Diversify to Survive: Making Passwords Stronger with Adaptive Policies

Sean Segreti, William Melicher, Saranga Komanduri, Darya Melicher, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Michelle Mazurek

Carnegie Mellon  UNIVERSITY OF MARYLAND  THE UNIVERSITY OF CHICAGO

“Top 10” Passwords of 2016

123456	1234567890
123456789	123467
qwerty	password
12345678	123123
111111	987654321

https://keepersecurity.com/public/Most-Common-Passwords-of-2016-Keeper-Security-Study.pdf

Example Password Policy

NIST recommendation (2006-2016)

- Minimum 8 character length
- At least one uppercase
- At least one lowercase
- At least one digit
- At least one special
- No dictionary words

National Institute of Standards and Technology

Example Password Policy

NIST recommendation (2006-2016)

- Minimum 8 character length
- At least one uppercase
- At least one lowercase
- At least one digit
- At least one special
- No dictionary words



Galiza1*

Traditional Password Policies Have Limits

Traditional Password Policies Have Limits

`C@rnival1` `Gracie1` `Ricoman#1`

Traditional Password Policies Have Limits

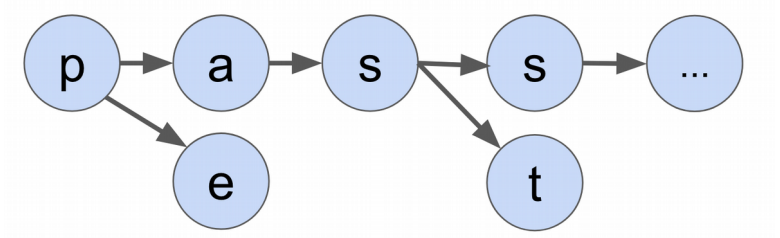
C@rnival1 Gracie1 Ricoman#1

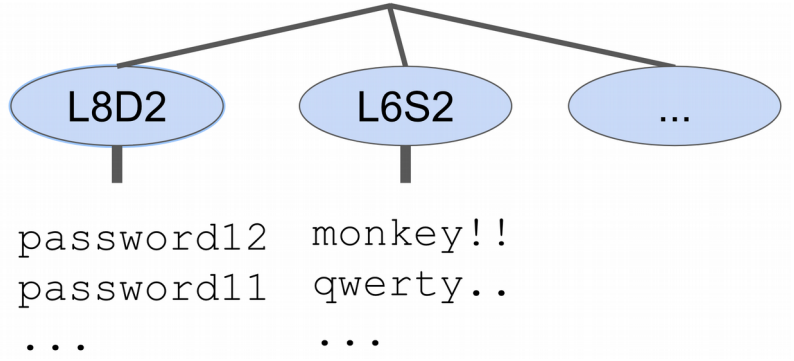
$1 → Append a “1”
c → Capitalize the first letter

Traditional Password Policies Have Limits

C@rnival1 Gracie1 Ricoman#1

$1 → Append a “1”
c → Capitalize the first letter





What if password policies could write themselves?

Traditional policies	
Password requirements statically defined	
Prevent passwords with known bad characteristics	

Traditional policies	Adaptive policies
Password requirements statically defined	
Prevent passwords with known bad characteristics	

Traditional policies	Adaptive policies
Password requirements statically defined	Password requirements evolve over time
Prevent passwords with known bad characteristics	

Traditional policies	Adaptive policies
Password requirements statically defined	Password requirements evolve over time
Prevent passwords with known bad characteristics	Prevent passwords with any shared characteristics

Traditional policies	Adaptive policies
Password requirements statically defined	Password requirements evolve over time
Prevent passwords with known bad characteristics	Prevent passwords with any shared characteristics

Adaptive policies enforce password diversity

Are adaptive policies a good idea?

Q1: Are adaptive policies beneficial to password security?

Are adaptive policies a good idea?

Q1: Are adaptive policies beneficial to password security?

Q2: What effect do they have on usability?

Structure-based Adaptive Policy

Leininger et al.'s approach (Pathwell)

Structure-based Adaptive Policy

Leininger et al.'s approach (Pathwell)

Password *structure*:

Structure-based Adaptive Policy

Leininger et al.'s approach (Pathwell)

Password *structure*: sequence of character classes

Structure-based Adaptive Policy

Leininger et al.'s approach (Pathwell)

Password *structure*: sequence of character classes

Password: `Galiza1*`

Structure-based Adaptive Policy

Leininger et al.'s approach (Pathwell)

Password *structure*: sequence of character classes

Password: `Galiza1*`

Structure: `ULLLLLLDS`

Structure-based Adaptive Policy

Leininger et al.'s approach (Pathwell)

Password *structure*: sequence of character classes

Utilizes a structure blacklist to encourage password structure uniqueness across accounts

Structure-based Adaptive Policy

Leininger et al.'s approach (Pathwell)

Password *structure*: sequence of character classes

Utilizes a structure blacklist to encourage password structure uniqueness across accounts

$Password_A$: `Galiza1*`

Structure-based Adaptive Policy

Leininger et al.'s approach (Pathwell)

Password *structure*: sequence of character classes

Utilizes a structure blacklist to encourage password structure uniqueness across accounts

$Password_A$: `Galiza1*`

$Password_B$:

Structure-based Adaptive Policy

Leininger et al.'s approach (Pathwell)

Password *structure*: sequence of character classes

Utilizes a structure blacklist to encourage password structure uniqueness across accounts

$Password_A$: `Galiza1*`

$Password_B$: `Tartan6!`

Structure-based Adaptive Policy

Leininger et al.'s approach (Pathwell)

Password *structure*: sequence of character classes

Utilizes a structure blacklist to encourage password structure uniqueness across accounts

Password_A: `Galiza1*` (ULLLLLLDS)

Password_B: ~~`Tartan6!`~~ (ULLLLLLDS)

Structure-based Adaptive Policy

Leininger et al.'s approach (Pathwell)

Password *structure*: sequence of character classes

Utilizes a structure blacklist to encourage password structure uniqueness across accounts

$Password_A$: `Galiza1*`

$Password_B$:

Structure-based Adaptive Policy

Leininger et al.'s approach (Pathwell)

Password *structure*: sequence of character classes

Utilizes a structure blacklist to encourage password structure uniqueness across accounts

$Password_A$: `Galiza1*`

$Password_B$: `Gal!za1*`

Structure-based Adaptive Policy

Leininger et al.'s approach (Pathwell)

Password *structure*: sequence of character classes

Utilizes a structure blacklist to encourage password structure uniqueness across accounts

Password_A: `Galiza1*` (ULLLLLLDS)

Password_B: `Gal!za1*` (ULLSLLDS)

String-based Adaptive Policy

Schechter et al.'s approach (HotSec 2010)

String-based Adaptive Policy

Schechter et al.'s approach (HotSec 2010)

Ensures that all users have unique passwords

String-based Adaptive Policy

Schechter et al.'s approach (HotSec 2010)

