

RSA[®]Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: HT-T06C

The Quest for Usable and Secure Passwords

Lujo Bauer

Associate Professor of ECE & CS
Carnegie Mellon University
[@lujobauer](#)



#RSAC

RSA[®]Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: HT-T06C

The Quest for Usable and Secure Passwords

Felicia Alfieri, Maung Aung, **Lujo Bauer**, Jonathan Bees, **Nicolas Christin**, Jessica Colnago, **Lorrie Faith Cranor**, Summer Devlin, Harold Dixon, Adam L. Durity, Serge Egelman, Pardis Emami-Naeini, Alain Forget, Hana Habib, Philip (Seyoung) Huh, Noah Johnson, Pranshu Kalvani, Patrick Gage Kelley, **Saranga Komanduri**, Joel Lee, Julio López, Michael Maass, **Michelle L. Mazurek**, Darya Melicher, **William Melicher**, Fumiko Noma, Maggie Oates, Timothy Passaro, Sarah Pearman, **Sean M. Segreti**, **Richard Shay**, Chelse Swoopes, Jeremy Thomas, **Blase Ur**, Timothy Vidas

#RSAC

How Do We Make Passwords Better?

Goal: Make passwords harder to guess
... without making them too hard to remember

Tools: Password-composition policies,
password meters, user education, ...

Problem: How to apply and evaluate these tools?

Scientific Experiments Need Data and Measurement

- What to measure?
 - Security (historically: entropy)
 - Usability \approx recall rates, timings, sentiment, ...
- How to obtain passwords?
 - Created under different policies, with/without meters, ...
 - Potential sources: Leaked plaintext passwords, leaked + cracked passwords, online studies, lab studies, real passwords

How to Measure Security of Passwords?

Easy for an attacker to guess → weak / insecure password

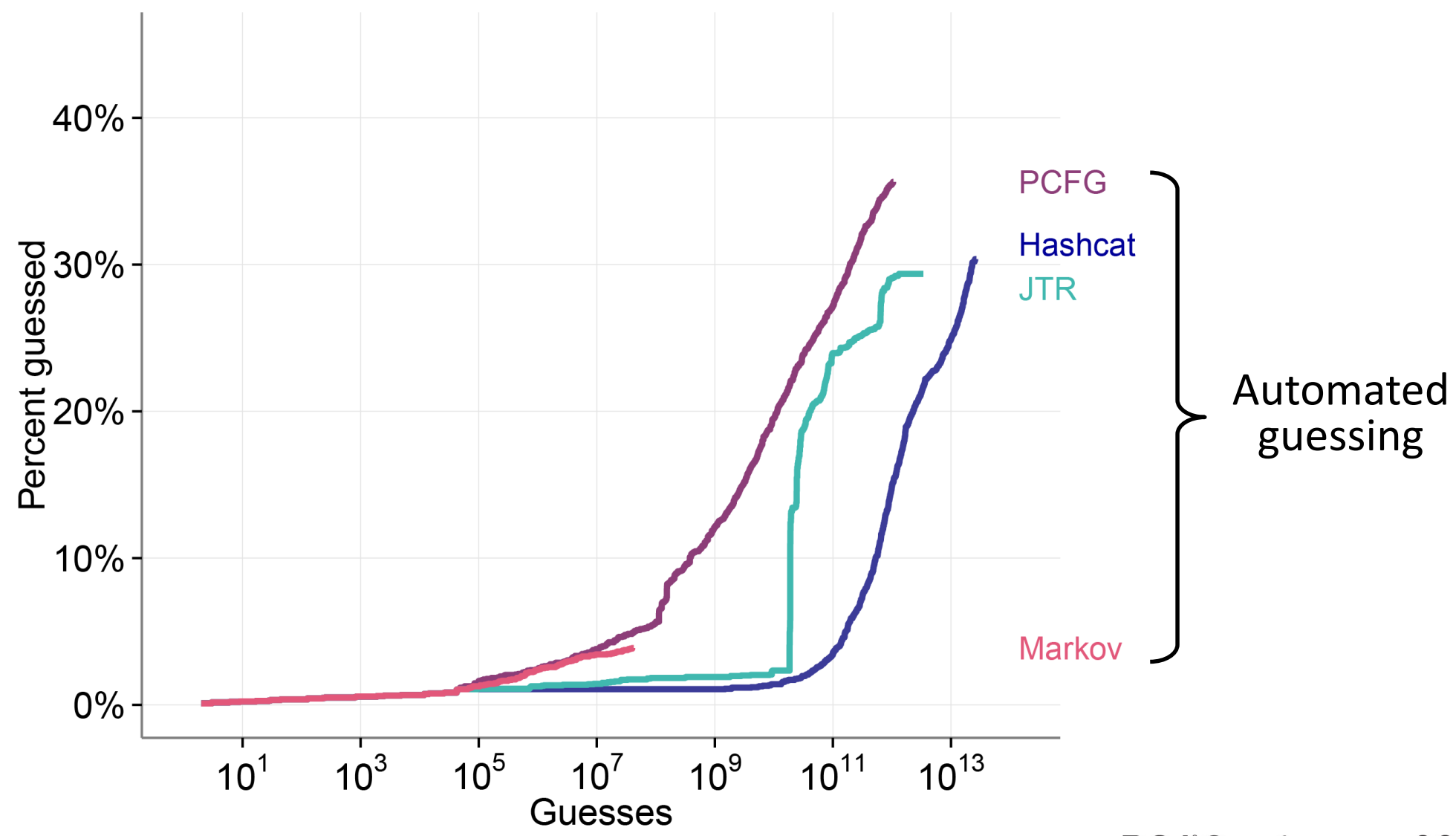
Hard for an attacker to guess → strong / secure password

