

Measuring the Security and Usability of Password-Composition Policies

Lujo Bauer

Carnegie Mellon University, CyLab & ECE

Sep 13, 2011

**Joint work with Nicolas Christin, Lorrie Cranor, and
Patrick Gage Kelley, Saranga Komanduri, Julio Lopez,
Michelle L. Mazurek, Rich Shay, Tim Vidas**

Motivation

- **CMU password policy changed one year ago**
- **Led us to investigate the guidance available to administrators**

Password Policies

WIKIPEDIA



Log in / create account

From Wikipedia, the free encyclopedia

Login error

Passwords must be at least 1 character.

Password Requirements

Adhere to the following password requirements, when selecting your Andrew account password.

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.*
Note: Verify that the letters within your password do not spell a word after you remove any non-alphabetical or special characters. The system checks all of the letters of the password together. [Details...](#)

****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.

Password Policies

- Administrators need help selecting a password policy
- Passwords often used for critical security applications

Existing Guidance

- CMU password policy based on NIST guidance
- NIST guide not based on empirical evidence

NIST would like to obtain more data on the passwords users actually choose, but, where they have the data, system administrators are understandably reluctant to reveal password data to others. – [Burr 2006]



Study Objectives

- **Understand effect of password-composition policies on usability and security**
- **Evaluate methodology for quantifying password strength**

Related Work

- **Small-scale studies**
[Proctor 2002, Vu 2007]
- **User surveys without plaintext passwords**
[Inglesant 2010, Shay 2010, Zviran 1999]
- **Large-scale field studies**
[Florencio 2007 & 2010]
- **Analysis of password corpora sans user study**
[Bishop 1995, Weir 2010, Zhang 2010]

Study Design

- Large-scale online experiment
- Assign participants to conditions
- Access to plaintext passwords

Methodology

Participants:

- Created a password under a randomly assigned condition
- Took a survey
- Recalled password
- Returned two days to recall password and take additional survey for additional payment

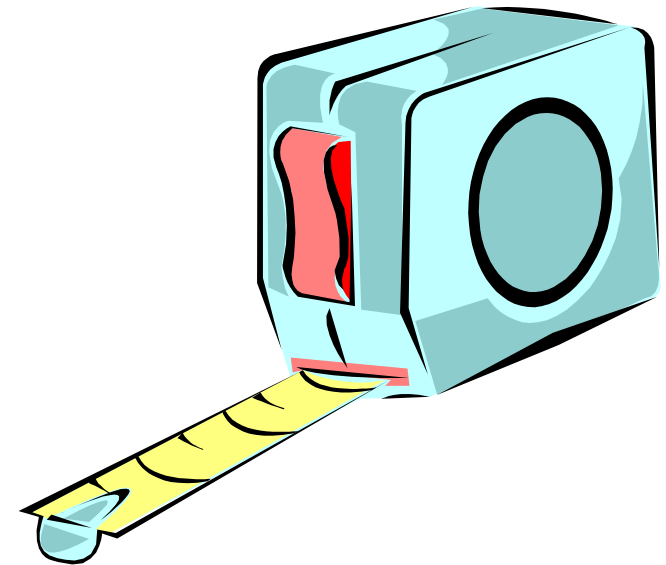
Metrics

■ Guessability

- ▼ Entropy [as described in Shay et al. 2010]
- ▼ Guessability by state-of-the-art cracking tools
- ▼ NIST estimates

■ Usability

- ▼ Creation attempts
- ▼ Recall attempts
- ▼ Reported sentiment (Likert)
- ▼ Writing down
- ▼ Study drop-out



Guessability by Cracking Tools

- Password-cracking algorithms try guesses in deterministic order
- Calculate how long it would take to crack a password, rather than trying to crack a password
- Best password-cracking algorithms use heuristics
 - ▼ Result depends on training data
 - ▼ Must try many training sets
- Hadoop to the rescue!
 - ▼ 64-node cluster
 - ▼ Experiments lasted several hours for several thousand passwords
 - ▼ 32 combinations of algorithms and training sets

Data Collection



- Used for recruitment and payment
- Enabled study of 12,000+ participants
- Email participants without collecting personally identifiable information

This study is being conducted as part of a Carnegie Mellon University research project. It is important that you answer questions honestly and completely.

