13 - Passwords

Lujo Bauer, Nicolas Christin, and Abby Marsh

February 24, 2016

05-436 / 05-836 / 08-534 / 08-734 / 19-534 / 19-734
Usable Privacy and Security

Carnegie Mellon University
CyLab

institute for SOFTWARE RESEARCH

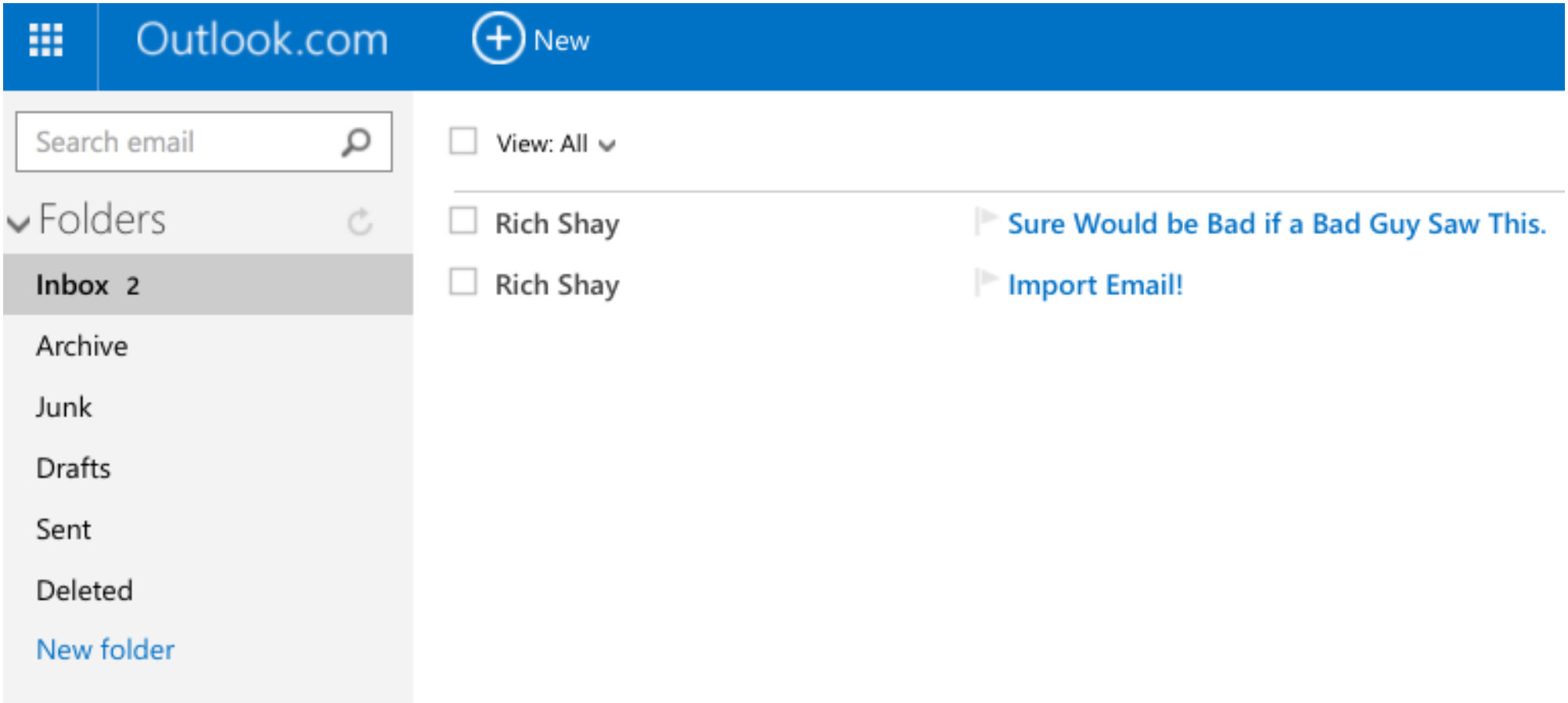
Engineering & Public Policy

Today's class

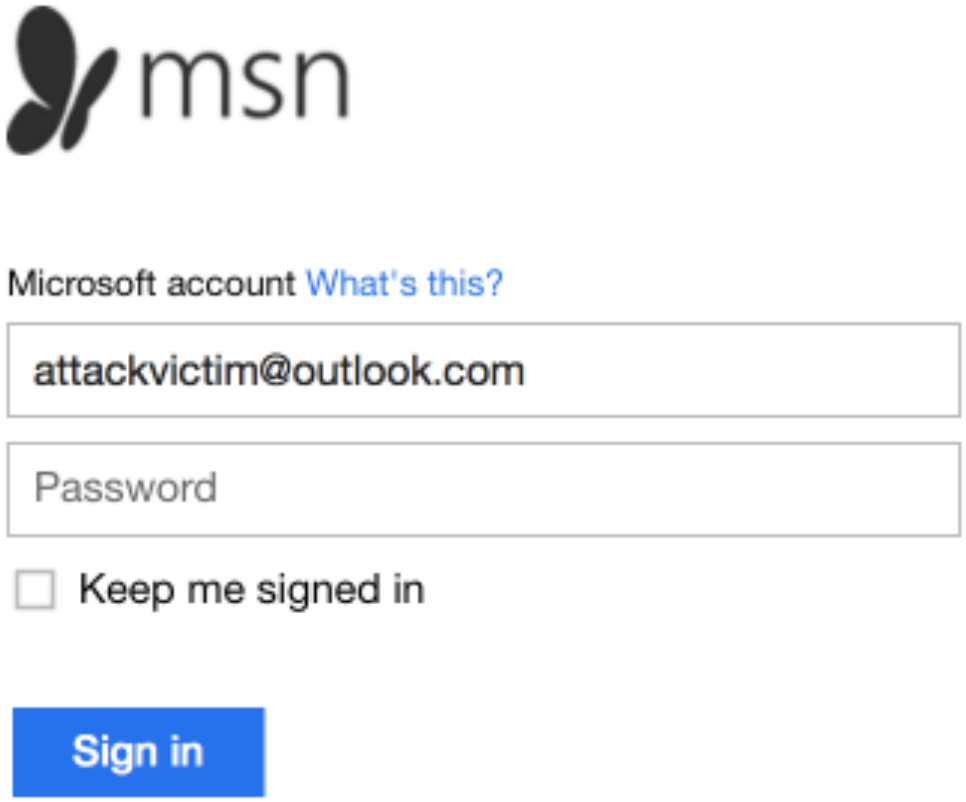
- Password Creation and Use
- Threats to Passwords
- Password Policies
- Presentation of a Password Study

Password Creation and Use

Online Accounts



Passwords


msn
Microsoft account What's this?
attackvictim@outlook.com
Password
Keep me signed in
Sign in

Password Creation

User

Service Provider

`Password!1`

Password Creation

`Password!1`

`Password!1`

Password Creation

User

Service Provider

`Password!1` 

h(`Password!1`**)**

Password Creation

Password!1 →

h(Password!1**)**

7e8d6b2fe300

Password Creation

`Password!1` → `7e8d6b2fe300`

h(`Password!1`**)**

`7e8d6b2fe300`

Authentication

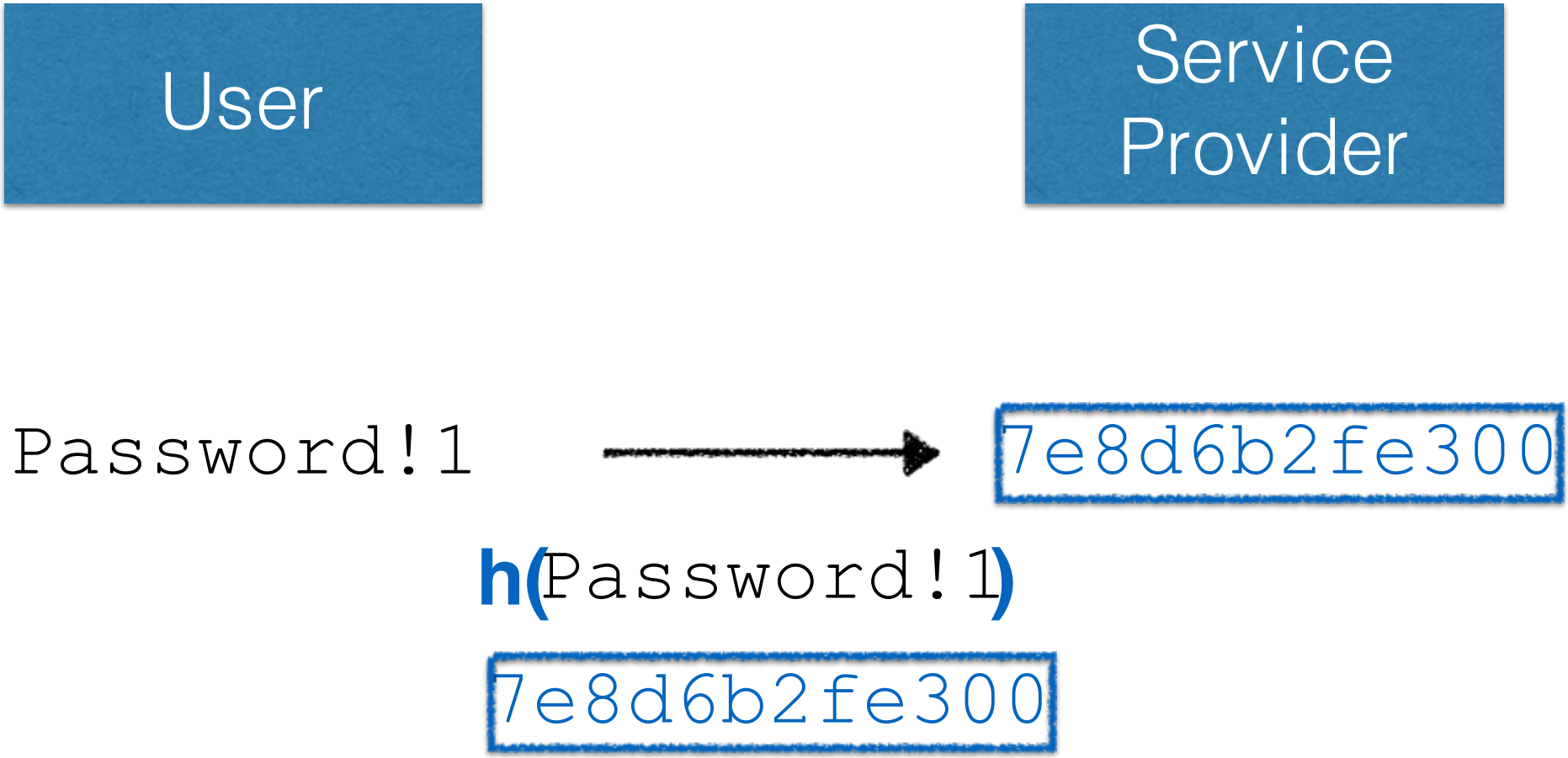
Authentication

`Password!1` → `7e8d6b2fe300`

h(`Password!1`**)**

`7e8d6b2fe300`

Authentication



Password Threats

Password Threats that Ignore Strength

- Phishing
- Key logging
- Government coercion
- Writing your password down on a sticky note

Password Threats that Ignore Strength

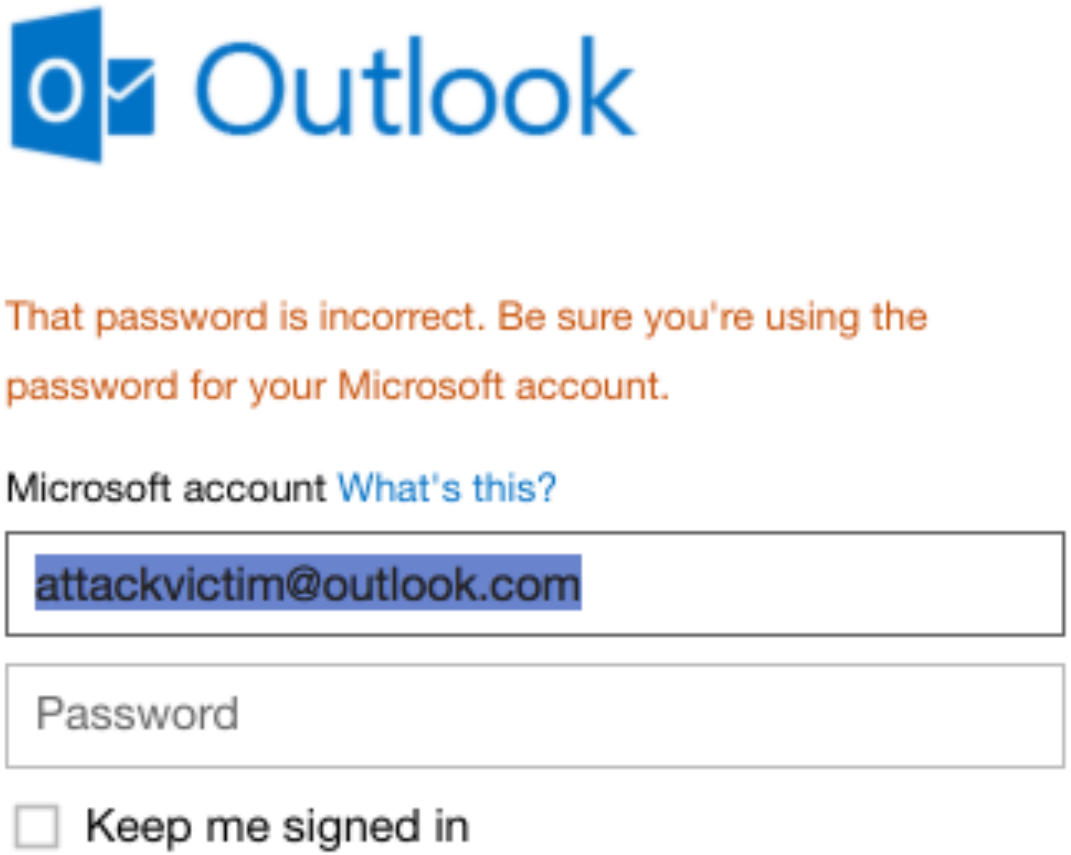
- Phishing
- Key logging
- Government coercion
- Writing your password down on a sticky note

- *Some* of these can be addressed via training.