Our approach: Measure security by simulating how long an attacker would need to guess a password

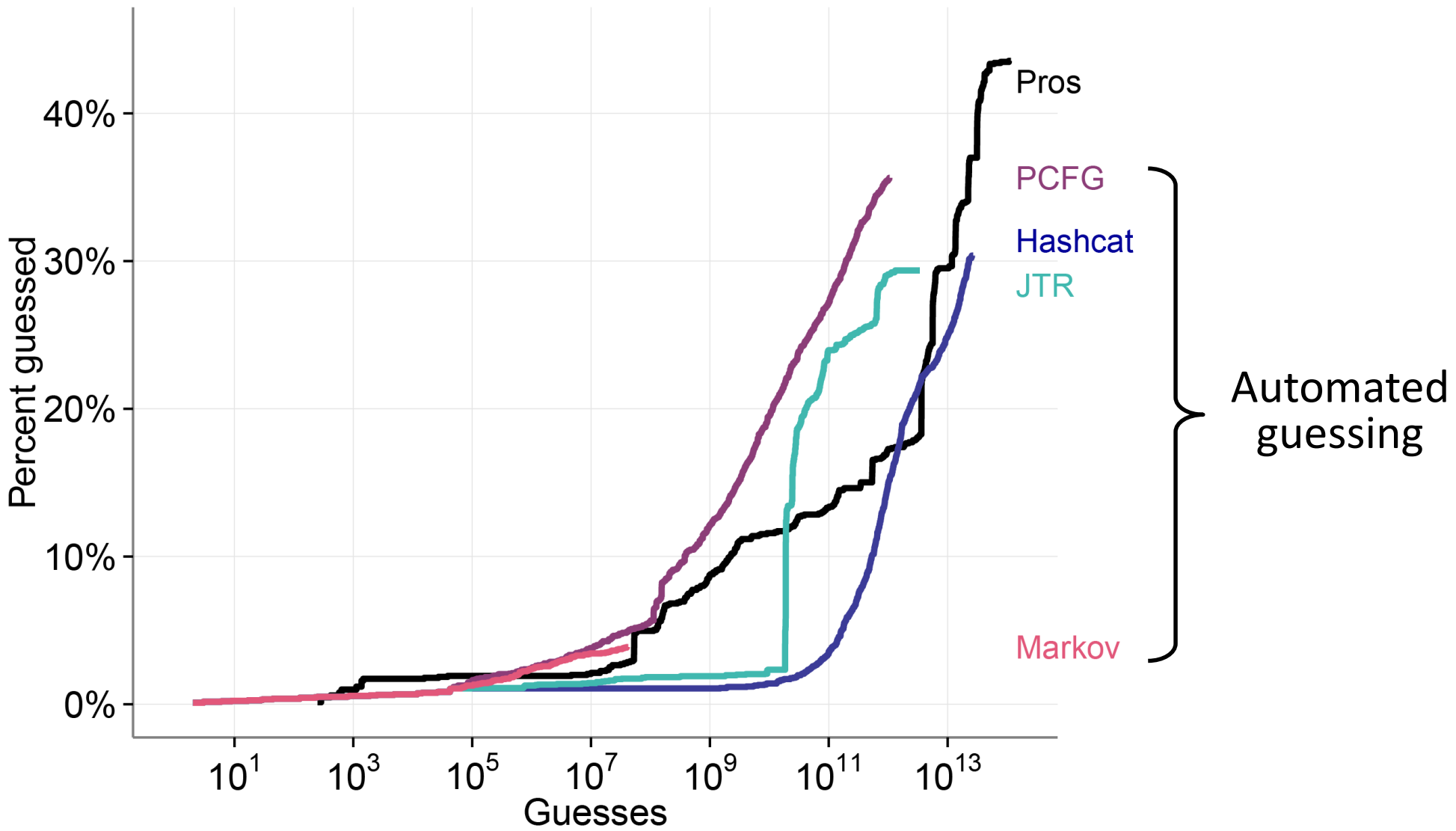
How to Simulate Attacker?