Imagine that your main email service provider has been attacked, and your account became compromised. You need to create a new password for your email account, since your old password may be known by the attackers. Because of the attack, your email service provider is also changing its password rules.

Please follow the instructions below to create a new password for your email account. We will ask you to use this password in a few days to log in again so it is important that you remember your new password. Please take the steps you would normally take to remember your email password and protect this password as you normally would protect the password for your email account. Please behave as you would if this were your real password!

Password Requirements: Password must have at least 8 characters including an uppercase and lowercase letter, a symbol, and a digit. It may not contain a dictionary word.

Choose a password:

Re-enter your password:

Proceed

Should you forget your password, we can email it to your Mechanical Turk email address.

Password Requirements: Password must have at least 8 characters including an uppercase and lowercase letter, a symbol, and a digit. It may not contain a dictionary word.

Password must contain 8 or more characters

Password must contain 1 or more uppercase characters

Password must contain 1 or more numbers

Password must contain 1 or more symbols, not including the underscore: _

The letters in your password are too similar to a word or name found in our dictionary

Choose a password:

Re-enter your password:

Proceed

Survey

5. Do you have a password or set of passwords you reuse in different places? *

- Yes
- No
- I prefer not to answer

6. Do you have a password that you use for different accounts with a slight modification for each account? *

- Yes
- No
- I prefer not to answer

Click to Go Back

Click to Next Page

28%

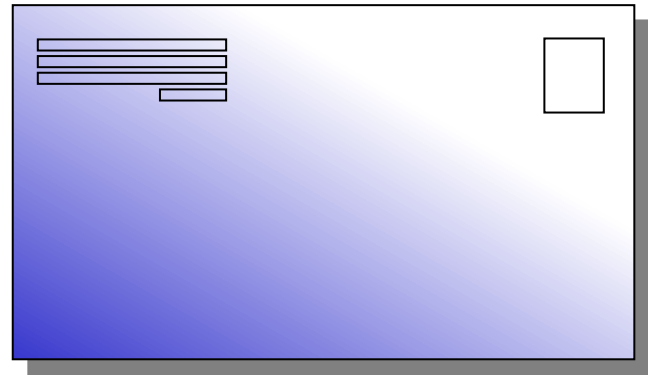
Online Surveys powered by SurveyGizmo



Take a look under the hood

Study Walkthrough

- Automatically sends return email to participants via Mechanical Turk



Please enter the password you created for this study:

Proceed

[I forgot my password](#)

Survey

Thank you for participating in this Carnegie Mellon University study. Please answer the following questions honestly. There are no right or wrong answers and everyone who finishes this task completely will receive his or her bonus payment.

1. How did you just enter your password for this study (please be honest, you get paid regardless, this will help our research)? *

- I typed it in from memory
- It was automatically filled in
- I use a password manager that filled it in for me
- I cut and pasted it from a text file
- It was stored in my browser
- I forgot my password and followed the password reset link
- I prefer not to answer
- I looked it up in the place I had recorded it earlier and then I typed it in

Other



password

NIST estimate: 18 bits

Condition: Dictionary8

password

NIST estimate: 24 bits

Passwrod1!

NIST estimate: 30 bits

Condition: Basic16

passwordpassword

NIST estimate: 30 bits

Three Blacklist Conditions

- **Only requirement is that candidate password is not on a blacklist**
- **Blacklists:**
 - ▼ Easy: Unix dictionary
 - ▼ Medium: ~40M entry cracking wordlist
 - ▼ Hard: 5B entry wordlist created by cracking algorithm

Participants

- **12,000 participants**
 - ▼ 1,000 per condition + extra 2,000 for some conditions