Many Threats Do Not Ignore Strength

- Password guessing is easier for some passwords than others

Online Attack



Online Attack

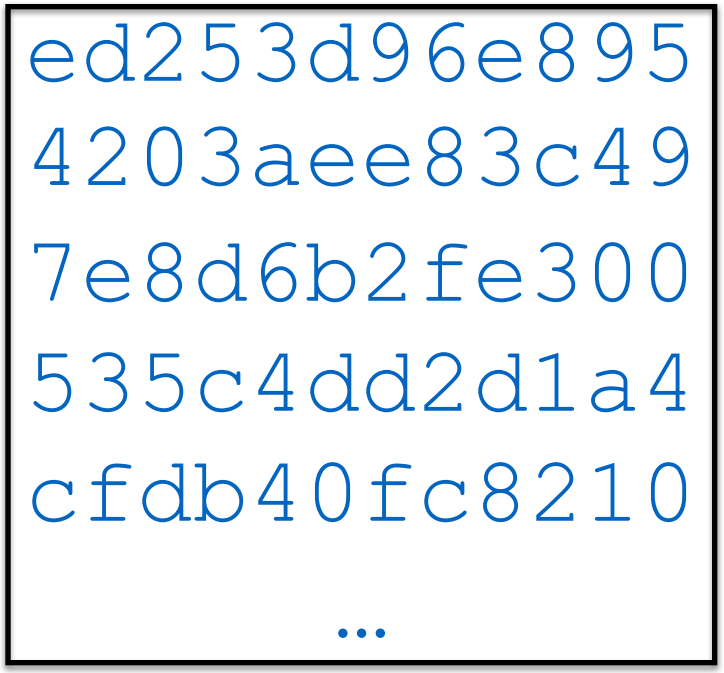
Sign-in is blocked

Sign-in with **attackvictim@outlook.com** is blocked for one of these reasons:

Someone entered the wrong password too many times.

Offline Attack

Service Provider



Password File

Offline Attack

Service Provider

```
ed253d96e895
4203aee83c49
7e8d6b2fe300
535c4dd2d1a4
cfdb40fc8210
...
```

Attacker

```
ed253d96e895
4203aee83c49
7e8d6b2fe300
535c4dd2d1a4
cfdb40fc8210
...
```

Offline Attack

2013 Examples

Company	Victims
Adobe	2.9 million
Evernote	50 million
Twitter	250,000
Living Social	50 million

Offline Attack

guess

h(guess **)**

41420474 31f5 ≠

Attacker

ed253d96e895
4203aee83c49
7e8d6b2fe300
535c4dd2d1a4
cfdb40fc8210
…

Offline Attack

guess2

h(guess2 **)**

5ac005ee92e8 ≠

Attacker

ed253d96e895
4203aee83c49
7e8d6b2fe300
535c4dd2d1a4
cfdb40fc8210
...

Offline Attack

Password!1

h(Password!1**)**

7e8d6b2fe300 **=**

Attacker

ed253d96e895
4203aee83c49
7e8d6b2fe300
535c4dd2d1a4
cfdb40fc8210
…

Password Policy

Passwords must have at least 8 characters and contain at least two of the following: uppercase letters, lowercase letters, numbers, and symbols.

New password

••••••••

8-character minimum; case sensitive

Reenter password

••••••••

Password Policies

Password Requirements

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

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 Requirements

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

Must Contain

- At least 8-characters.

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 Requirements

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

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., ~!@#$%^&*()_-+=).

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 Requirements

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

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., ~!@#$%^&*()_-+=).

remove any non-alphabetical or special characters. The system checks all of the letters of the password together. Details...

- A word that is found in a standard dictionary.

Additional Policies

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

Can Long Passwords Be Secure and Usable?

Richard Shay, Saranga Komanduri, Adam L. Durity,
Phillip (Seyoung) Huh, Michelle L. Mazurek,
Sean M. Segreti, Blase Ur, Lujo Bauer, Nicolas Christin,
and Lorrie Faith Cranor

Carnegie Mellon University

Prior: CHI 2011, Oakland 2012

- Examined policies including comp8, a typical strong policy
- Examined one "longer" policy, basic16
- Longer, simple passwords fairly usable and strong after many guesses
  - But some very easily guessed

Study Objective

- Investigate password policies that
  - Take advantage of length
  - Are not too complicated
  - Prevent easily guessable passwords

Question: Metrics

- What metrics should we look at for meeting our objectives?

Strength Metrics

- Percent of passwords guessed after 10e6 & 10e12 guesses

Usability Metrics

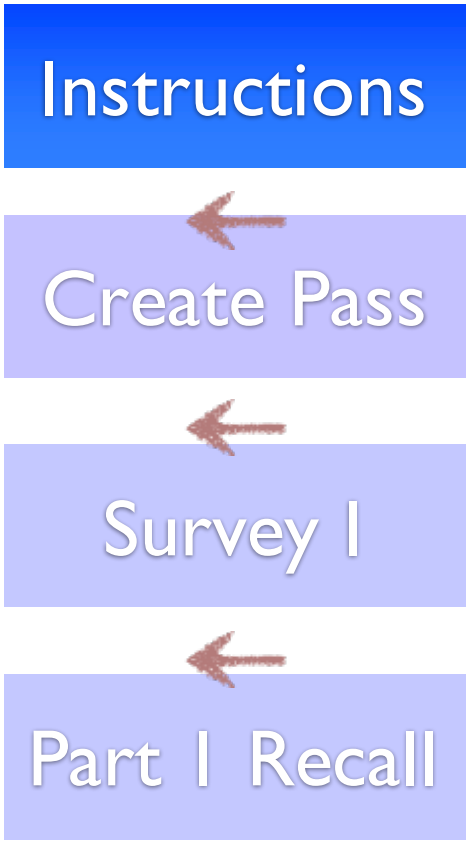
- Sentiment
  - Creation difficulty, recall difficulty
- Time
  - Password creation and recall
- Memorability
  - Recall attempts, password writedown

Study Overview

- Two-part Mechanical Turk study
- Compensation:
  55 cents for part-one, 70 for part-two
- 8,143 participants finished both

Study walkthrough

Study walkthrough



"Imagine that your main email service provider has been attacked. You need to use a new password for your email account, since your old password may be known by the attackers."