- Compared 4 main guessing algorithms/tools
 - John the Ripper (JTR)
 - Hashcat
 - Markov model-based
 - PCFG
 - And hired a professional password recovery firm!
 - Professionals \approx attackers
- × many configs and training data sets

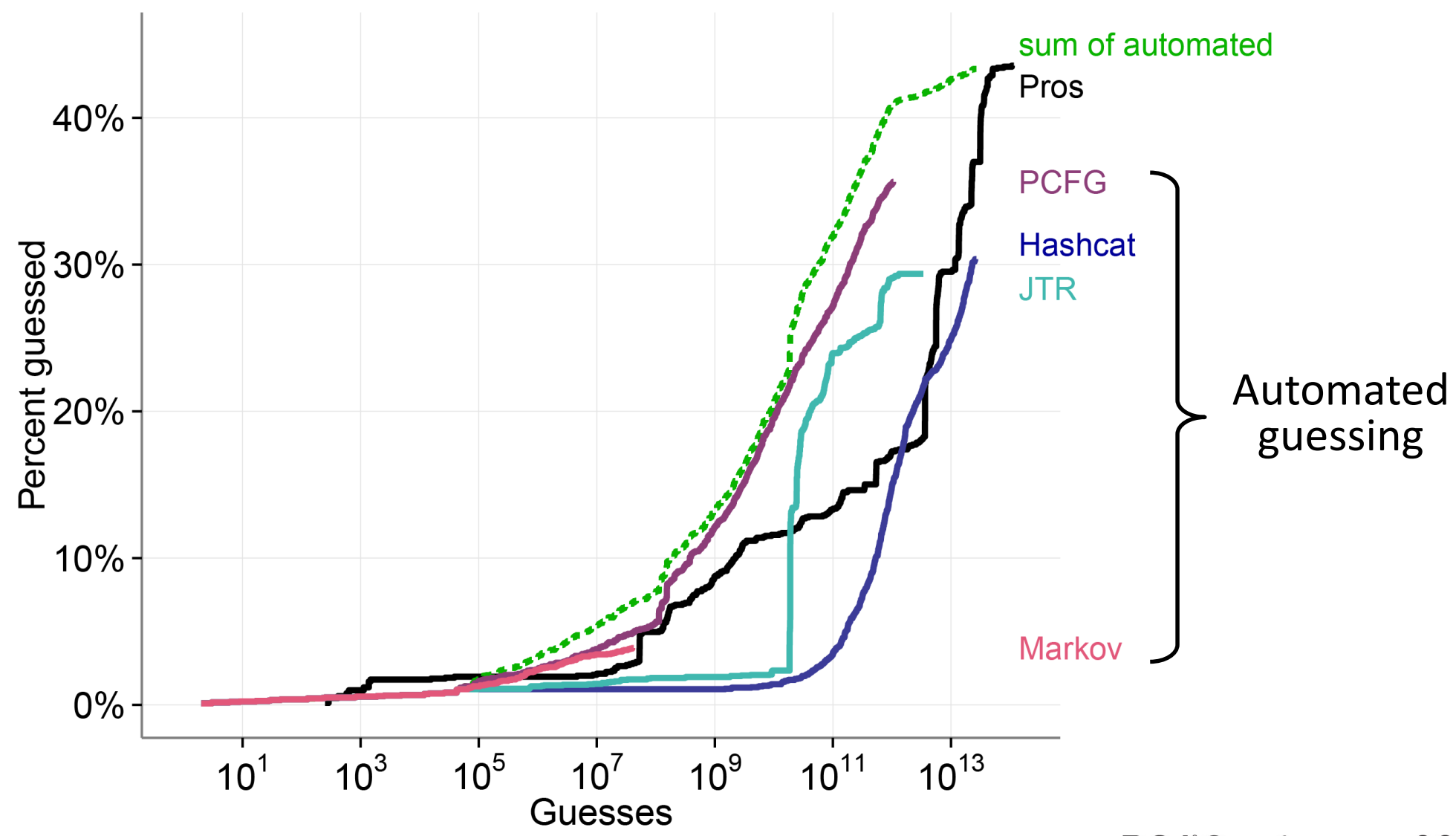
Comparing Approaches to Simulate Attacker