Results Outline

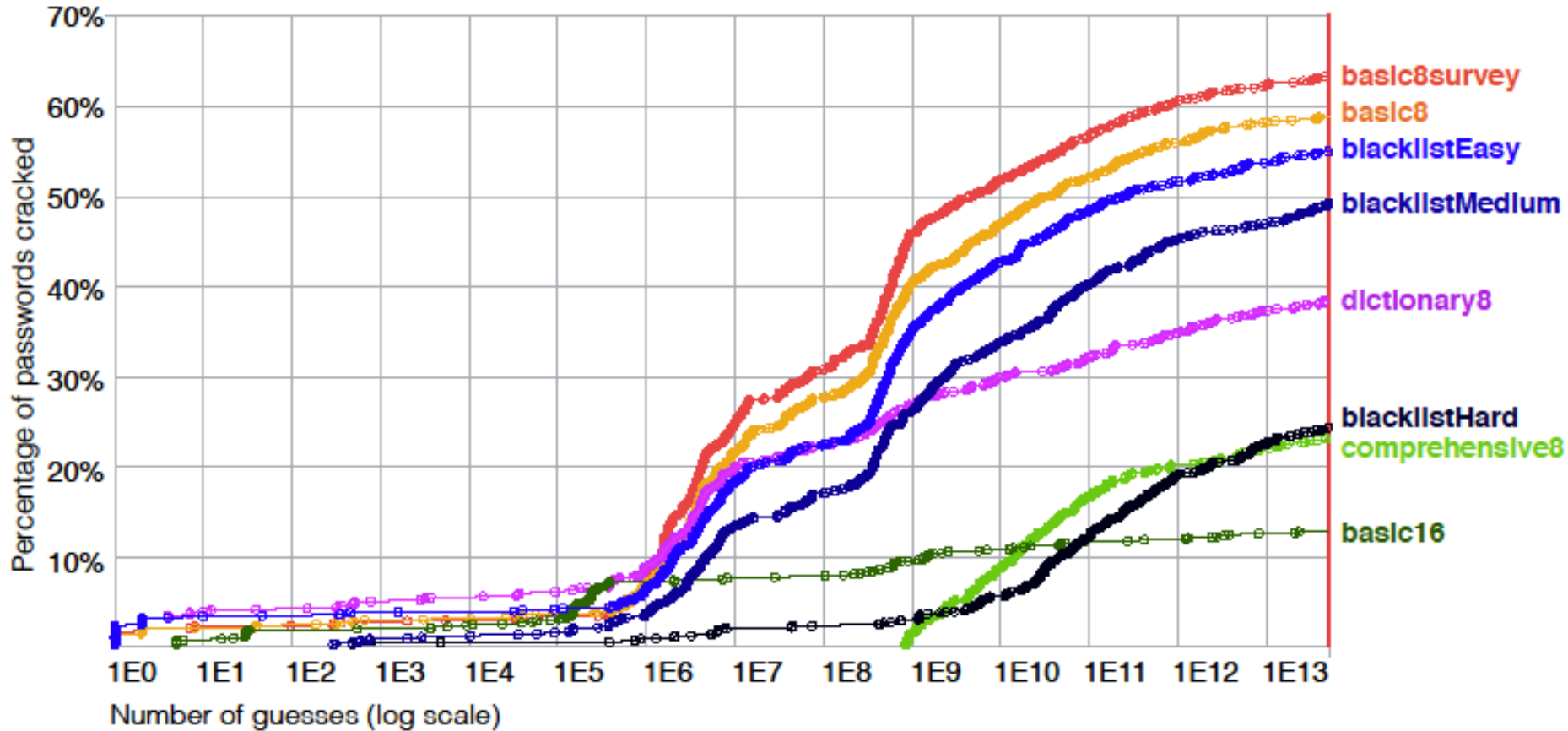
■ Results about password-composition policies