Ensures that all users have unique passwords

Implements a dynamic dictionary check

User Study Methodology

User Study Methodology

2,619-participant between-subjects online experiment

User Study Methodology

2,619-participant between-subjects online experiment

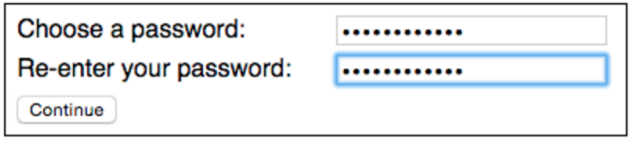
Two-part study

User Study Methodology

2,619-participant between-subjects online experiment

Two-part study

- Part 1: password creation

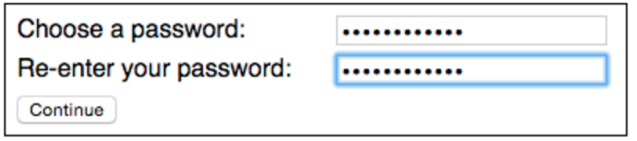


User Study Methodology

2,619-participant between-subjects online experiment

Two-part study

- Part 1: password creation



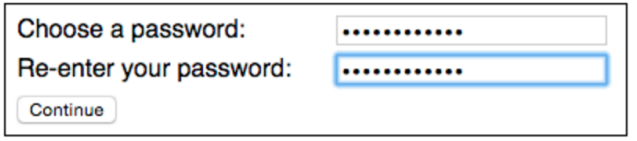
- Part 2: 48 hours later → password recall