Comparing Approaches to Simulate Attacker



Finding: Sum of Automated Guessing \approx Attackers



Scientific Experiments Need Data and Measurement

- What to measure?
 - Security (historically: entropy)
 - Usability \approx recall rates, timings, sentiment, ...
- How to obtain passwords?
 - Created under different policies, with/without meters, ...
 - Potential sources: Leaked plaintext passwords, leaked + cracked passwords, online studies, lab studies, real passwords



Scientific Experiments Need Data and Measurement

- What to measure?
 - Security \approx guessability
 - Usability \approx recall rates, timings, sentiment, ...
- How to obtain passwords?
 - Created under different policies, with/without meters, ...
 - Potential sources: Leaked plaintext passwords, leaked + cracked passwords, online studies, lab studies, real passwords



Scientific Experiments Need Data and Measurement

- What to measure?

- Security \approx guessability
- Usability \approx recall rates, timings, sentiment, ...

efficiently ?

Deep learning can measure password strength faster and more accurately!

- How to obtain passwords?

- Created under different policies, with/without meters, ...
- Potential sources: Leaked plaintext passwords, leaked + cracked passwords, online studies, lab studies, real passwords

Scientific Experiments Need Data and Measurement

- What to measure?

- Security \approx guessability
- Usability \approx recall rates, timings, sentiment, ...



Pwd strength calculation service:
pgs.ece.cmu.edu

Neural network:
[github.com/cupslab/
neural_network_cracking](https://github.com/cupslab/neural_network_cracking)

- How to obtain passwords?

- Created under different policies, with/without meters, ...
- Potential sources: Leaked plaintext passwords, leaked + cracked passwords, online studies, lab studies, real passwords

Scientific Experiments Need Data and Measurement

- What to measure?
 - Security \approx guessability
 - Usability \approx recall rates, timings, sentiment, ...
- How to obtain passwords?
 - Created under different policies, with/without meters, ...
 - Potential sources: Leaked plaintext passwords, leaked + cracked passwords, online studies, lab studies, real passwords



How to Obtain Passwords to Study?

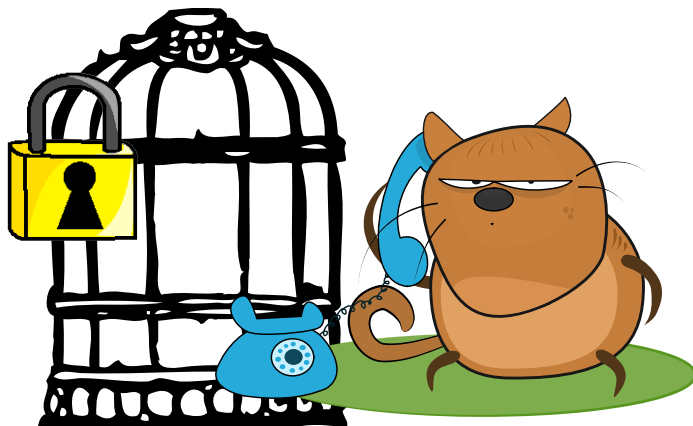
Recipe:

1. Become *very* good friends with IT and information security groups at your institution
2. Collect real-world plaintext passwords for analysis
3. Compare strength against: leaked plaintext passwords, leaked + cracked passwords, online studies, lab studies

How to Obtain Passwords to Study?