- ▼ Basic16 vs Comprehensive8
- ▼ Password components

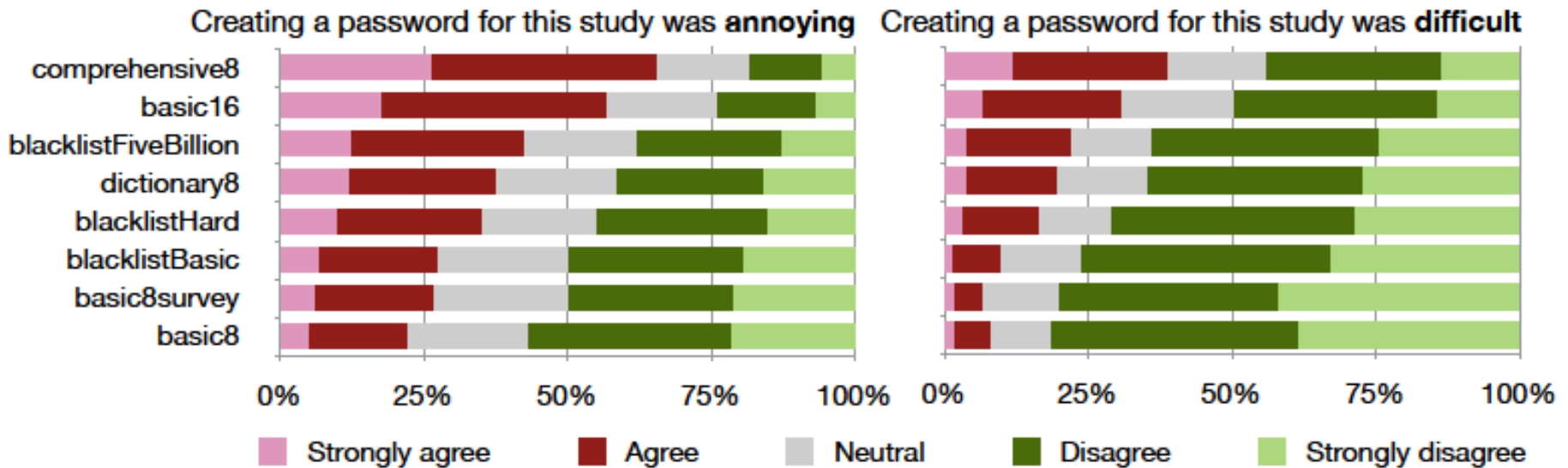
■ Results about methodology

- ▼ Password-composition scenario
- ▼ Effect of specialized training data
- ▼ Choosing test sets
- ▼ Metrics for measuring or estimating password security