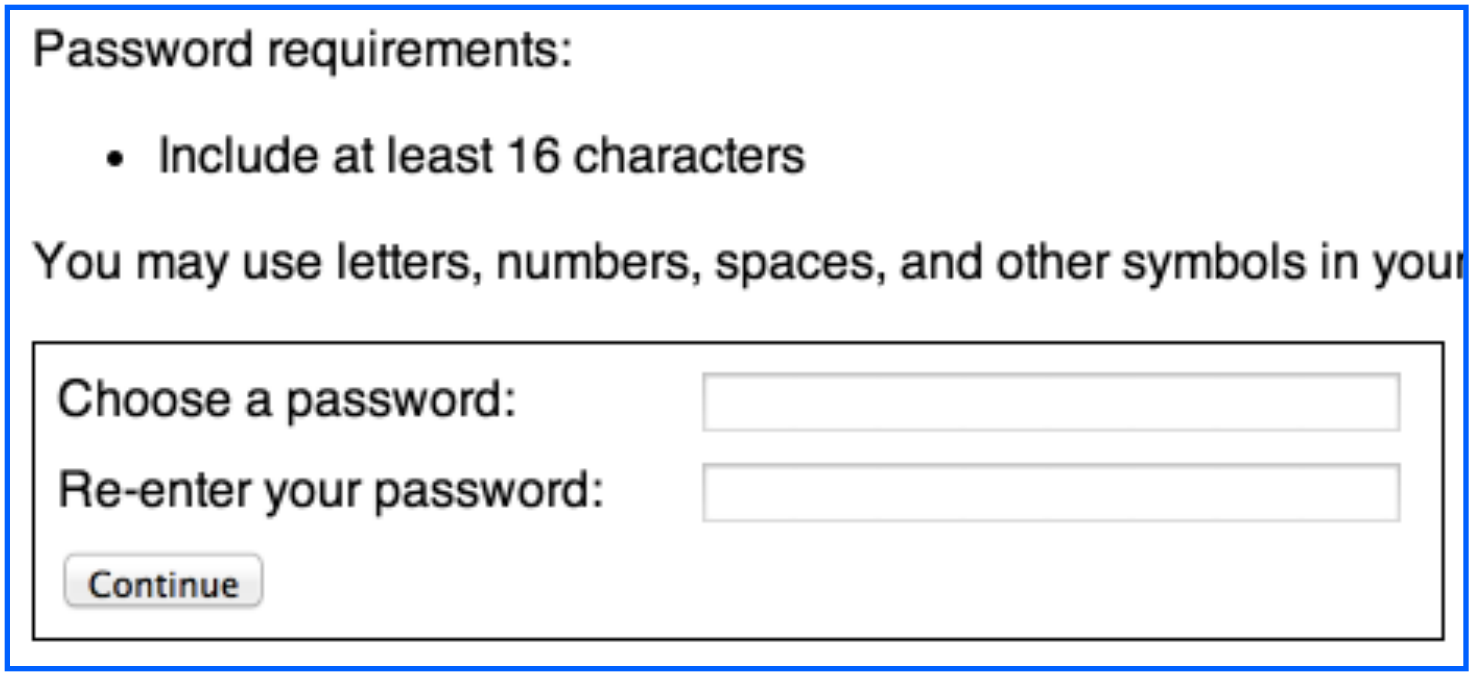
Study walkthrough

Instructions

Create Pass

Survey 1

Part 1 Recall



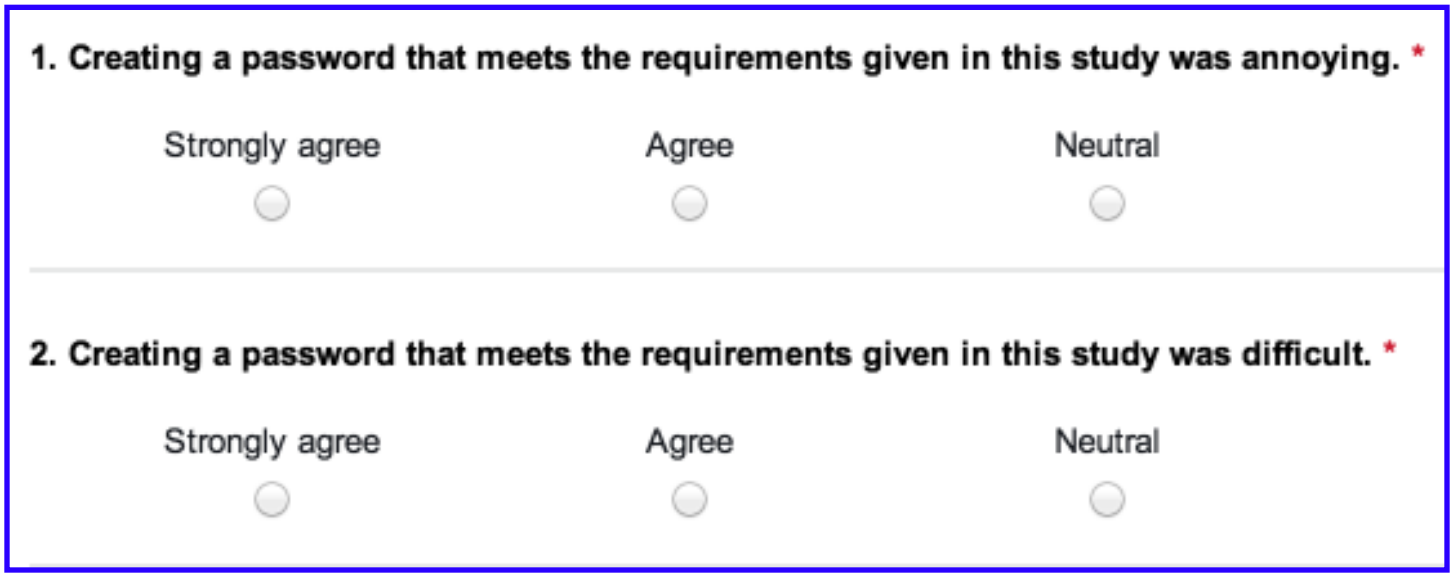
Study walkthrough

Instructions

Create Pass

Survey 1

Part 1 Recall



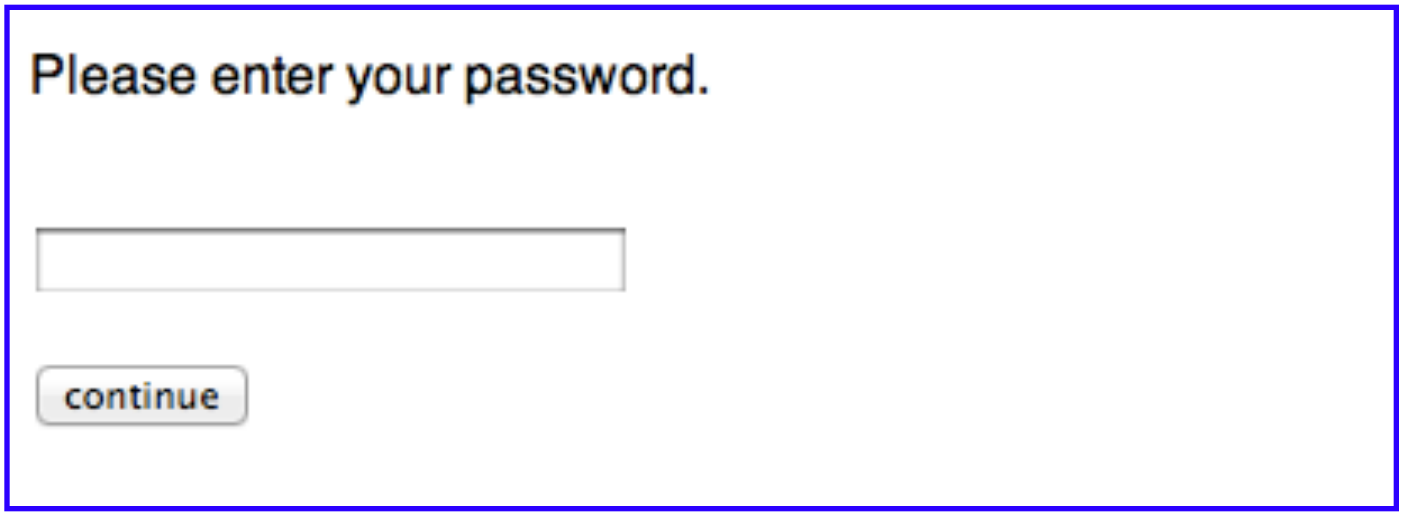
Study walkthrough

Instructions

Create Pass

Survey 1

Part 1 Recall



Study walkthrough

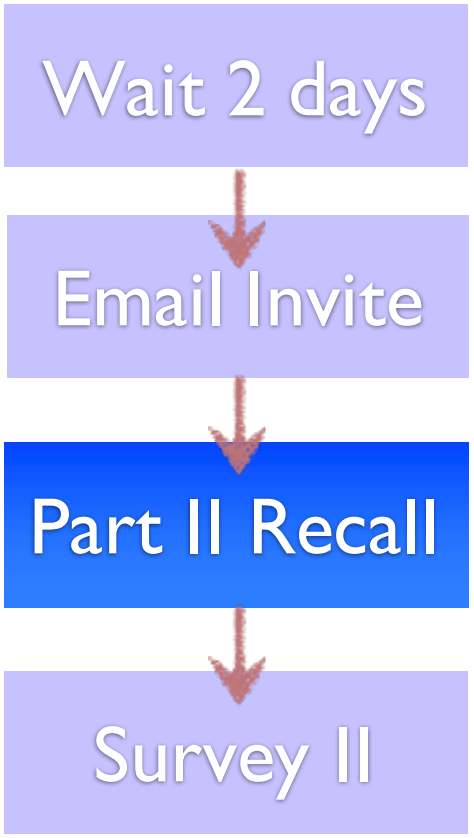
Wait 2 days

Email Invite

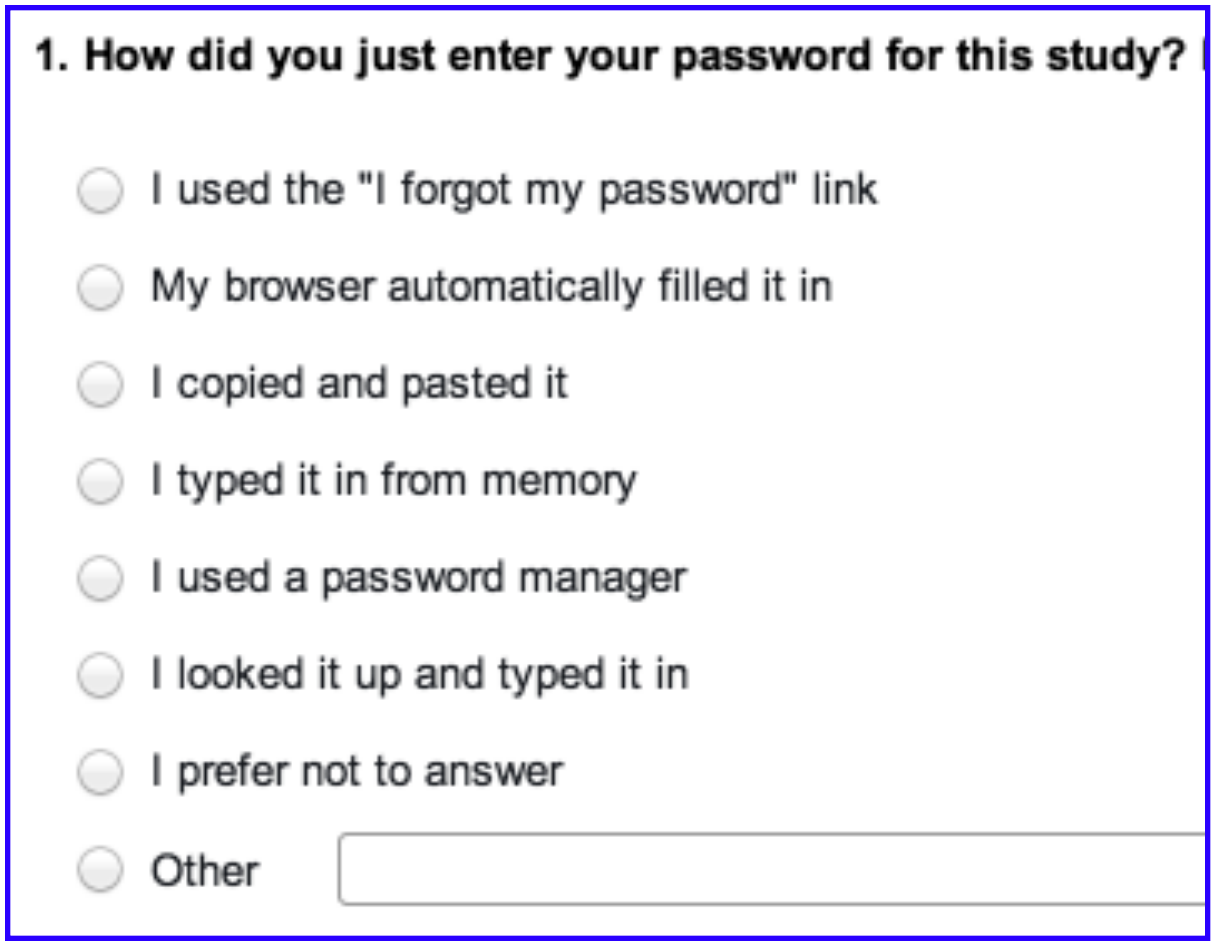
Part II Recall

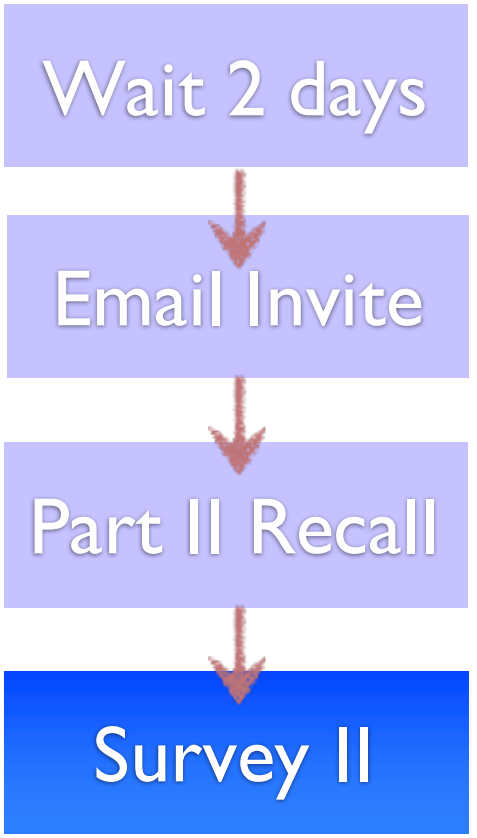
Survey II

Study walkthrough



Study walkthrough





Conditions

- 8 conditions
  - each with a different password policy
- Between subjects, assigned round-robin

comp8

- Based on the CMU policy
- Represents typical strong password policy
- 8 characters
- Letters can't form dictionary word
- Uppercase, lowercase, digit, symbol

AWordPass1!
1!WordWordWord

basic12, basic16, basic20

- Require 12, 16, 20 characters
- Study length as the only requirement for strength
- Prior work has examined basic16

passwords
passwordpassword
password passwordpass

3class12, 3class16

- Study both length and class requirement
- 12, 16 characters
- 3 of uppercase, lowercase, digit, symbol

`CMUpassword1`
`passCMUpassword1`

2word12, 2word16

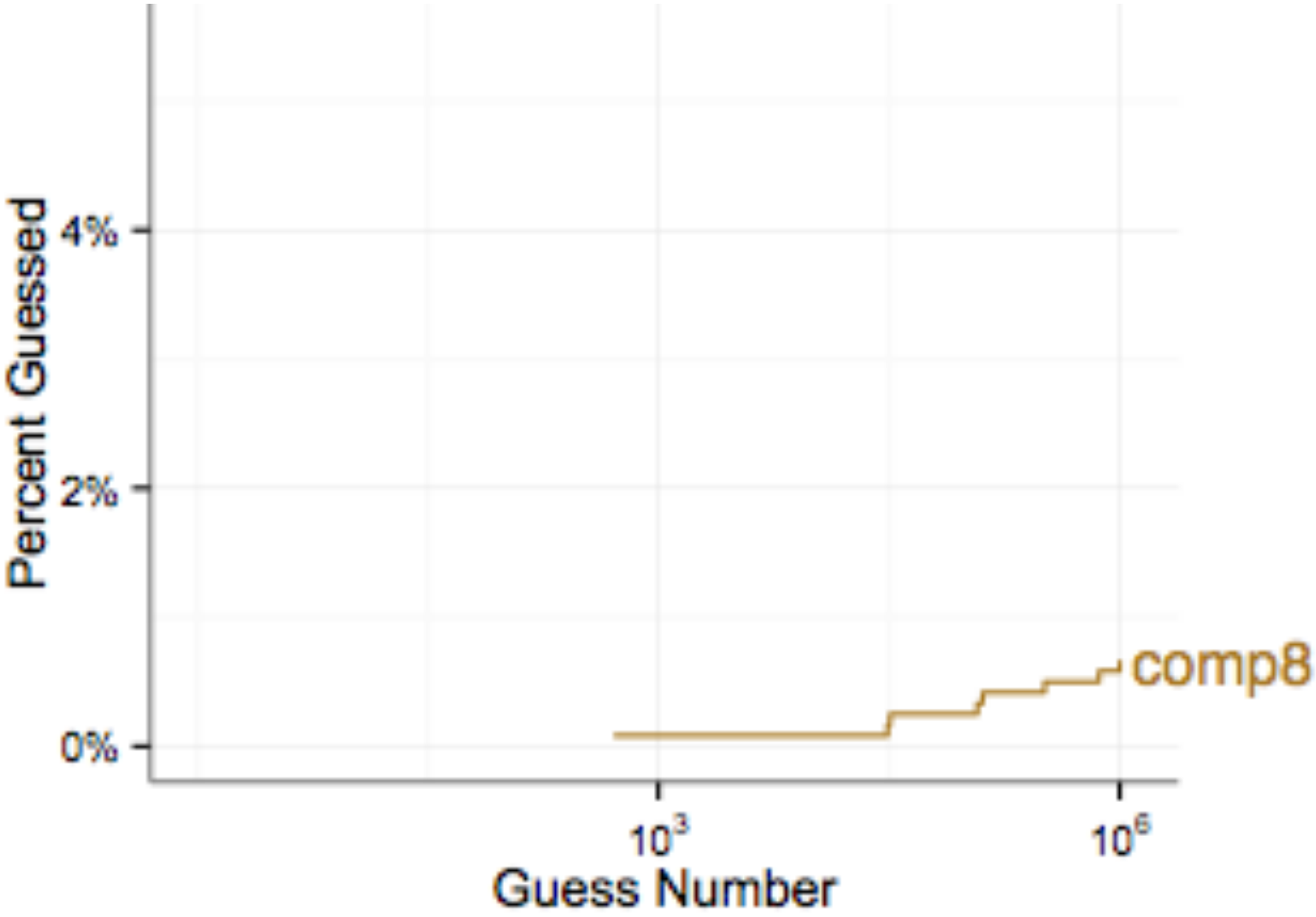
- Encourage a passphrase
- 12, 16 characters
- Letters separated by a non-letter