User Study Methodology

2,619-participant between-subjects online experiment

Two-part study

- Part 1: password creation



- Part 2: 48 hours later → password recall

Created password in one of 12 conditions

Independent Variables

Independent Variables

Adaptive policy enabled/disabled

Independent Variables

Adaptive policy enabled/disabled

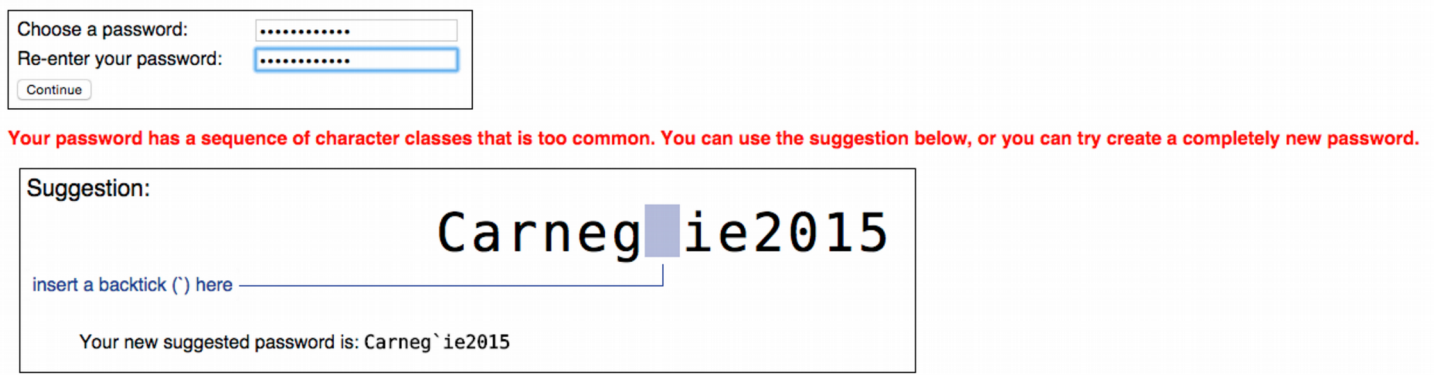
Number of pre-existing users