Measuring Guessability



Measuring Usability



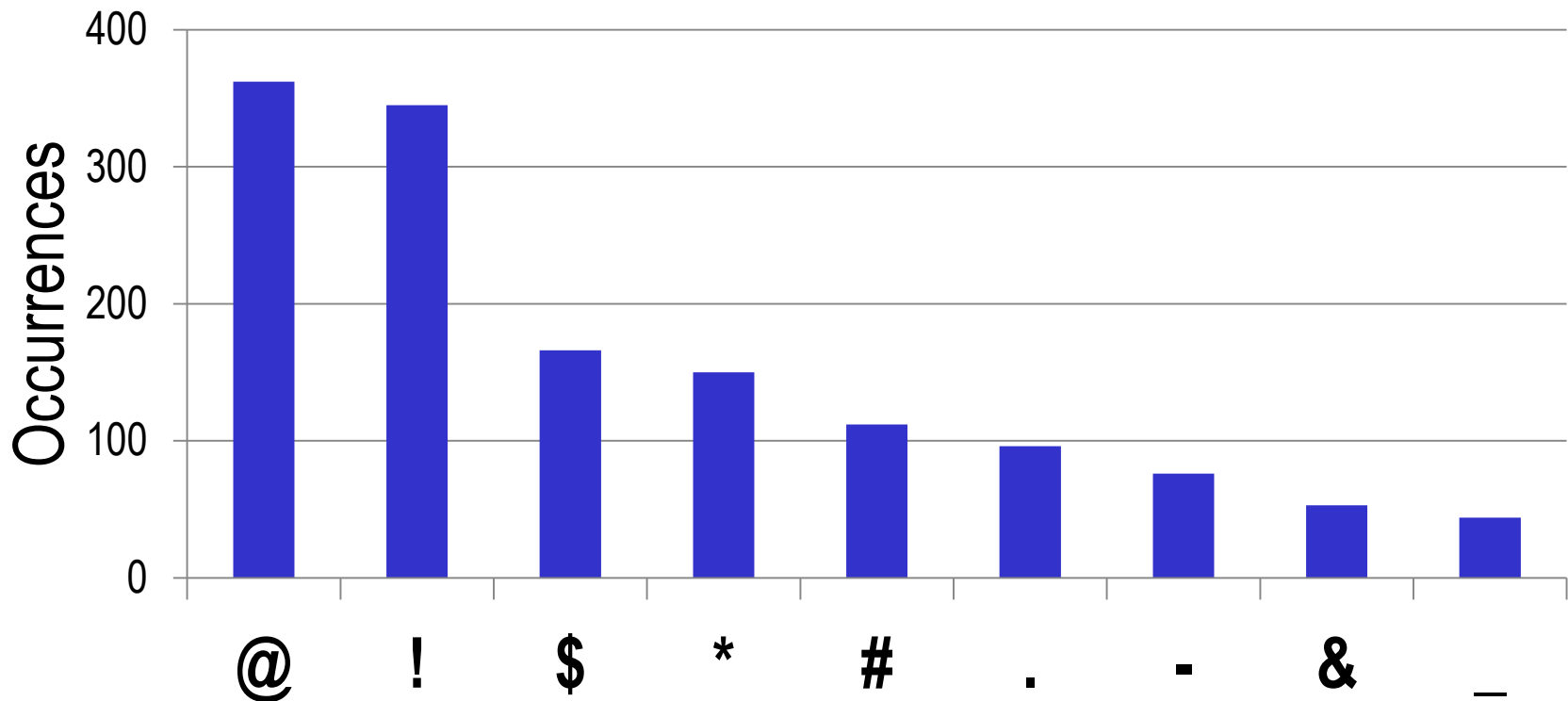
Basic16 vs Comprehensive8

- **Basic16 requires significantly fewer attempts in password creation**
 - ▼ 53% vs 18% success on first attempt, $p < 0.001$
 - ▼ 1.66 vs 3.35 attempts total, $p < 0.001$

Entropy of Password Components

■ Symbols don't contribute much

▼ Consistent with NIST prediction



Entropy of Password Components

- **Symbols don't contribute much**
 - ▼ Consistent with NIST prediction
- **Digits are used when not required**
 - ▼ Does not match NIST prediction

Entropy of Password Components

- **Symbols don't contribute much**
 - ▼ Consistent with NIST prediction
- **Digits are used when not required**
 - ▼ Does not match NIST prediction
- **Future work – Testing individual requirements**

Results Outline

■ Results about password-composition policies

- ▼ Basic16 vs Comprehensive8
- ▼ Password components

■ Results about methodology

- ▼ Password-composition scenario
- ▼ Effect of specialized training data
- ▼ Choosing test sets
- ▼ Metrics for measuring or estimating password security