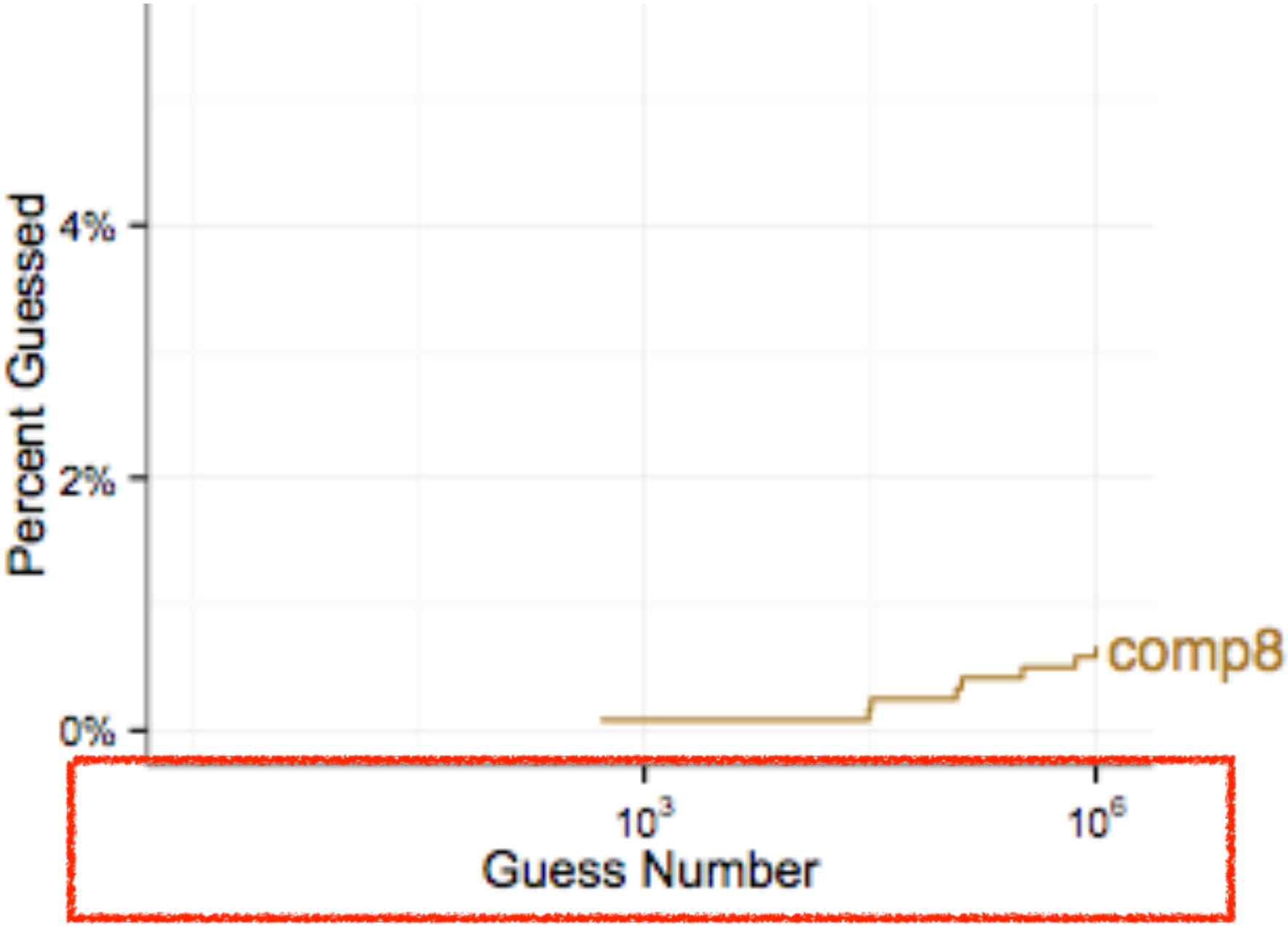
password@cmu
password@cmupass

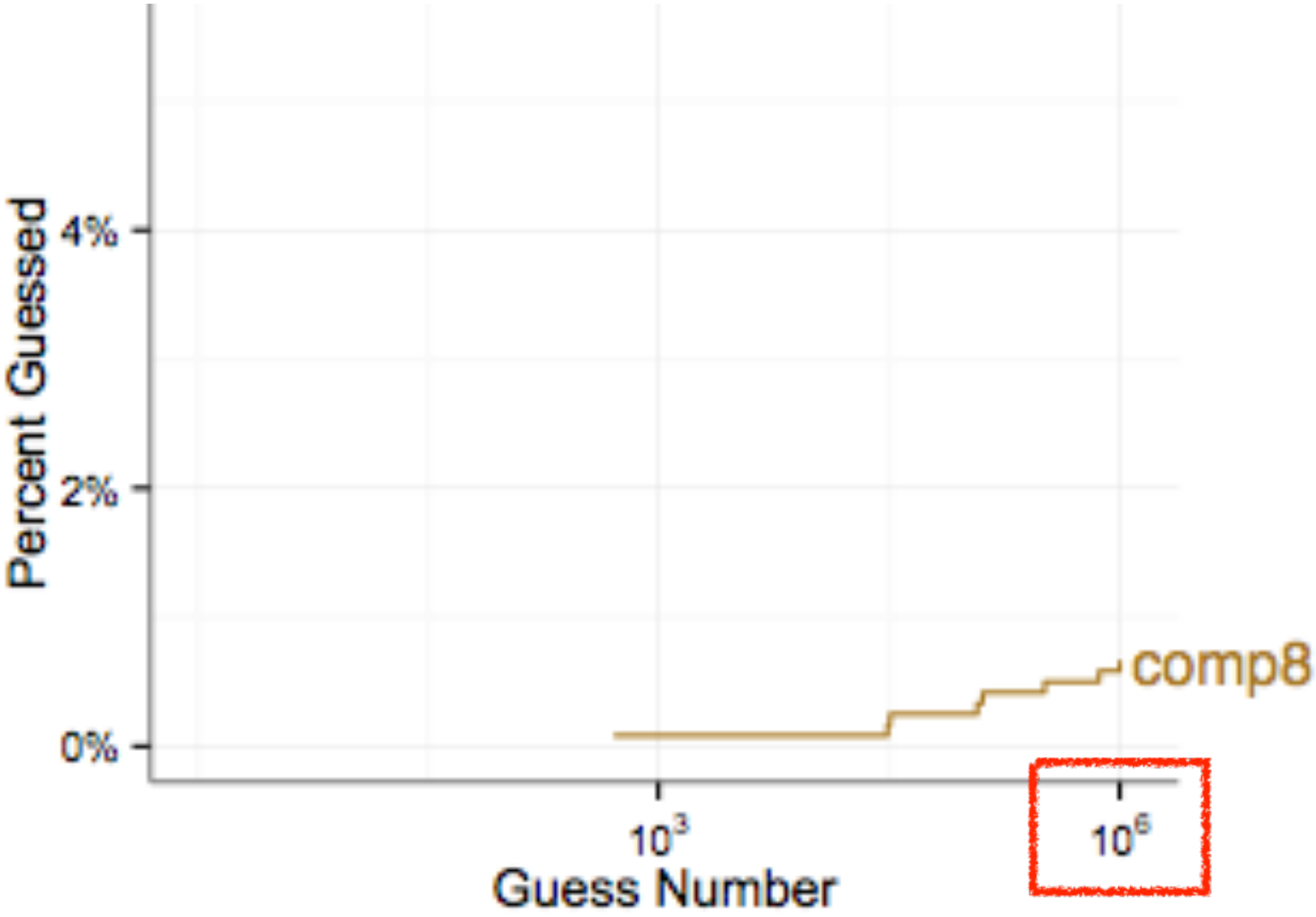
Results: Security

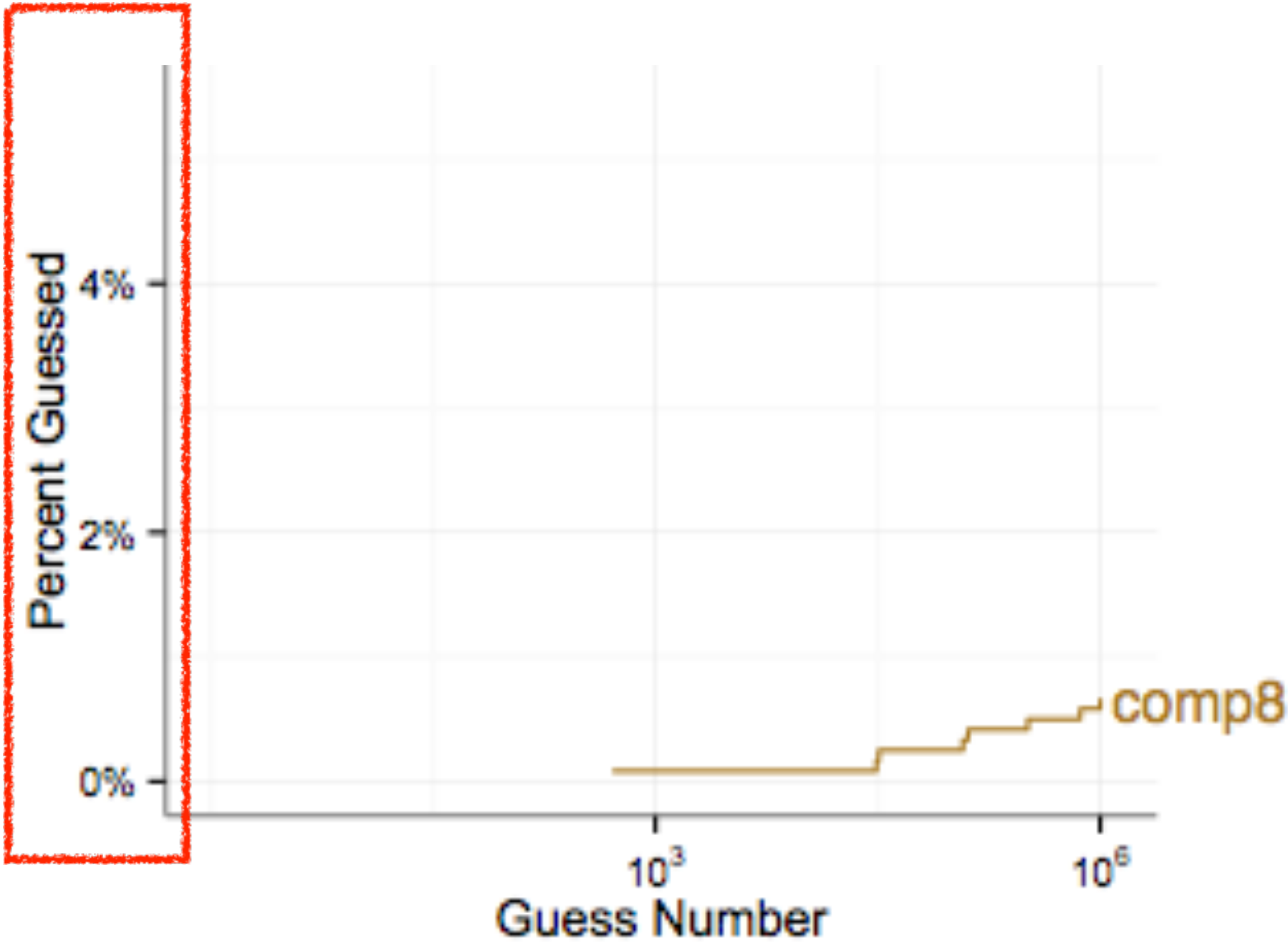
Password Strength

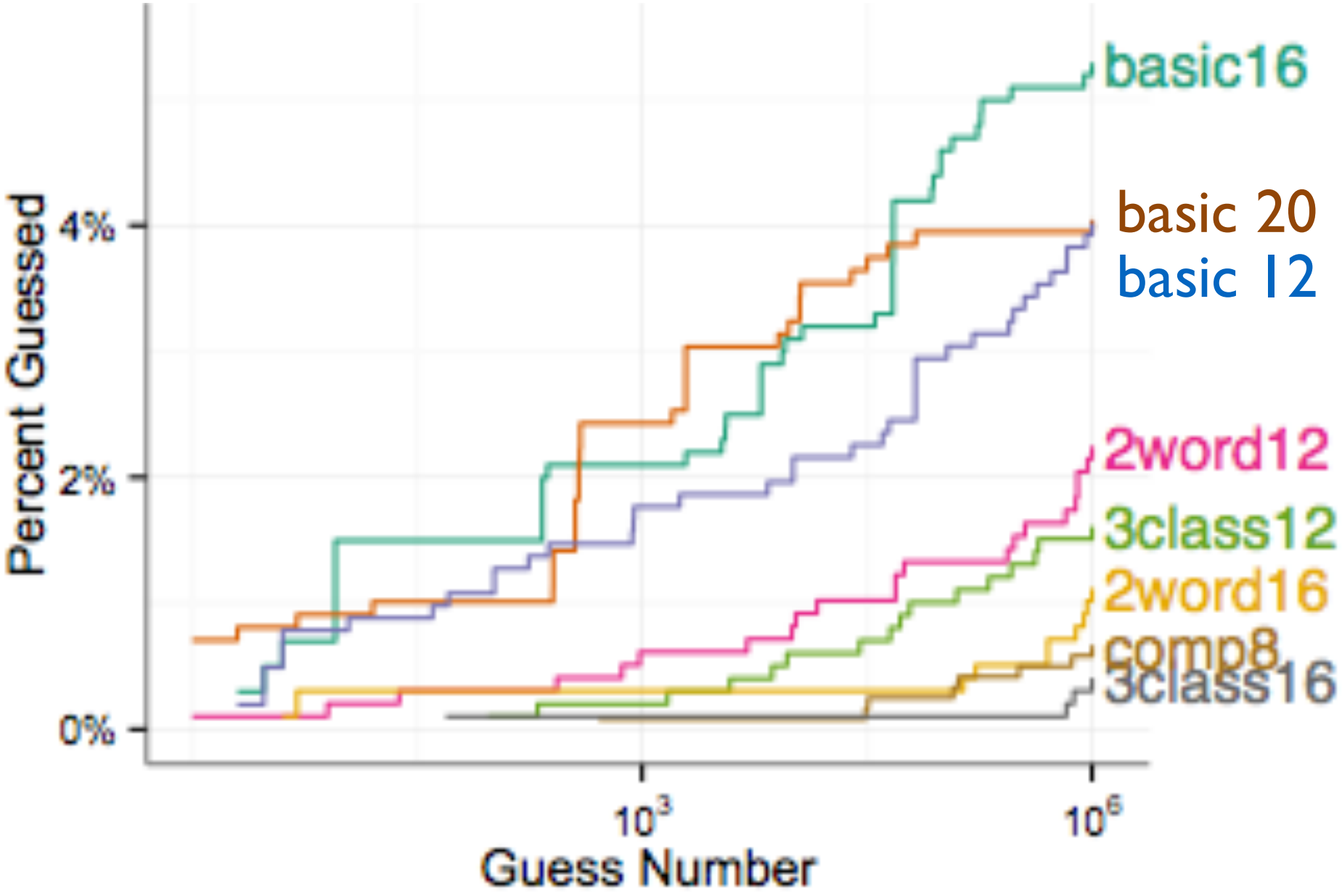
- Generated guess number for each password, up to a cutoff (Kelley et al. Oakland 2012)
- Used a context-free-grammar based cracker (Weir et al. IEEE SP 2009) tuned per condition
- Results presented as percent guessed by log number of guesses