Independent Variables

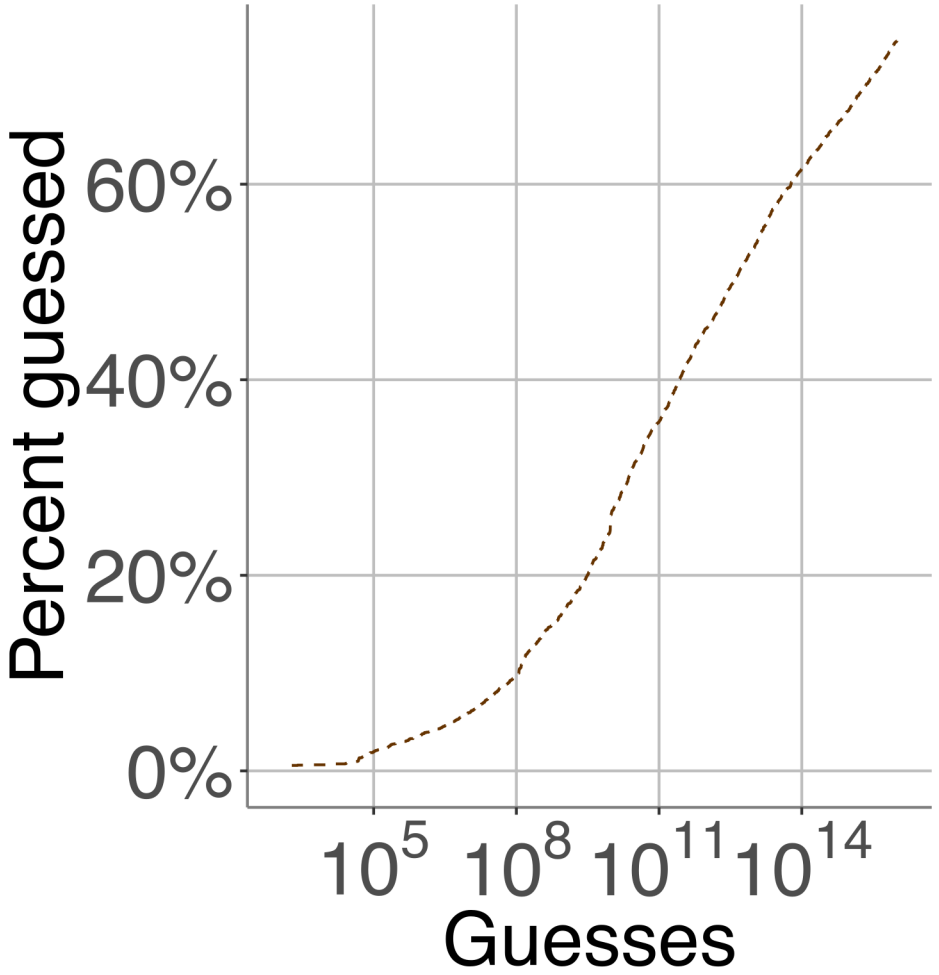
Adaptive policy enabled/disabled

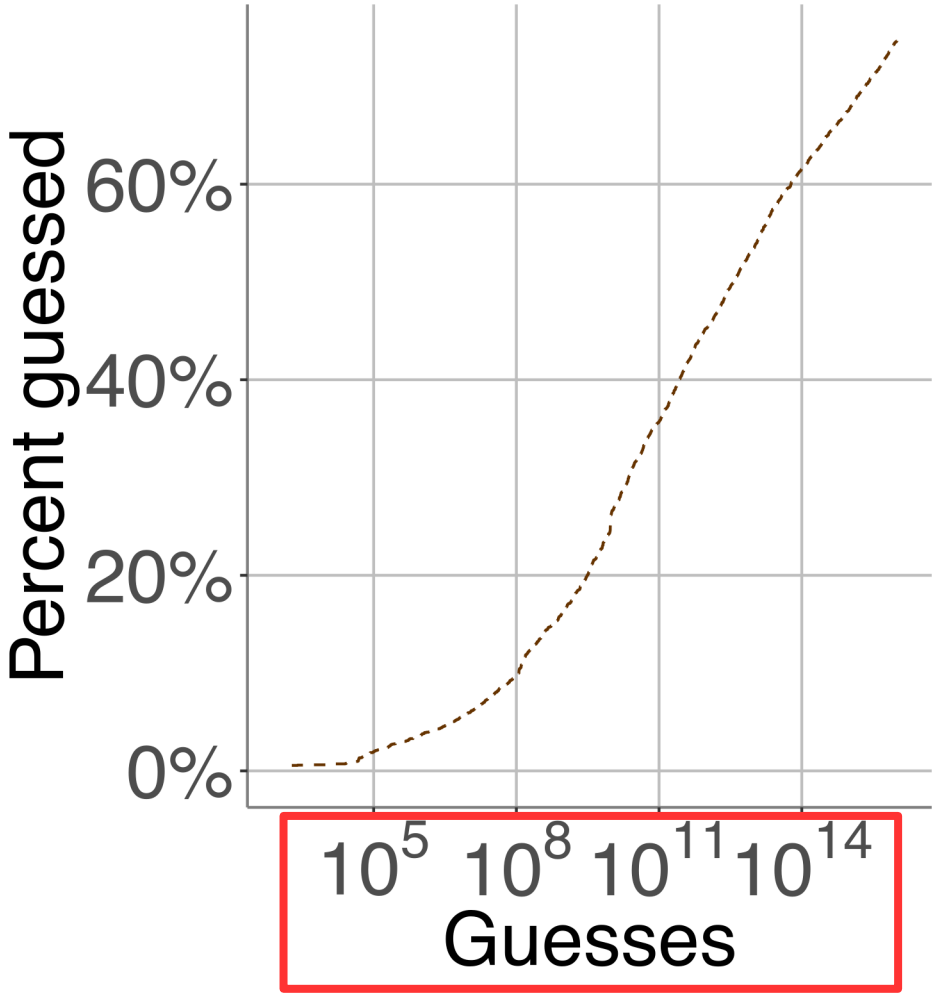
Number of pre-existing users

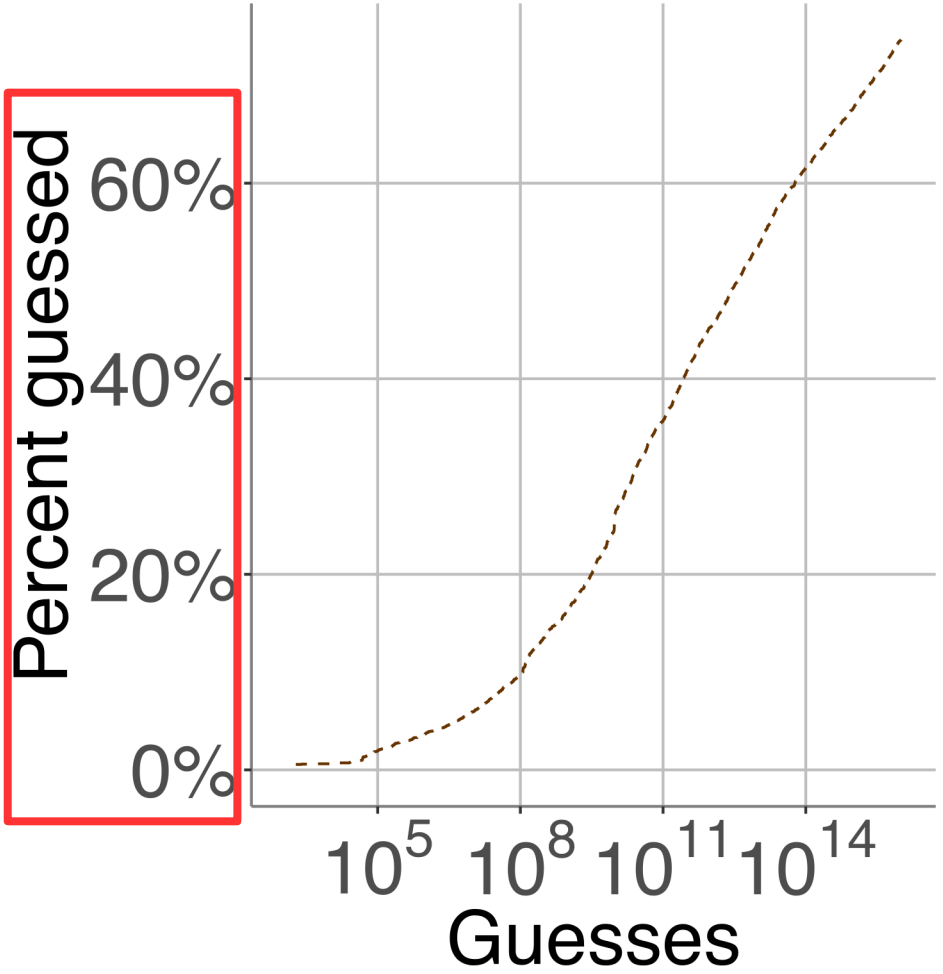
User feedback

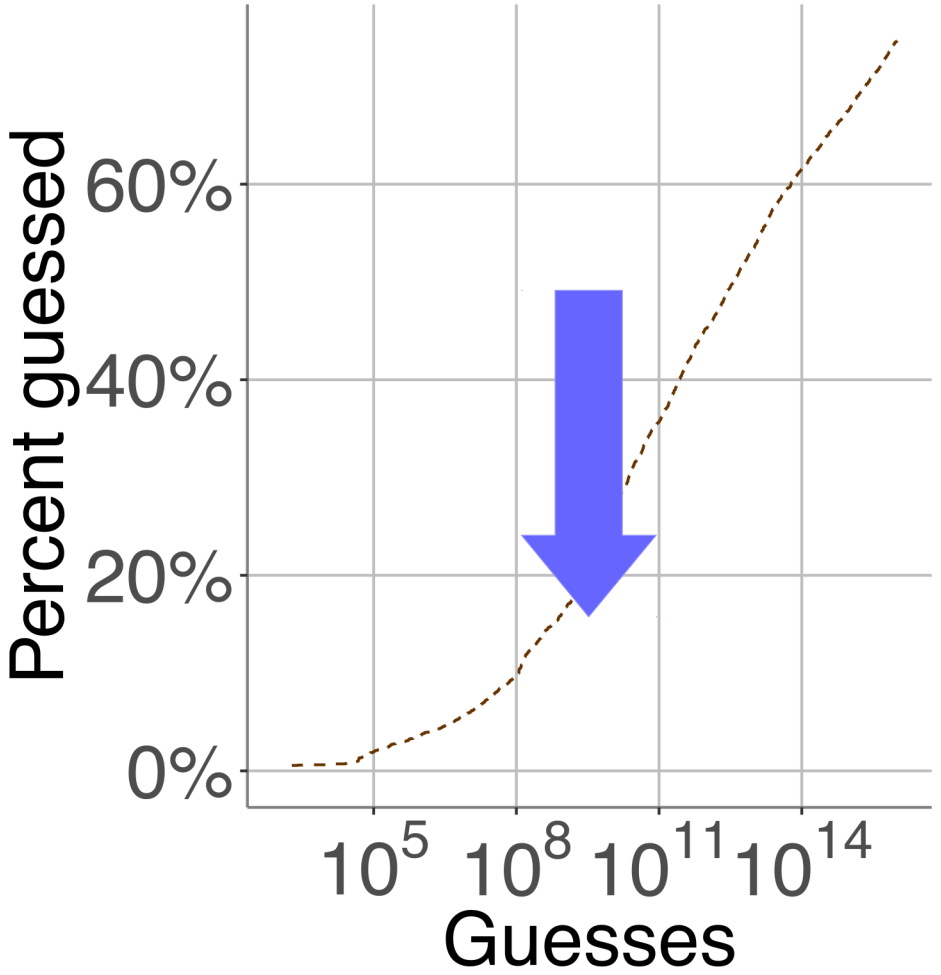


Password Strength	Password Usability
Syntactic characteristics	Participant observations
Resistance to simulated guessing attacks	Participant sentiment