Experiment Scenarios

■ Basic8 Survey condition

- ▼ Participant told password just used for taking surveys

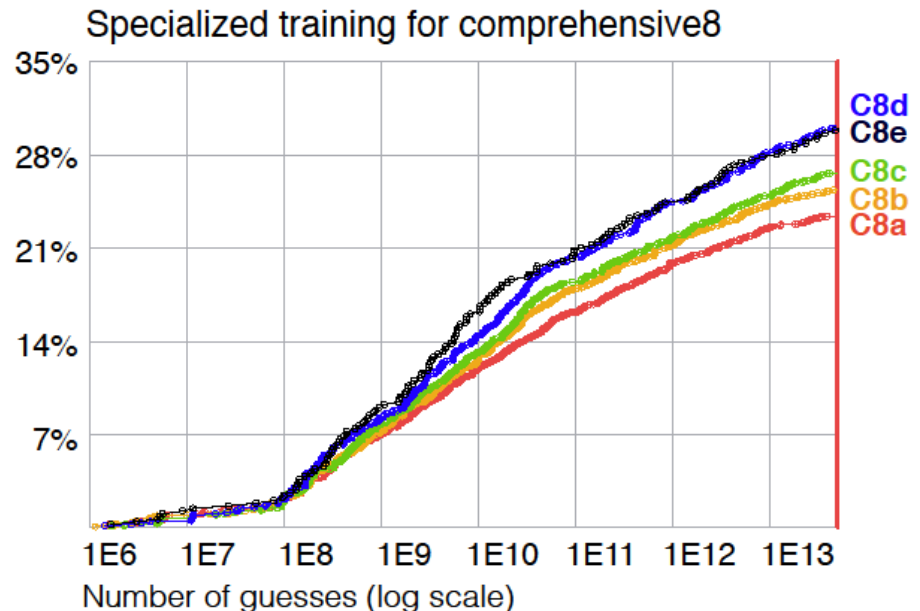
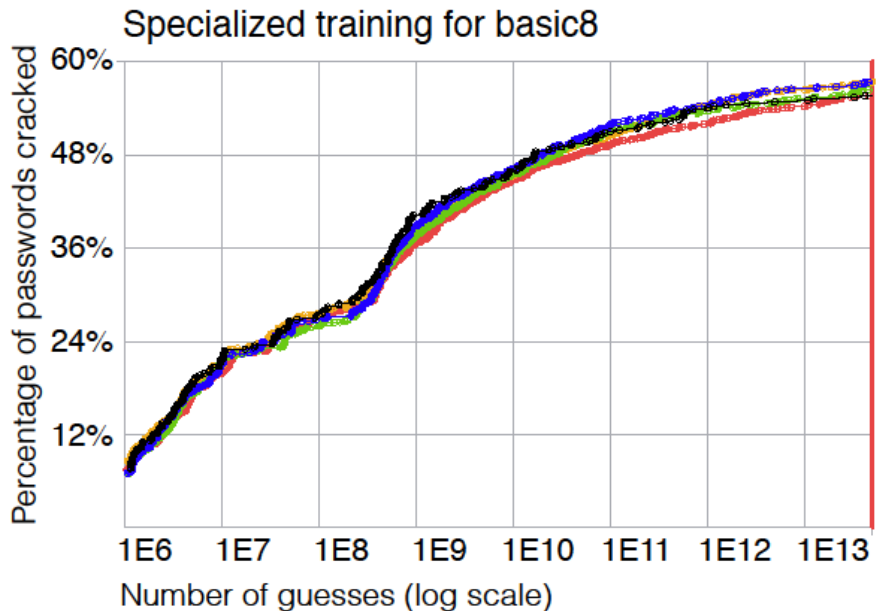
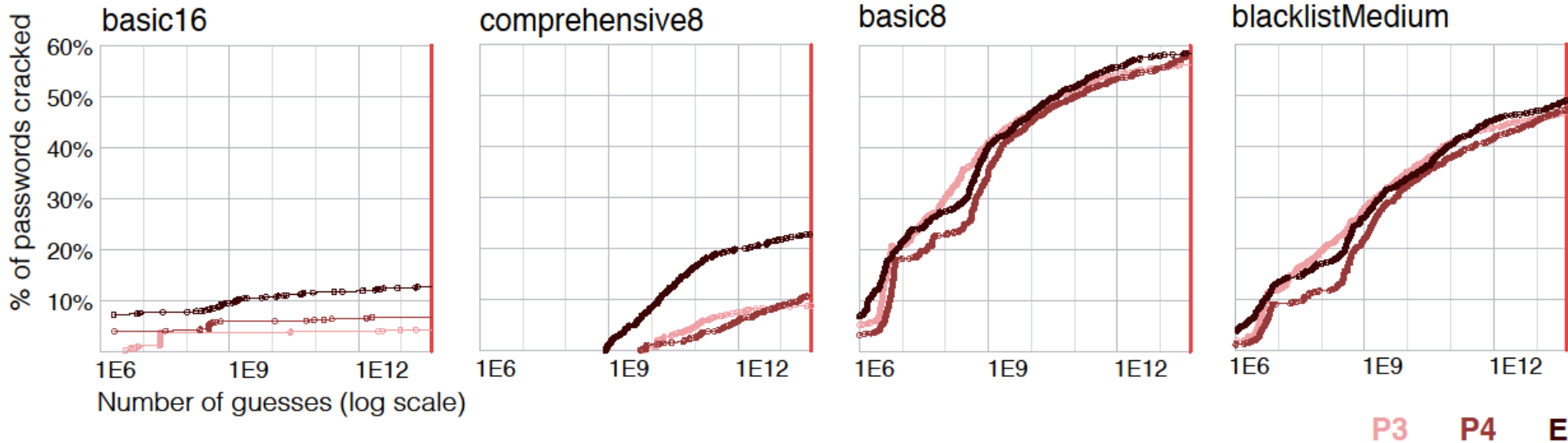
■ Basic8 Email condition

