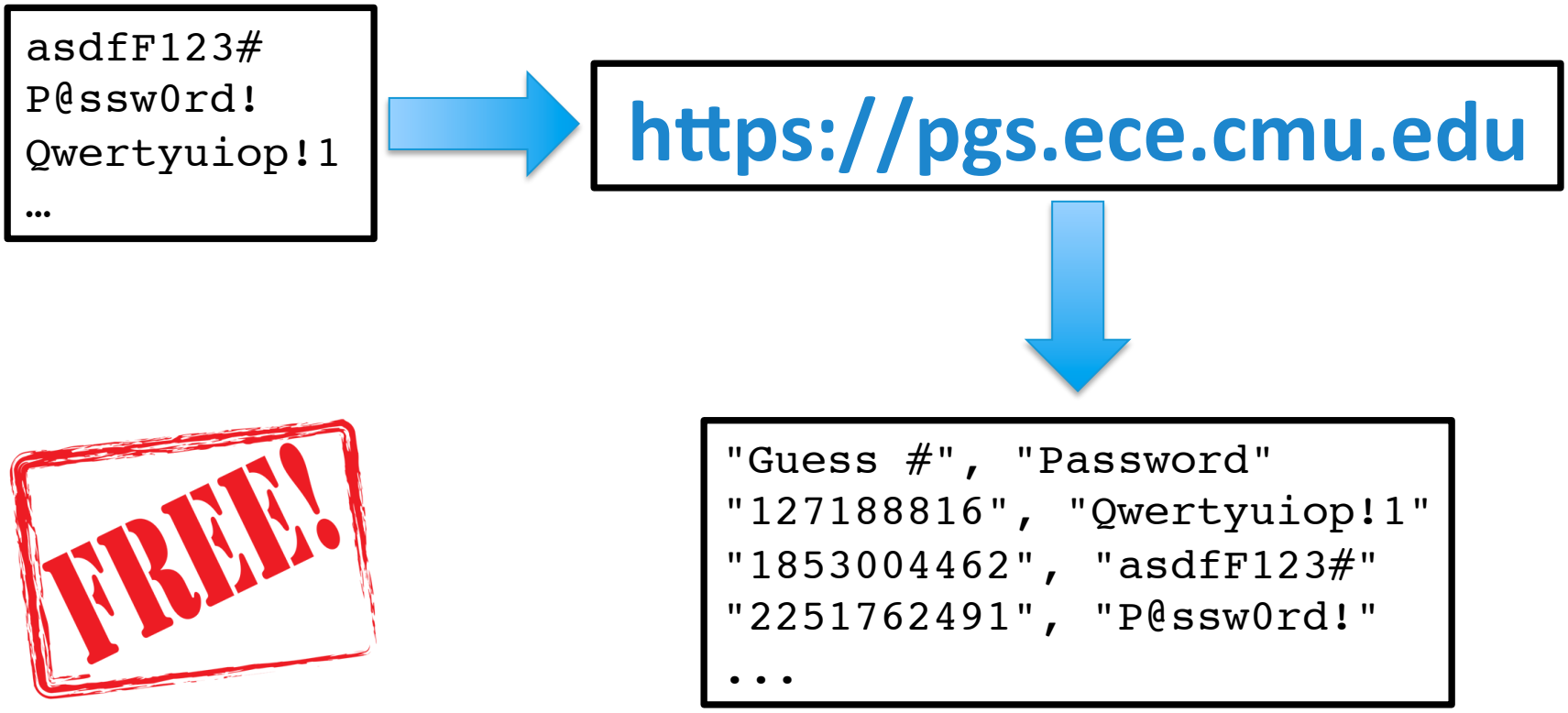
# Password Guessability Service (PGS)

- Guessability of plaintext passwords



# Password Guessability Service (PGS)

- Guessability of plaintext passwords



# Outline

1) 8:30am – 8:40am Intros

2) 8:40am – 8:50am Relevance of passwords

3) 8:50am – 9:10am Password security (threats, metrics)

4) 9:10am – 9:35am Robust, reliable experiments on passwords

5) 9:35am – 10:00am What we know about passwords

*10:00am – 10:30am Break*

6) 10:30am – 10:45am Approaches to guessing passwords

7) 10:45am – 11:10am Hands-on intro to Hashcat

8) 11:10am – 12:10pm Password-cracking contest