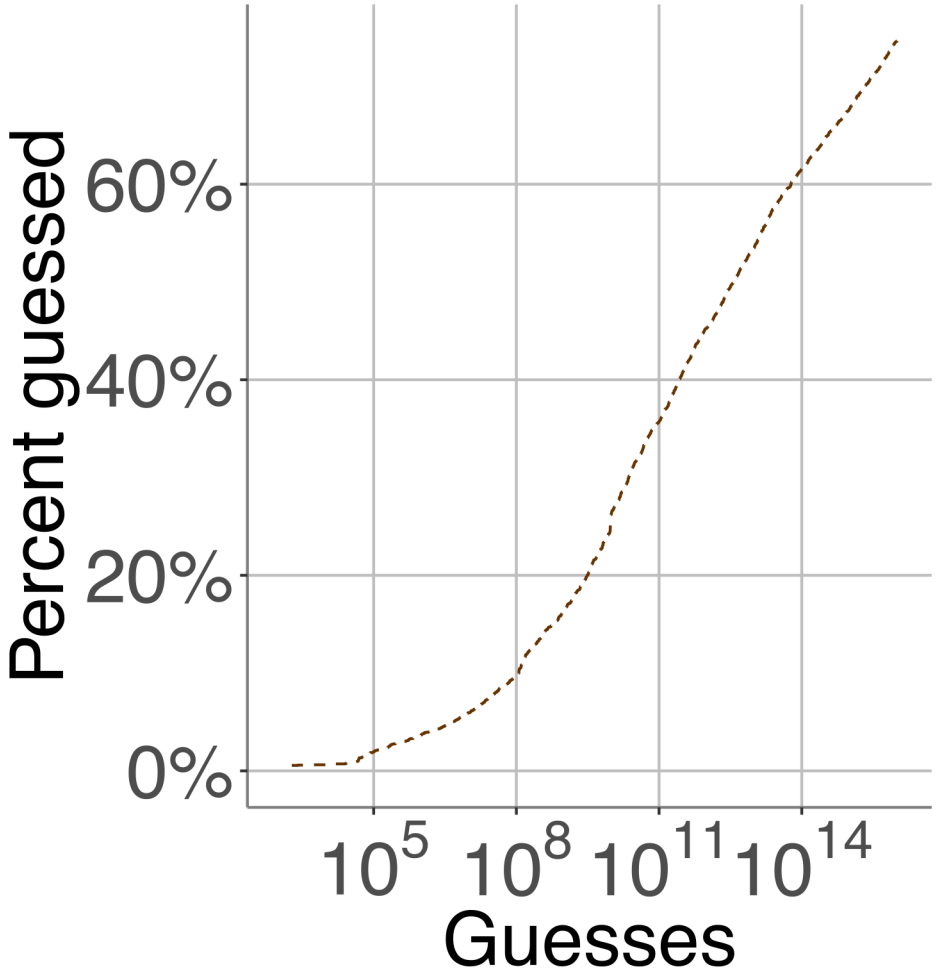

Percent guessed
60%
40%
20%
0%
10^5 10^8 10^{11} 10^{14}
Guesses


Percent guessed
60%
40%
20%
0%
10^5 10^8 10^{11} 10^{14}
Guesses

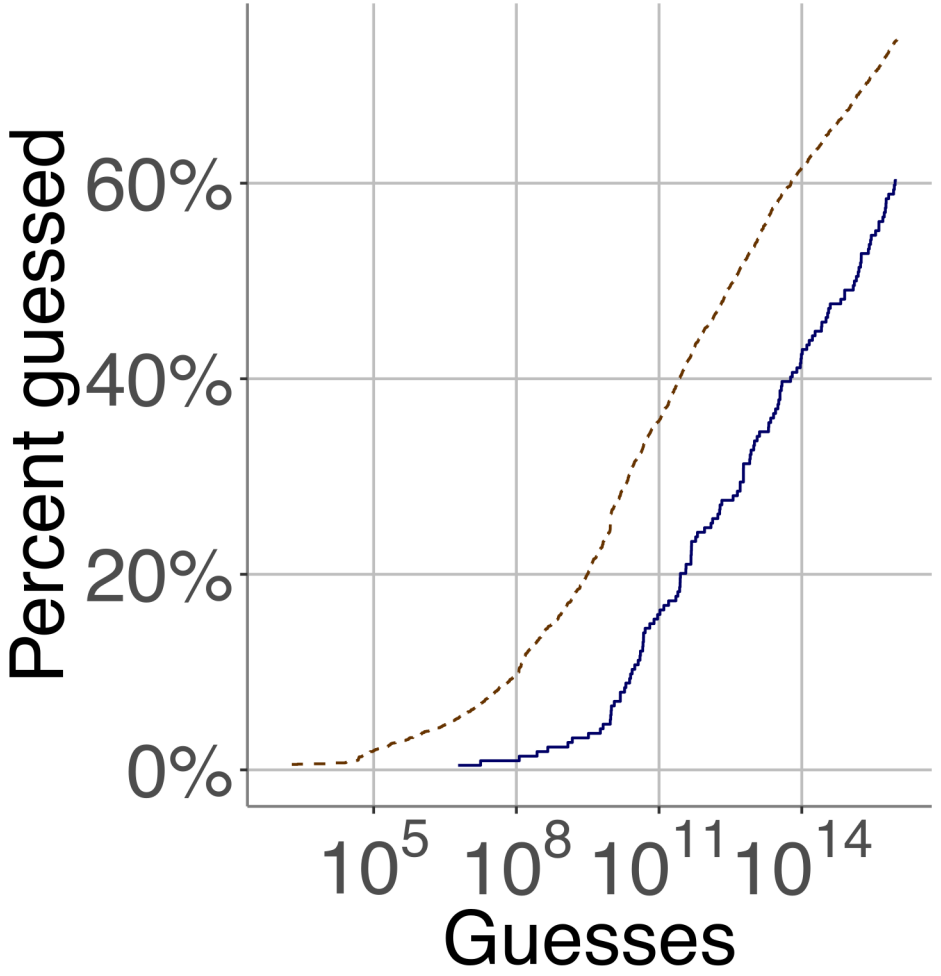

Percent guessed
60%
40%
20%
0%
10^5 10^8 10^{11} 10^{14}
Guesses



Harder to guess passwords