- ▼ Participant asked to imagine their primary email was compromised

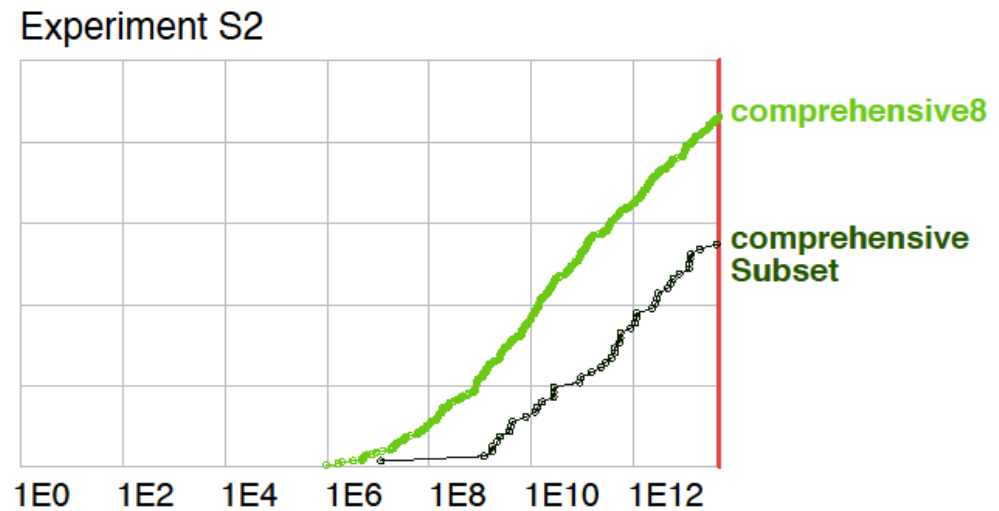
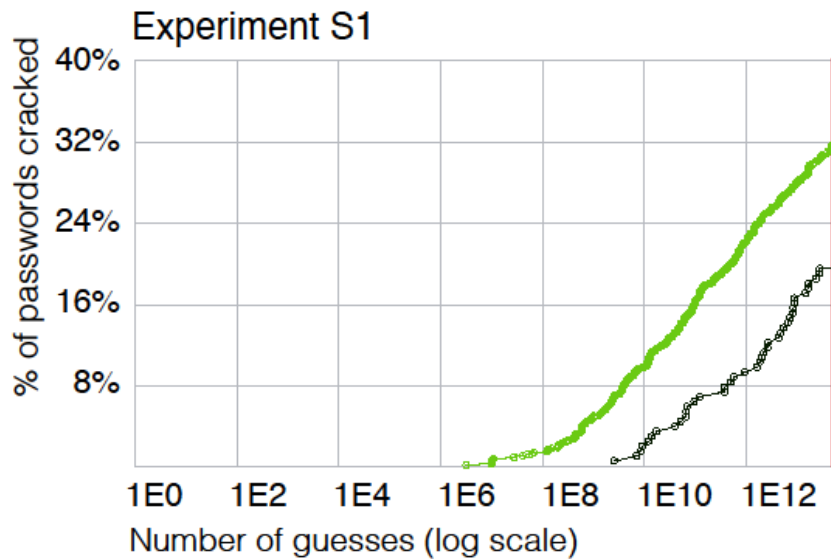
Survey vs Email Scenario