Recipe:

1. Become *very* good friends with IT and information security groups at your institution
2. Collect real-world plaintext passwords for analysis



How to Obtain Passwords to Study?

Outcome:

1. Passwords collected in *carefully crafted* online studies can be a good approximation of real-world passwords*
2. Yes, computer scientists have stronger passwords than engineers**
3. ... but both have much stronger passwords than business school students and faculty***

Scientific Experiments Need Data and Measurement

- What to measure?
 - Security \approx guessability
 - Usability \approx recall rates, timings, sentiment, ...
- How to obtain passwords?
 - Created under different policies, with/without meters, ...
 - Potential sources: Leaked plaintext passwords, leaked + cracked passwords, online studies, lab studies, real passwords



100,000+ User Study Passwords Later ...

Some insights and guidelines for strong and usable passwords

- Length is better than complexity for both security and usability
 - But need a little complexity, too
- Blacklisting weak passwords is a must
 - But have to explain reasoning to users, too
- Feedback to users can help to create stronger passwords
 - But can't be too strict or too complicated

100,000+ User Study Passwords Later ...

Some insights and guidelines for strong and usable passwords

+

neural networks to measure strength

=

an effective, deployable password meter

100,000+ User Study Passwords Later ...

Feedback based on
data + measurement!

The screenshot shows a password creation form. The 'Username' field contains 'Lujo'. The 'Password' field contains 'Monkey456789' and is highlighted with a red box. Below the password field is a 'Show Password & Detailed Feedback' checkbox. To the right of the password field is a feedback panel, also outlined in red, which contains the following text:

Your password is very easy to guess.

- Don't use dictionary words (**Monkey**) ([Why?](#))
- Capitalize a letter in the middle, rather than the first character ([Why?](#))
- Consider inserting digits into the middle, not just at the end ([Why?](#))

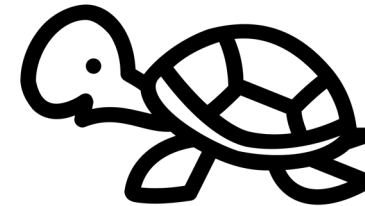
A better choice: **M456789onke>y**

[How to make strong passwords](#)

At the bottom of the form is a 'Continue' button.

What Can Users Do?

- Don't reuse passwords!
- Pick longer passwords, include symbols and numbers (and not just at the end)
- Don't use your pet turtle's name, even if you didn't tell anyone what it was
- Use a password manager to *auto-generate and store passwords*



What Can Information Security Officers Do?

- Relax rules, but weed out common passwords
- Give users feedback about their password:
cups.cs.cmu.edu/meter
- Remember that users have 100 other accounts that are just as important to them

The screenshot shows a password creation form with the following fields and elements:

- Username:** A text input field containing the text "Lujo".
- Password:** A text input field containing the text "Monkey456789". Below the input is a red progress bar indicating low strength.
- Show Password & Detailed Feedback:** A checkbox that is currently checked.
- Confirm Password:** An empty text input field.
- Continue:** A blue button located at the bottom right of the form.
- Feedback Panel (Right):**
 - Header: "Your password is very easy to guess."
 - Item 1: "Don't use dictionary words (Monkey)" with a blue square icon and a "(Why?)" link.
 - Item 2: "Capitalize a letter in the middle, rather than the first character" with a blue square icon and a "(Why?)" link.
 - Item 3: "Consider inserting digits into the middle, not just at the end" with a blue square icon and a "(Why?)" link.
 - Recommendation: "A better choice: M456789onke>y" where "M456789" is in pink and "onke>y" is in blue.
 - Link: "[How to make strong passwords](\"#\")"

What Can Usable Security Researchers Do?

- Adopt our methodology to study passwords (and other usability problems!)
- Use our password guessability service: pgs.ece.cmu.edu