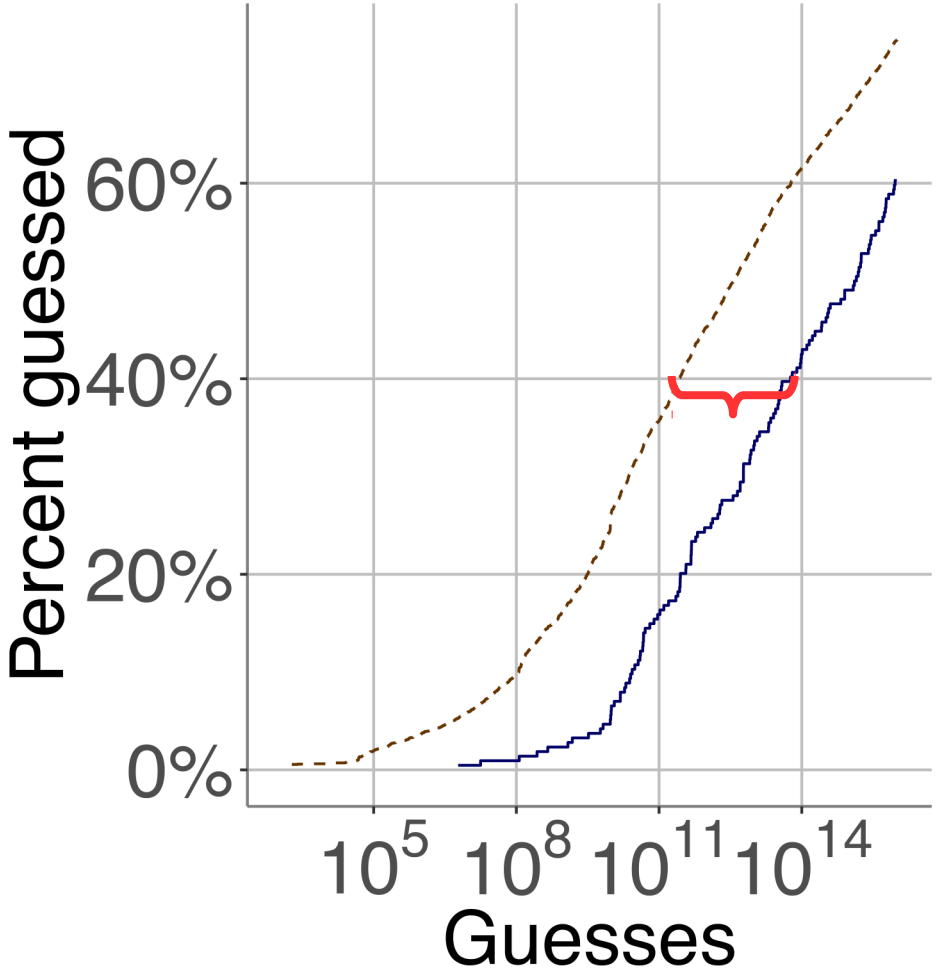


NIST recommended



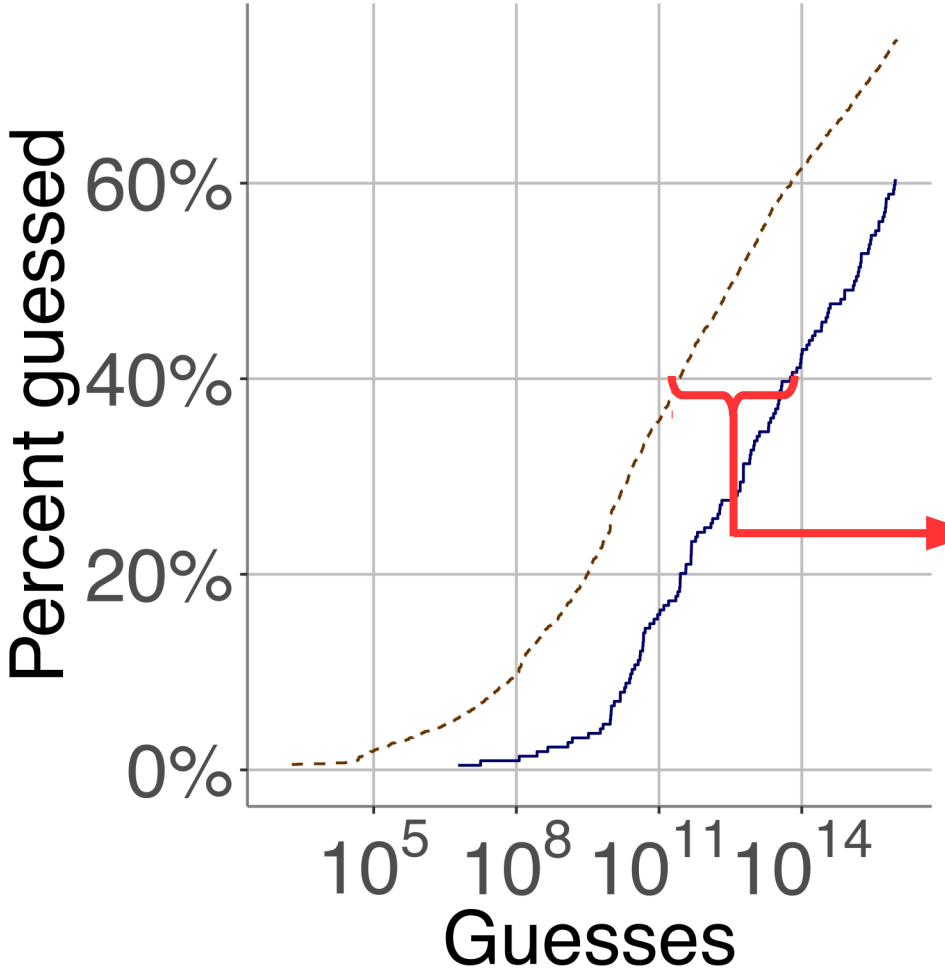
NIST recommended

NIST + structure-based policy



NIST recommended

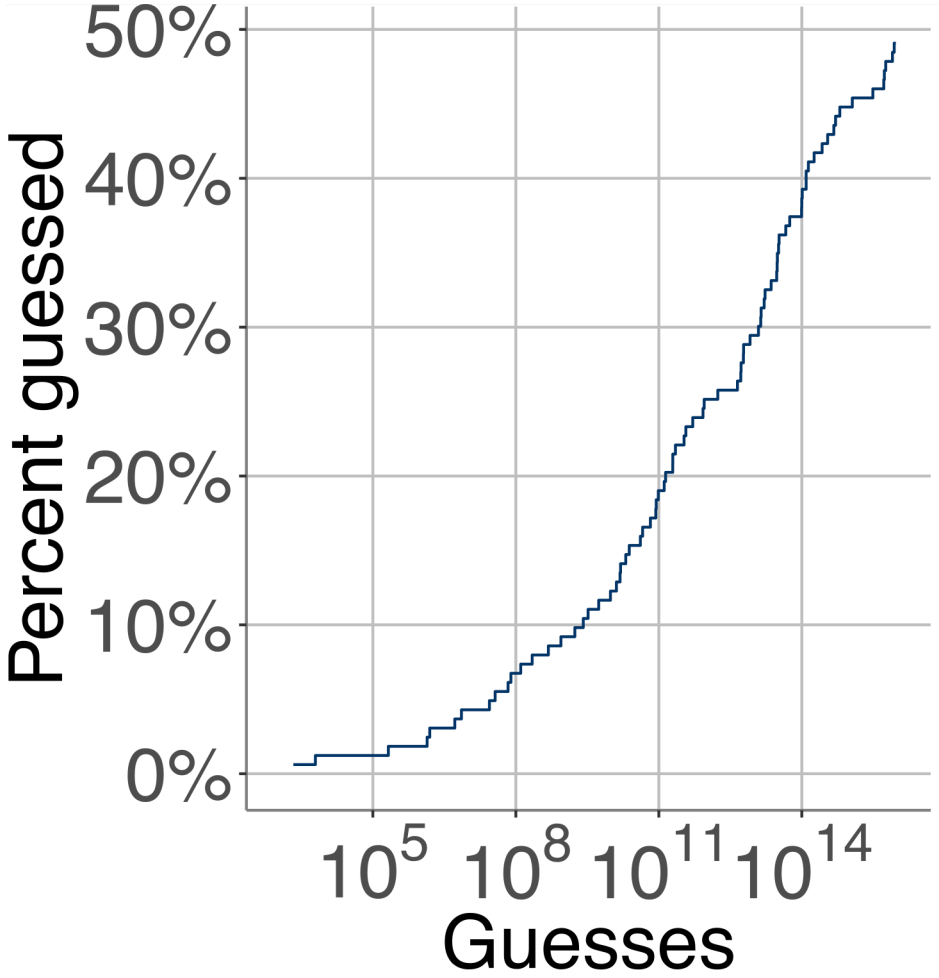
NIST + structure-based policy



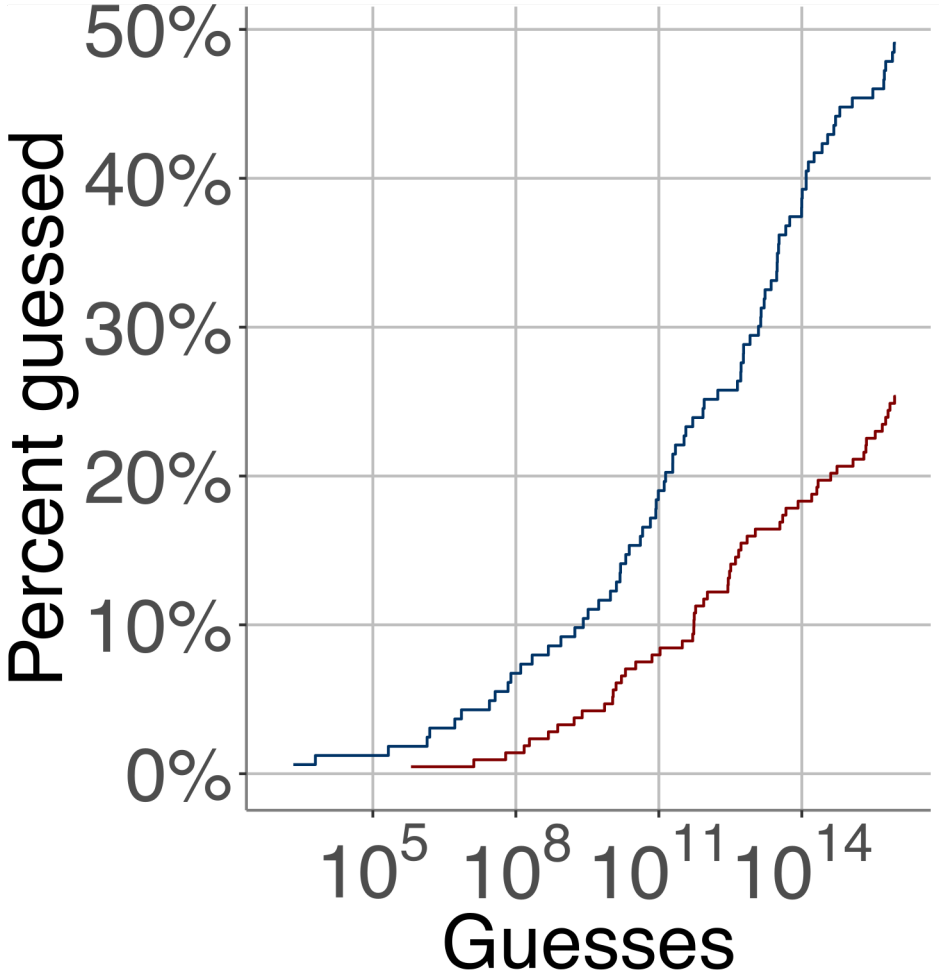
NIST recommended