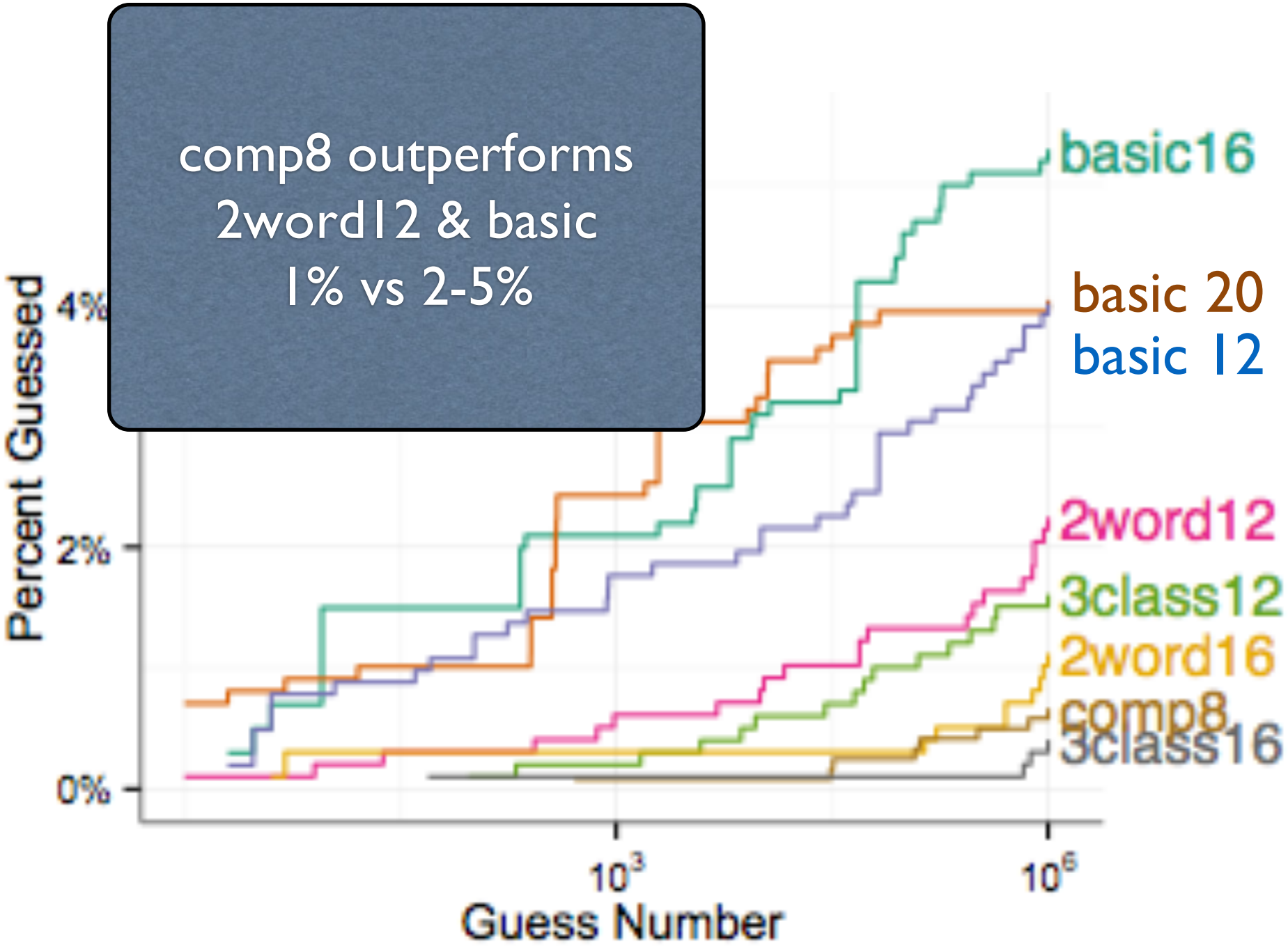

Percent Guessed
4%
2%
0%
comp8
10^3
10^6
Guess Number

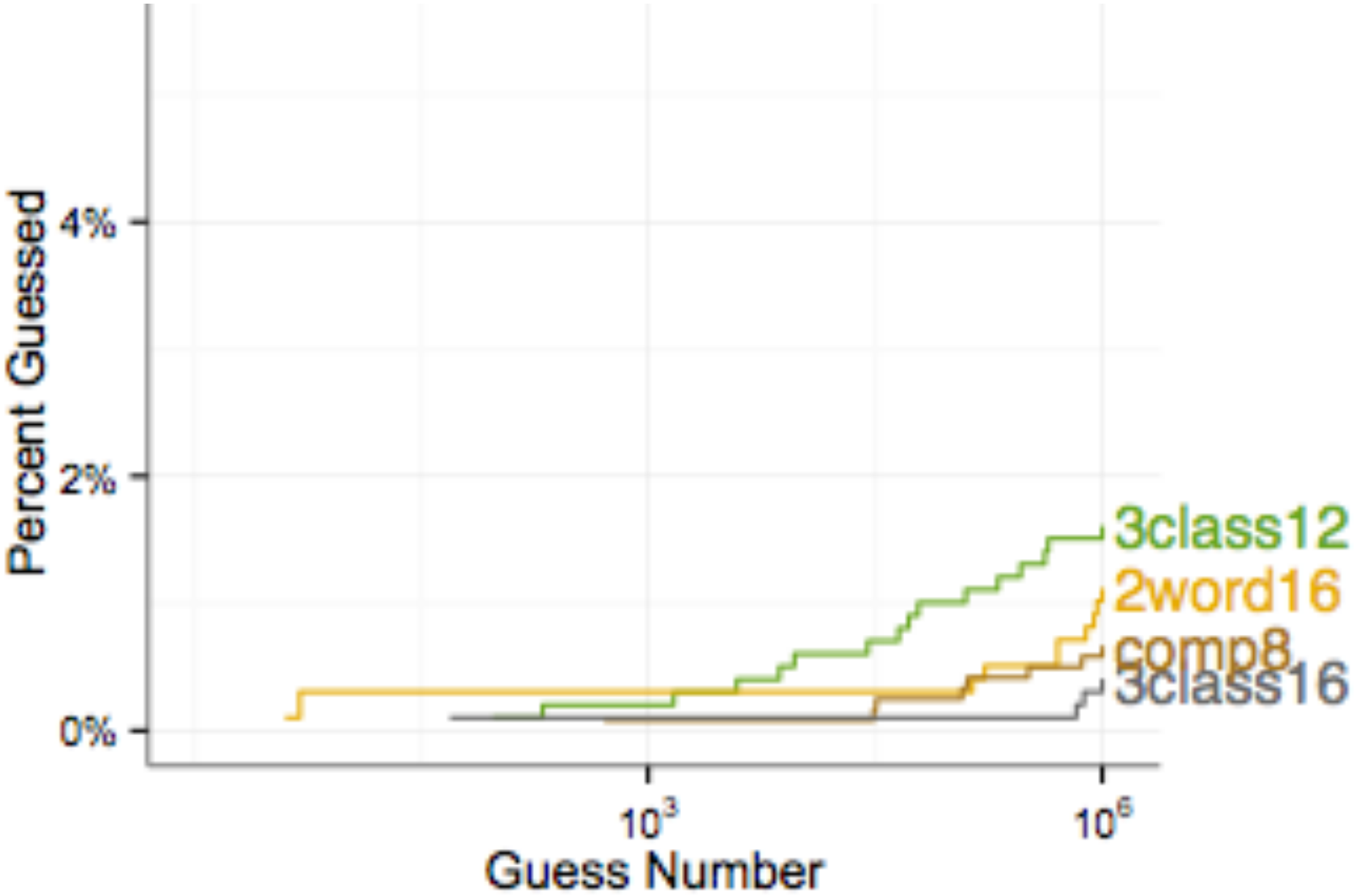

Percent Guessed
4%
2%
0%
comp8
10^3
10^6
Guess Number

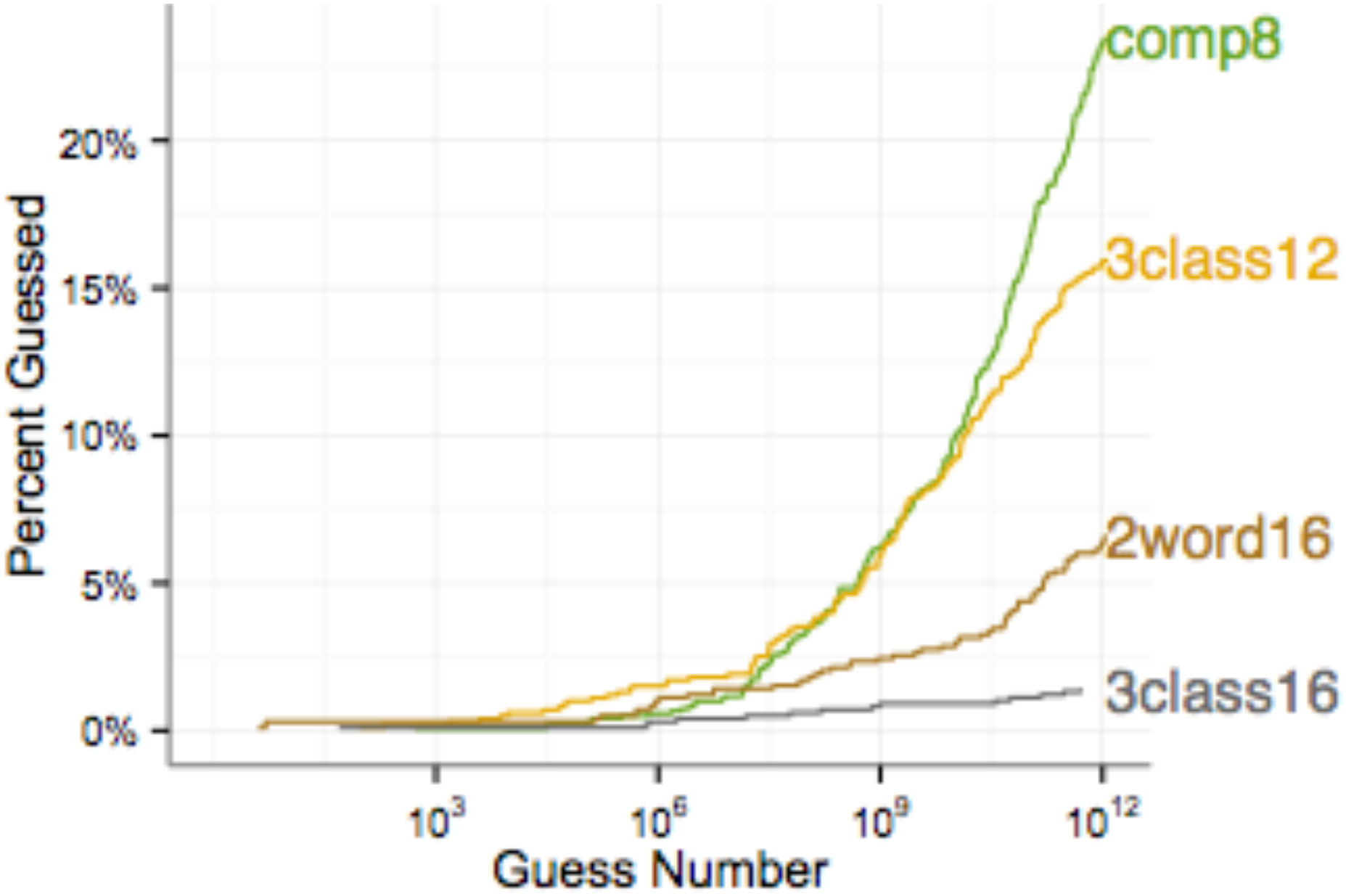

Percent Guessed
4%
2%
0%
comp8
10^3
10^6
Guess Number

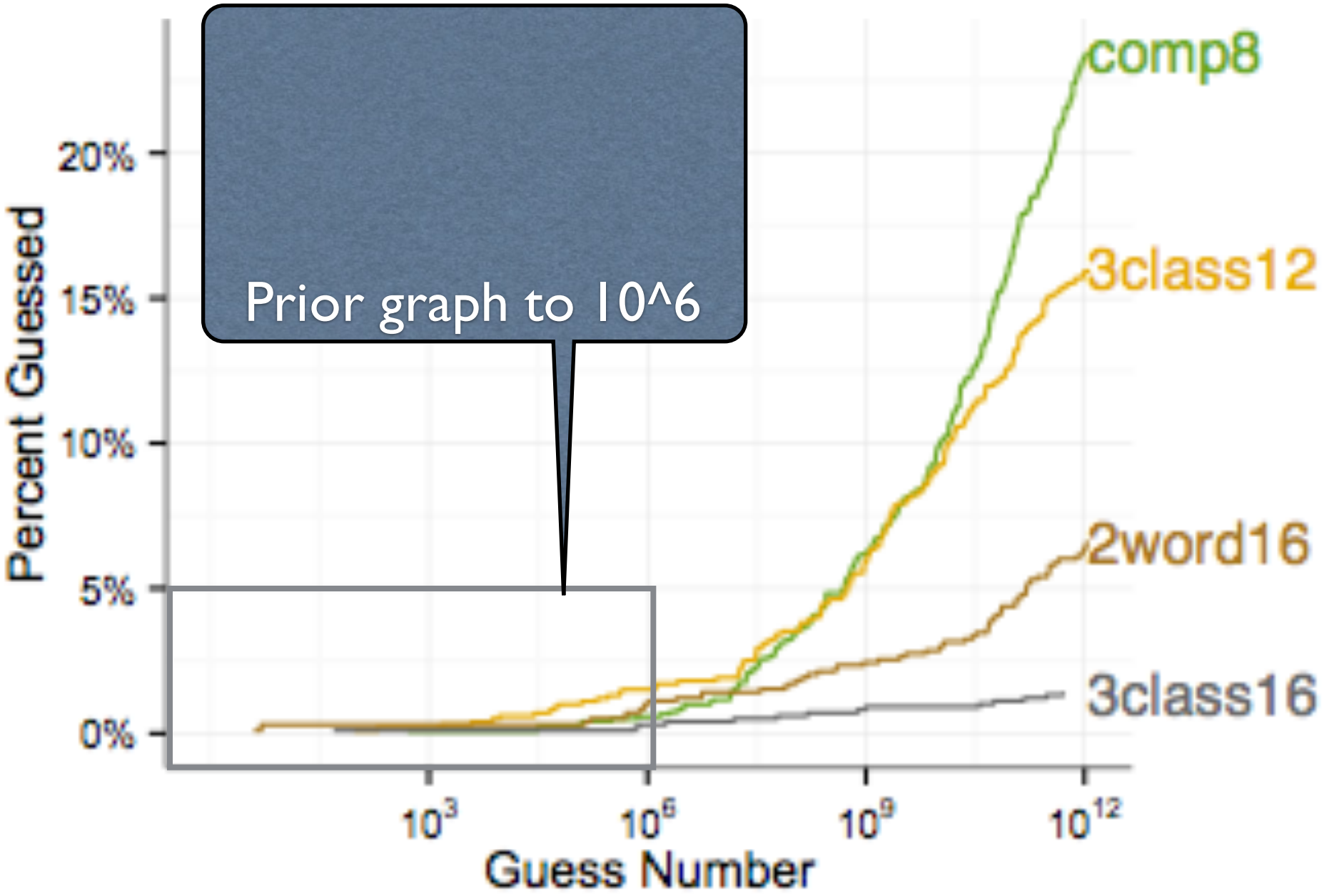

Percent Guessed
4%