- **Basic8 (survey) has significantly less entropy than Basic8 (email), $p < 0.001$**
 - ▼ Difference of 2.2 bits
 - ▼ Differs only in scenario
 - ▼ Not accounted for in NIST guidelines

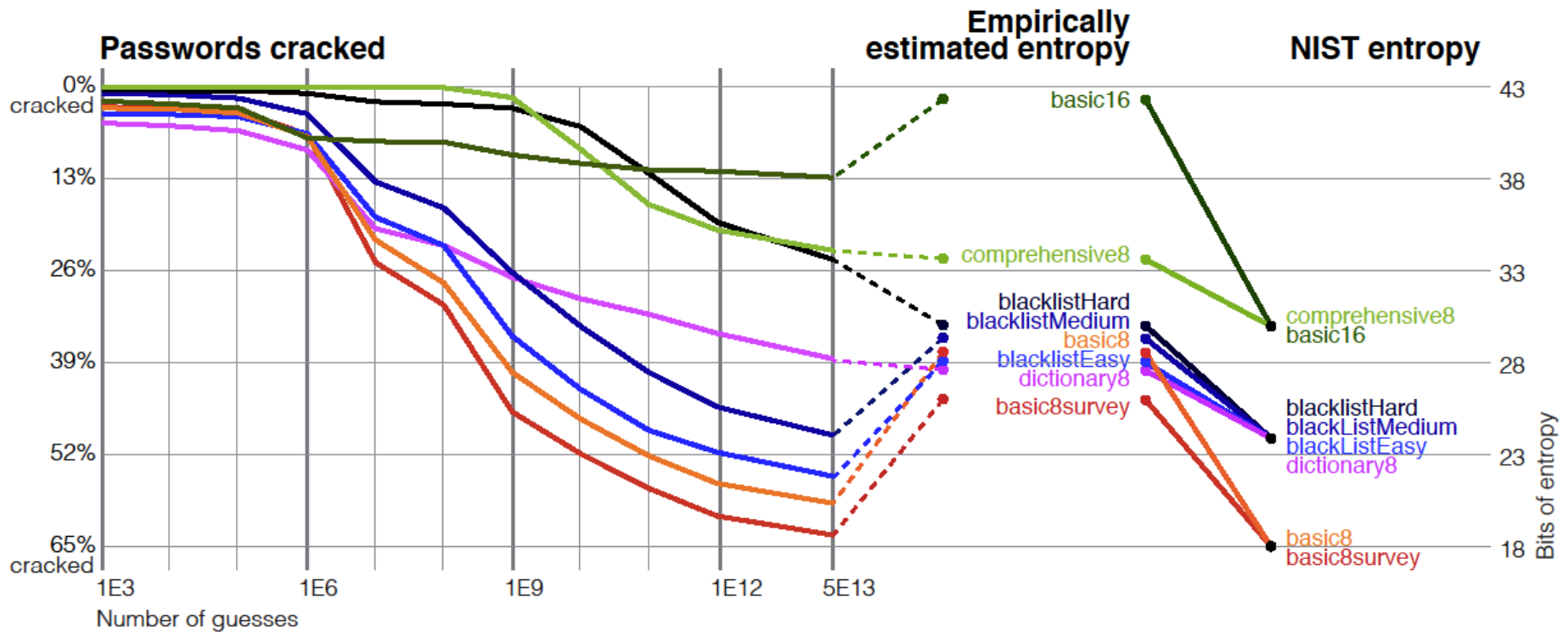
Increasing Training Data



Choosing the Right Test Data



Comparing Metrics



Conclusion

- Large-scale, 12,000 participants study
- Randomized experiment on password policies
- Condition based on length more secure and usable than character requirements
- Digits add more entropy than symbols
- Password creation context can affect strength
- Entropy estimates poor at quantifying guessability
- Significant effects of choice of training and testing data