NIST + structure-based policy

1000x as many guesses

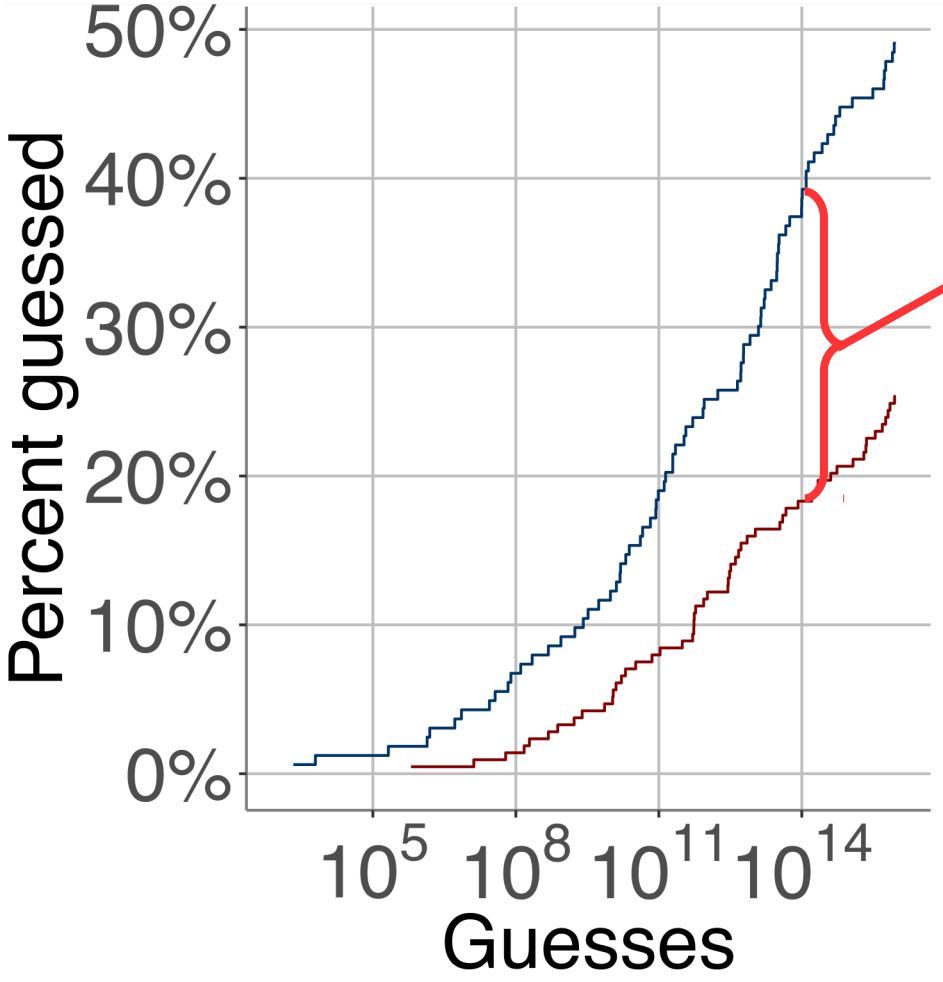


Longer traditional policy



Longer traditional policy

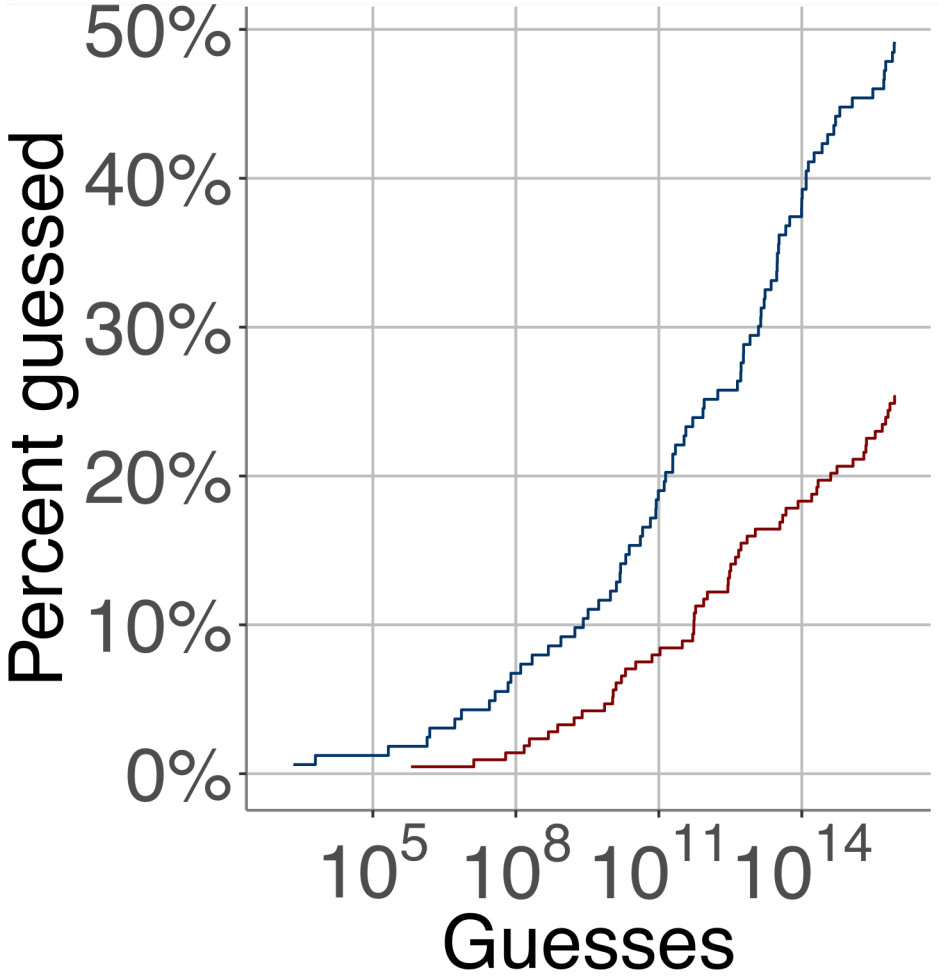
+ structure-based policy



Longer traditional policy

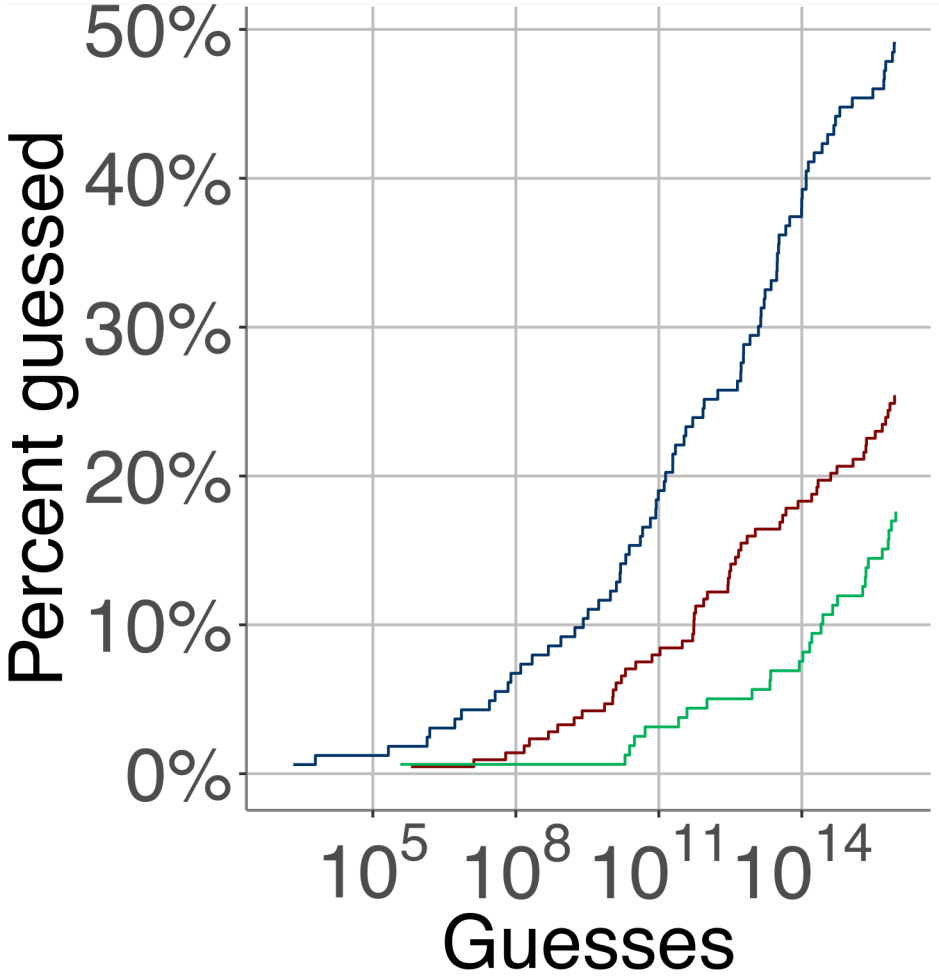
Half as many “cracks”