2%
0%
comp8
10^3
10^6
Guess Number

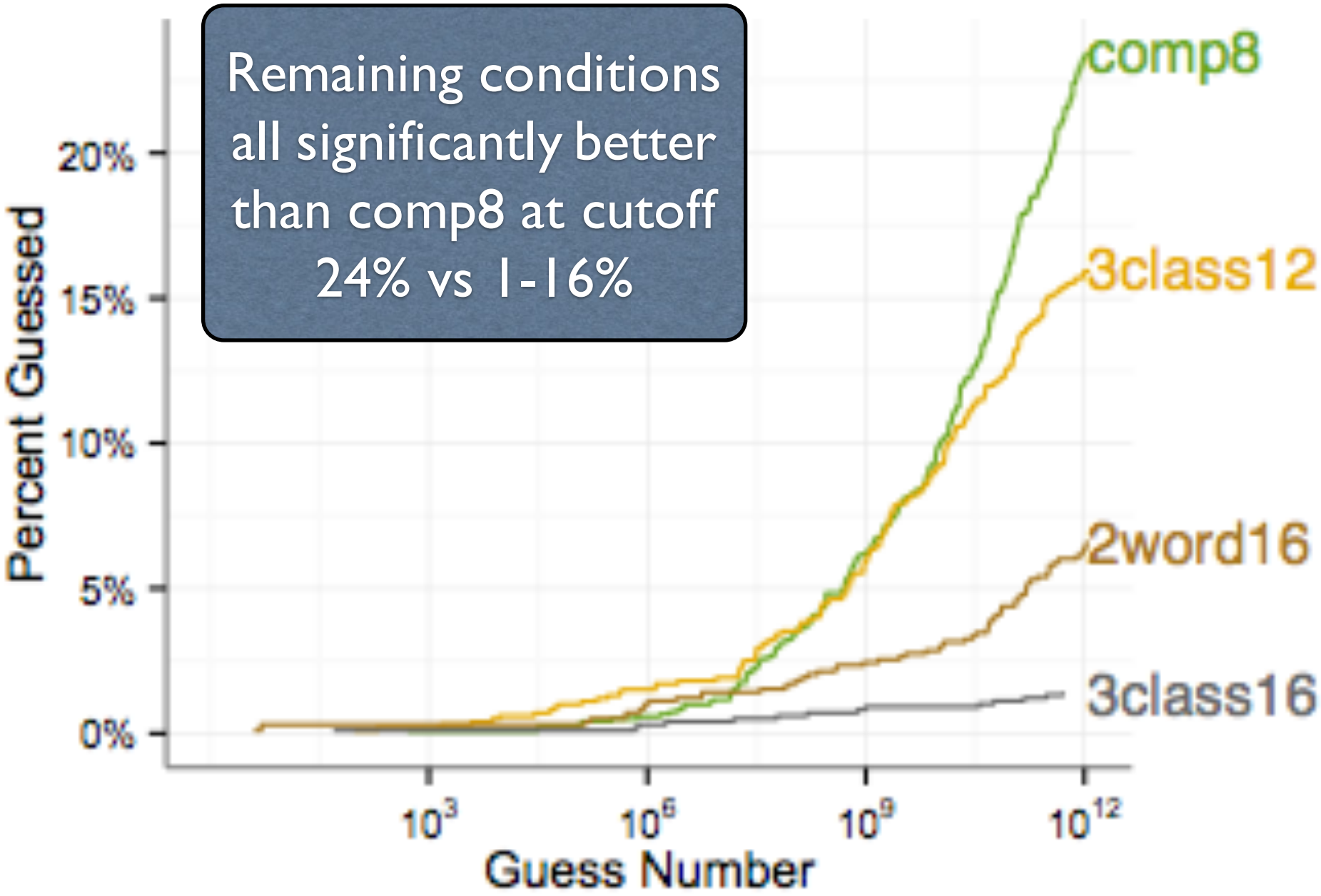

basic16
basic 20
basic 12
2word12
3class12
2word16
comp8
3class16
Percent Guessed
4%
2%
0%
10^3
10^6
Guess Number


comp8 outperforms
2word12 & basic
1% vs 2-5%
basic16
basic 20
basic 12
2word12
3class12
2word16
comp8
3class16
4%
2%
0%
Percent Guessed
10^3
10^6
Guess Number


Percent Guessed
4%
2%
0%
3class12
2word16
comp8
3class16
10^3
10^6
Guess Number

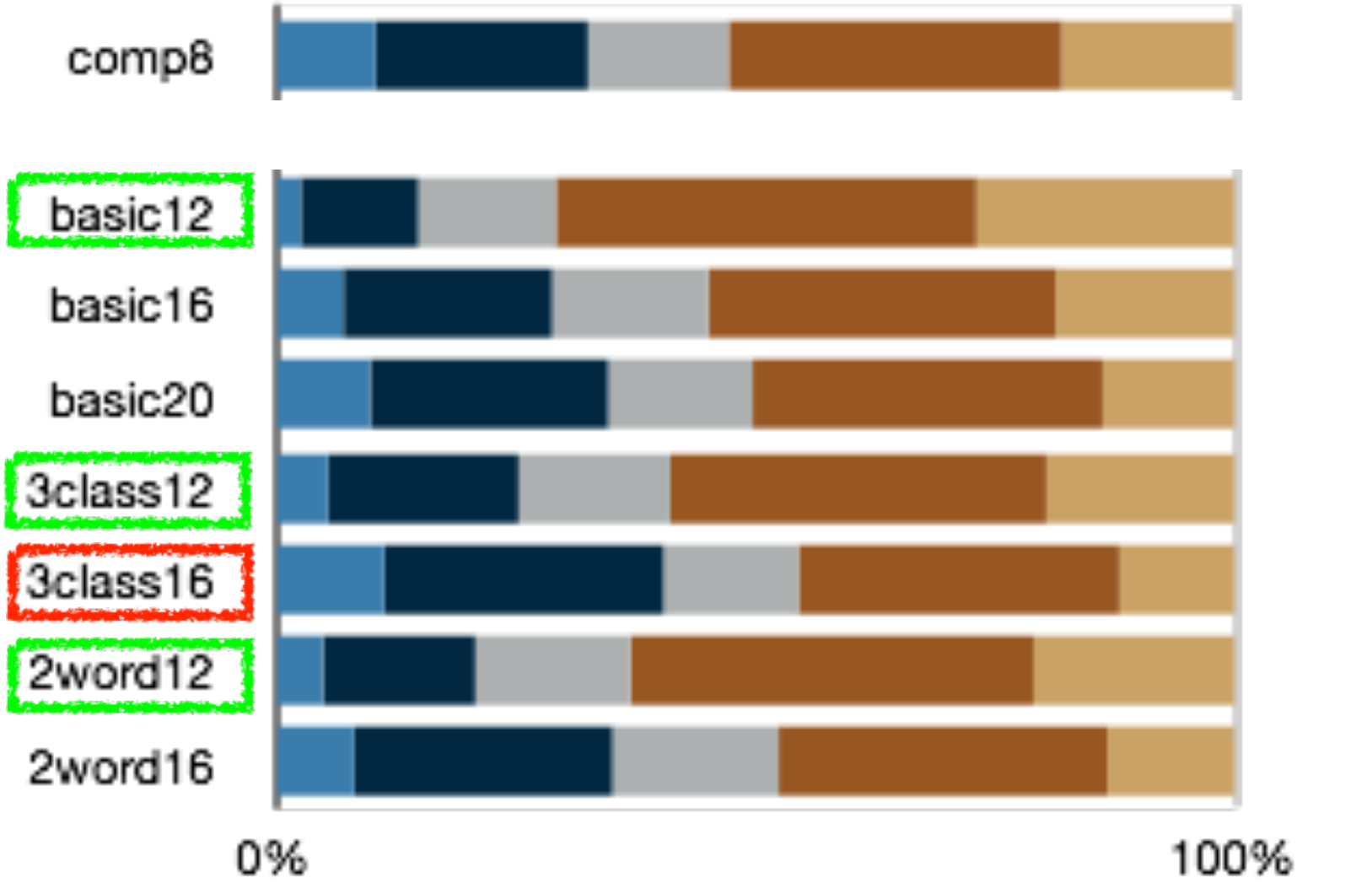

comp8
3class12
2word16
3class16
20%
15%
10%
5%
0%
Percent Guessed
10^3
10^6
10^9
10^{12}
Guess Number


Prior graph to 10^6
comp8
3class12
2word16
3class16
20%
15%
10%
5%
0%
Percent Guessed
10^3
10^6
10^9
10^{12}
Guess Number


Remaining conditions all significantly better than comp8 at cutoff 24% vs 1-16%
comp8
3class12
2word16
3class16
20%
15%
10%
5%
0%
Percent Guessed
10^3
10^6
10^9
10^{12}
Guess Number

Usability Results

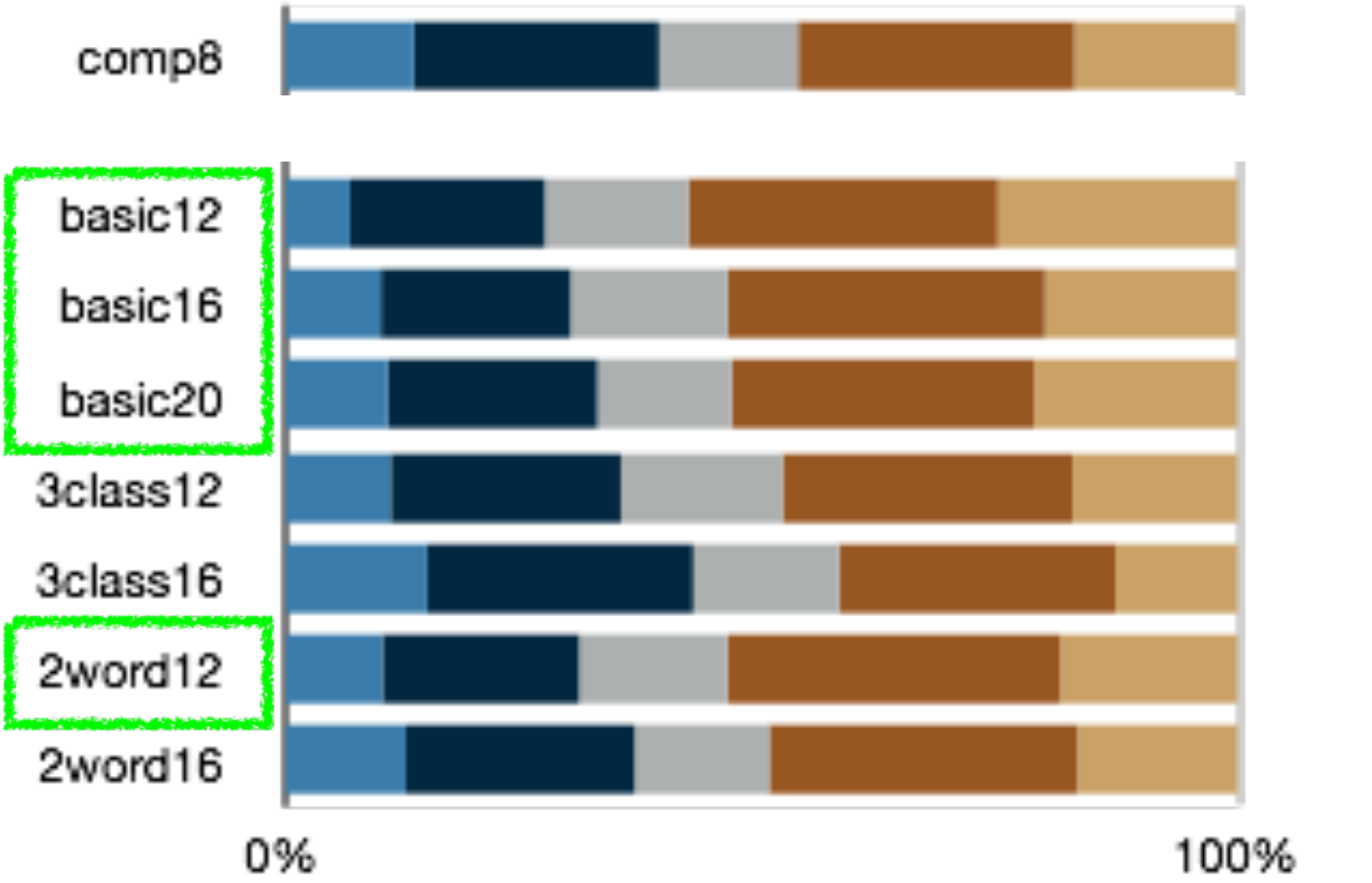
Creation Difficult



Agreement

Disagreement

Recall Difficult



Agreement

Disagreement

comp8						
basic12						
basic16						
basic20						
2word12						
2word16						
3class12						
3class16						

	% cracked 10^6					
comp8	0.6					
basic12	3.9					
basic16	5.2					
basic20	3.9					
2word12	2.1					
2word16	1.0					
3class12	1.5					
3class16	0.3					

	% cracked 10^6	% cracked cutoff				
comp8	**0.6**	**23.5**				
basic12	3.9	24.5				
basic16	5.2	12.4				
basic20	3.9	7.1				
2word12	2.1	22.7				
2word16	1.0	6.6				
3class12	1.5	16.0				
3class16	0.3	1.4				

	% cracked 10^6	% cracked cutoff	% finished part1			
comp8	**0.6**	**23.5**	**83.0**			
basic12	3.9	24.5	94.5			
basic16	5.2	12.4	93.9			
basic20	3.9	7.1	93.9			
2word12	2.1	22.7	92.0			
2word16	1.0	6.6	92.1			
3class12	1.5	16.0	92.0			
3class16	0.3	1.4	90.5			

	% cracked 10^6	% cracked cutoff	% finished part1	% creation difficult		
comp8	**0.6**	**23.5**	**83.0**	**32.6**		
basic12	3.9	24.5	94.5	14.9		
basic16	5.2	12.4	93.9	28.9		
basic20	3.9	7.1	93.9	34.7		
2word12	2.1	22.7	92.0	20.9		
2word16	1.0	6.6	92.1	35.2		
3class12	1.5	16.0	92.0	25.4		
3class16	0.3	1.4	90.5	40.5		

	% cracked 10^6	% cracked cutoff	% finished part1	% creation difficult	part2 recall tries	
comp8	**0.6**	**23.5**	**83.0**	**32.6**	1.4	
basic12	3.9	24.5	94.5	14.9	1.3	
basic16	5.2	12.4	93.9	28.9	1.3	
basic20	3.9	7.1	93.9	34.7	1.3	
2word12	2.1	22.7	92.0	20.9	1.3	
2word16	1.0	6.6	92.1	35.2	1.4	
3class12	1.5	16.0	92.0	25.4	1.4	
3class16	0.3	1.4	90.5	40.5	1.4	

	% cracked 10^6	% cracked cutoff	% finished part1	% creation difficult	part2 recall tries	entry time (sec.)
comp8	**0.6**	**23.5**	**83.0**	**32.6**	1.4	**13.2**
basic12	3.9	24.5	94.5	14.9	1.3	11.6
basic16	5.2	12.4	93.9	28.9	1.3	13.7
basic20	3.9	7.1	93.9	34.7	1.3	15.3
2word12	2.1	22.7	92.0	20.9	1.3	13.1
2word16	1.0	6.6	92.1	35.2	1.4	14.6
3class12	1.5	16.0	92.0	25.4	1.4	14.8
3class16	0.3	1.4	90.5	40.5	1.4	16.2

What would you choose?	% cracked 10^6	% cracked cutoff	% finished part1	% creation difficult	part2 recall tries	entry time (sec.)
comp8	**0.6**	**23.5**	**83.0**	**32.6**	1.4	**13.2**
basic12	3.9	24.5	94.5	14.9	1.3	11.6
basic16	5.2	12.4	93.9	28.9	1.3	13.7
basic20	3.9	7.1	93.9	34.7	1.3	15.3
2word12	2.1	22.7	92.0	20.9	1.3	13.1
2word16	1.0	6.6	92.1	35.2	1.4	14.6
3class12	1.5	16.0	92.0	25.4	1.4	14.8
3class16	0.3	1.4	90.5	40.5	1.4	16.2

	% cracked 10^6	% cracked cutoff	% finished part1	% creation difficult	part2 recall tries	entry time (sec.)
comp8	0.6	23.5	83.0	32.6	1.4	13.2
basic12	3.9	24.5	94.5	14.9	1.3	11.6
basic16	5.2					13.7
basic20	3.9					15.3
2word12	2.1	22.7	92.0	20.9	1.3	13.1
2word16	1.0	6.6	92.1	35.2	1.4	14.6
3class12	1.5	16.0	92.0	25.4	1.4	14.8
3class16	0.3	1.4	90.5	40.5	1.4	16.2

2word16, 3class12 sometimes better than comp8, never worse

	% cracked 10^6	% cracked cutoff	% finished part1	% creation difficult	part2 recall tries	entry time (sec.)
comp8	0.6	23.5	83.0	32.6	1.4	13.2
basic12	3.9	24.5	94.5	14.9	1.3	11.6
basic16	5.2					13.7
basic20						15.3
2word12	2.1	22.7	92.0	20.9	1.3	13.1
2word16	1.0	6.6	92.1	35.2	1.4	14.6
3class12	1.5	16.0	92.0	25.4	1.4	14.8
3class16	0.3	1.4	90.5	40.5	1.4	16.2

2word16 more secure than 3class12

	% cracked 10^6	% cracked cutoff	% finished part1	% creation difficult	part2 recall tries	entry time (sec.)
comp8	0.6	23.5	83.0	32.6	1.4	13.2
basic12	3.9	24.5	94.5	14.9	1.3	11.6
basic16	5.2					13.7
basic20	3.9					15.3
2word12	2.4	22.7	92.0	20.9	1.3	13.1
2word16	1.0	6.6	92.1	35.2	1.4	14.6
3class12	1.5	16.0	92.0	25.4	1.4	14.8
3class16	0.3	1.4	90.5	40.5	1.4	16.2

3class12 more usable during creation than 2word16

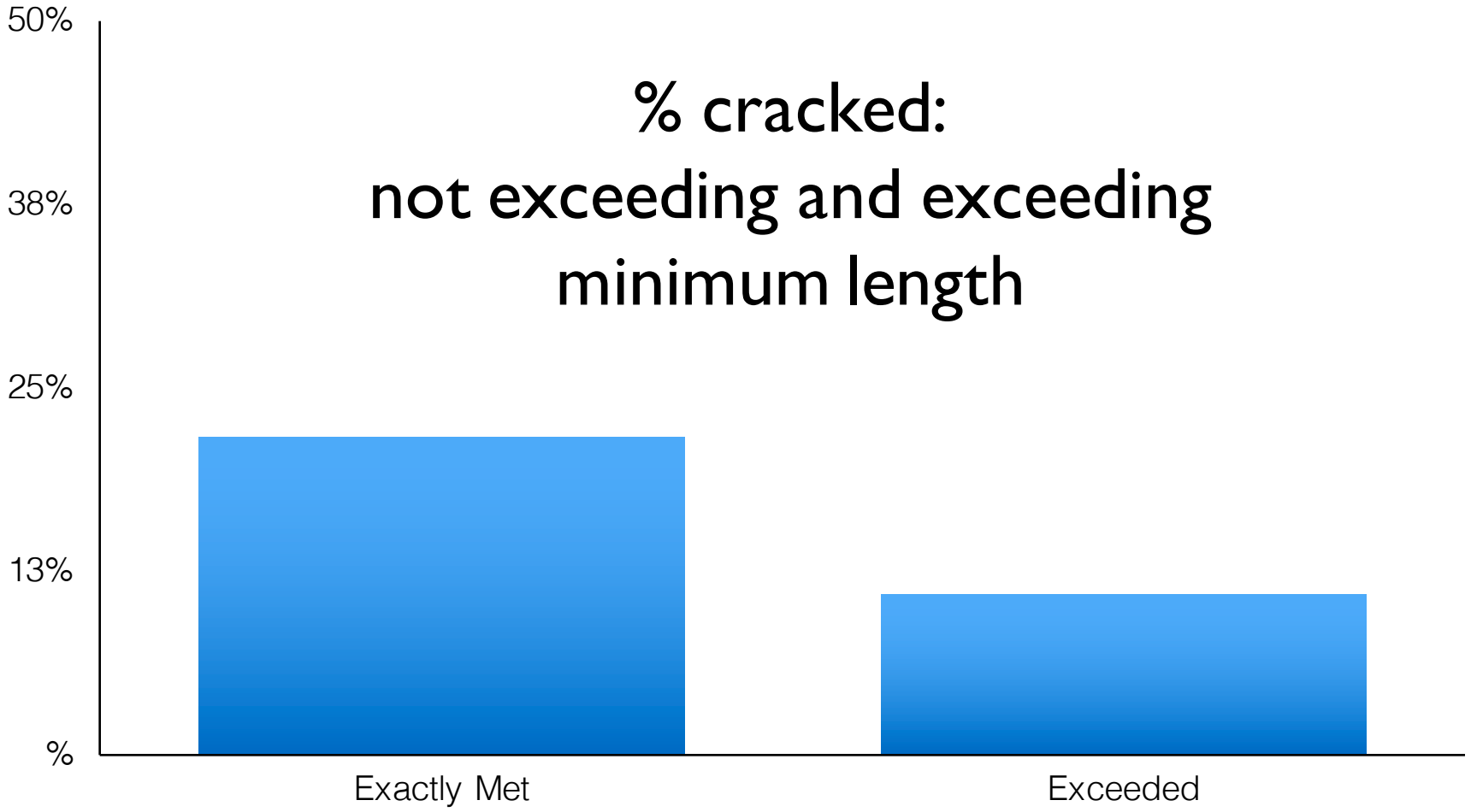
Meeting Requirements

- Prior work speculated users meet requirements in predictable, minimal ways (e.g., NIST 06)
- This was not true in some cases

Exceeding Length Requirement

66% made a longer password than required

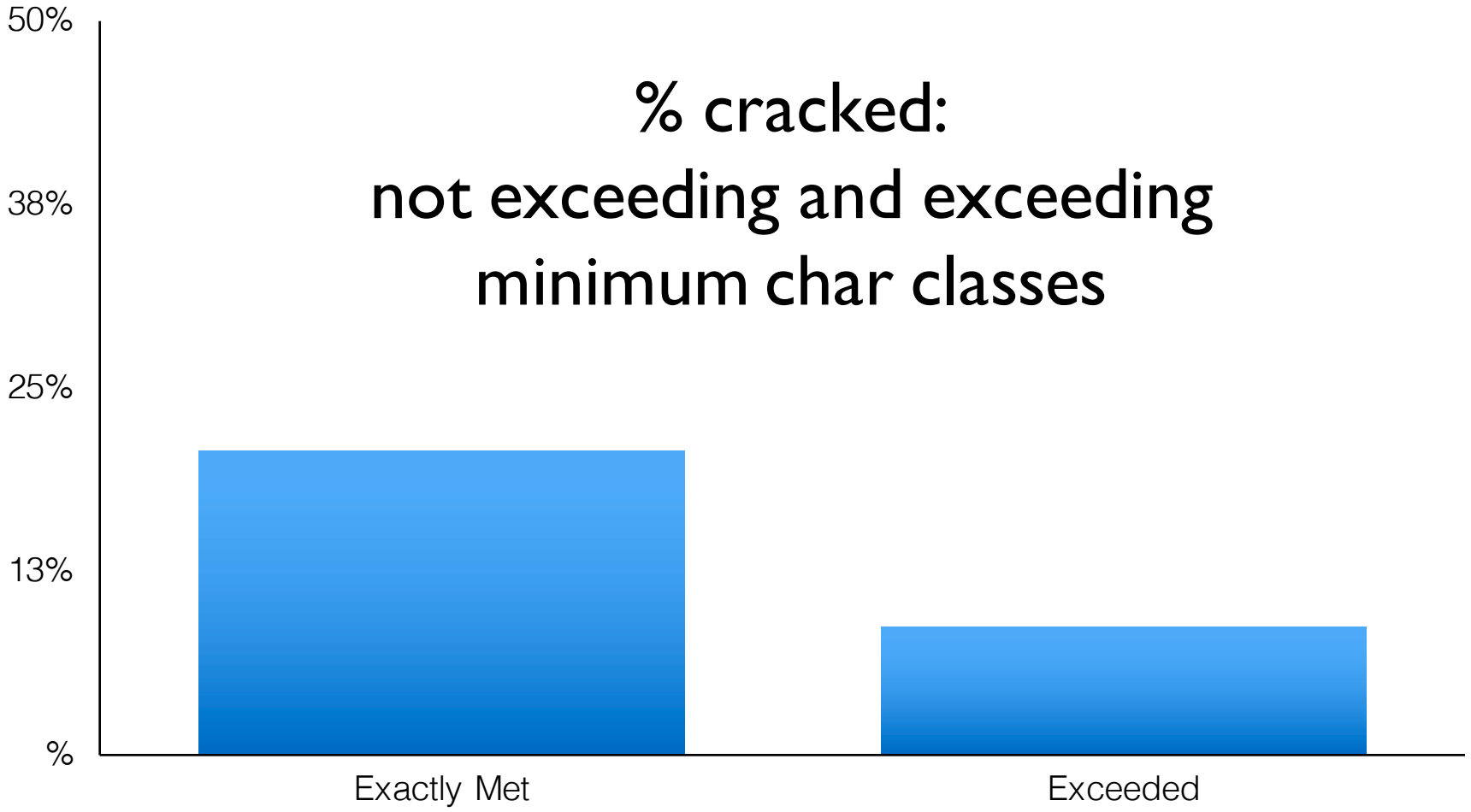
Exceeding Length Requirement



Exceeding Character Class Requirement

64% used more classes than required, ignoring comp8 that needed to use all four

Exceeding Character Class Requirement



Common Substrings in Cracked Passwords

Certain substrings within passwords were a hallmark of more easily cracked passwords

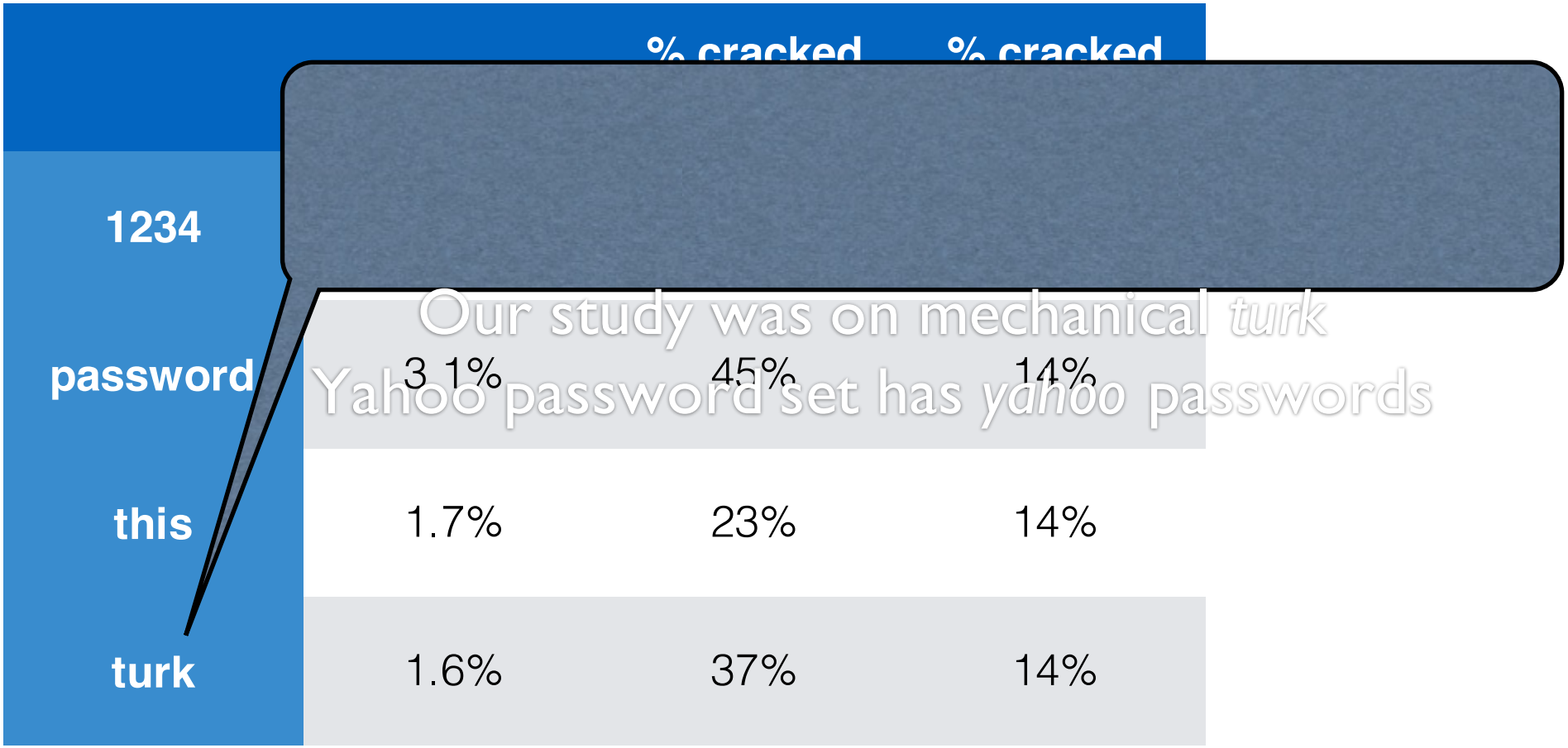
Common Substrings

	containing
1234	4.2%
password	3.1%
this	1.7%
turk	1.6%

Common Substrings

	containing	% cracked with	% cracked without
1234	4.2%	44%	13%
password	3.1%	45%	14%
this	1.7%	23%	14%
turk	1.6%	37%	14%

Common Substrings



	% cracked	% cracked
1234		
password	3.1%	45%	14%
this	1.7%	23%	14%
turk	1.6%	37%	14%

Our study was on mechanical *turk*

Yahoo password set has *yahoo* passwords

Limitations

- What do you think they were?

Limitations

- Only test recall after 5 minutes & 2 days
- Passwords not protecting actual value
  - Recent work showed MTurk workers make similar passwords to real users (CCS 2013)

Conclusion

- Longer password policies can be more usable, sometimes more secure, than traditional "strong" policies
- 3class12, 2word16 emerged as promising
- Patterns emerged in cracked passwords