+ structure-based policy



Longer traditional policy

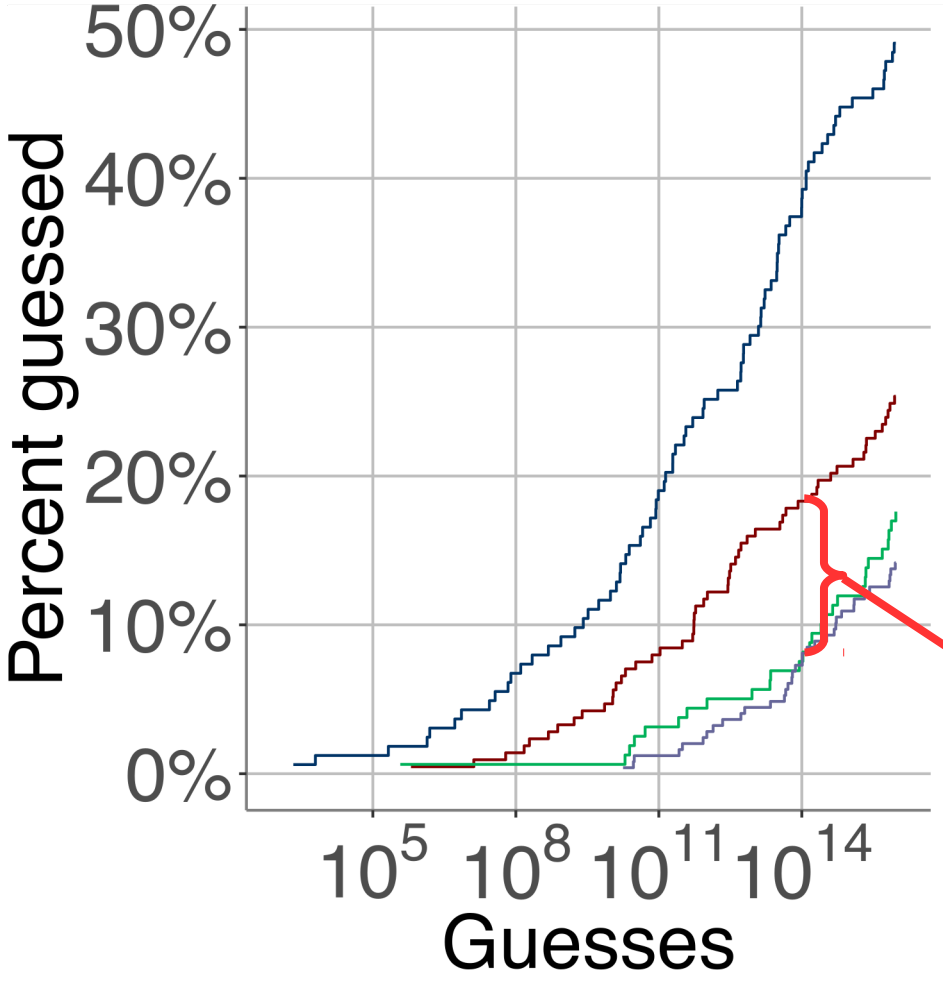
~2,000 blacklisted structures



Longer traditional policy

~2,000 blacklisted structures

~9,000 blacklisted structures



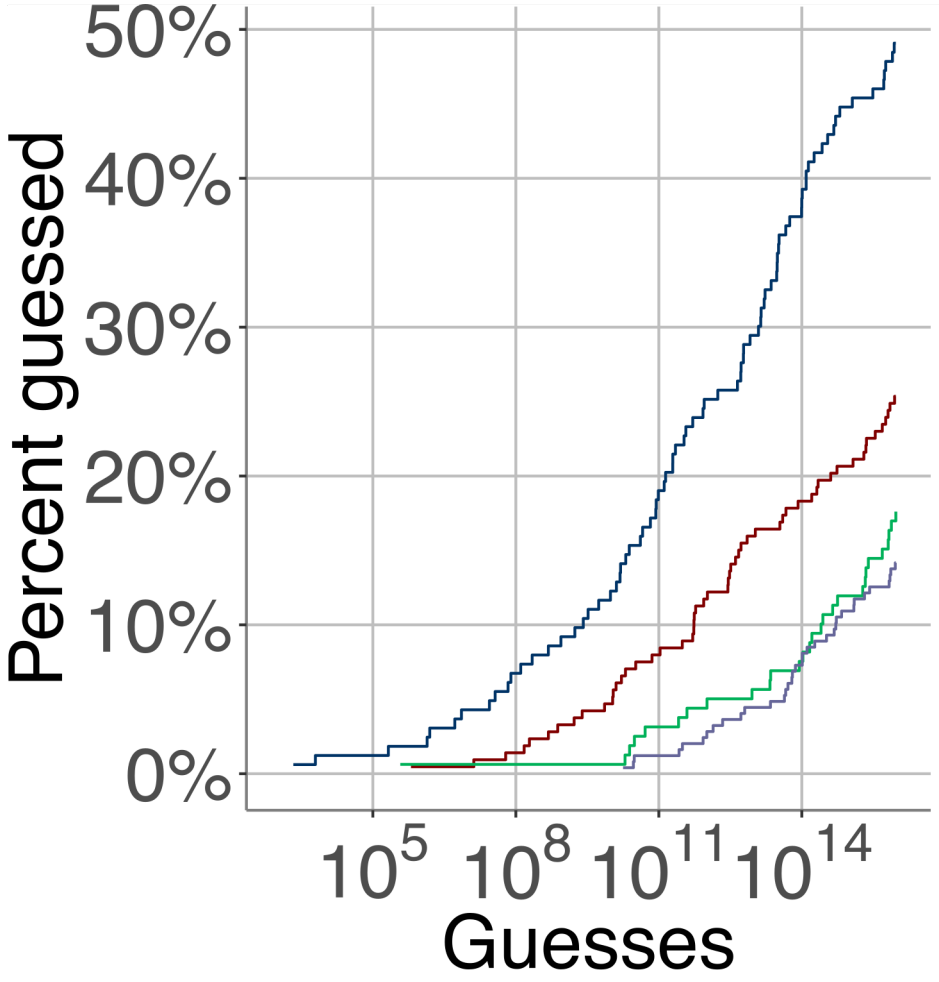
Longer traditional policy

~2,000 blacklisted structures

~9,000 blacklisted structures

~48,000 blacklisted structures

Half as many “cracks”

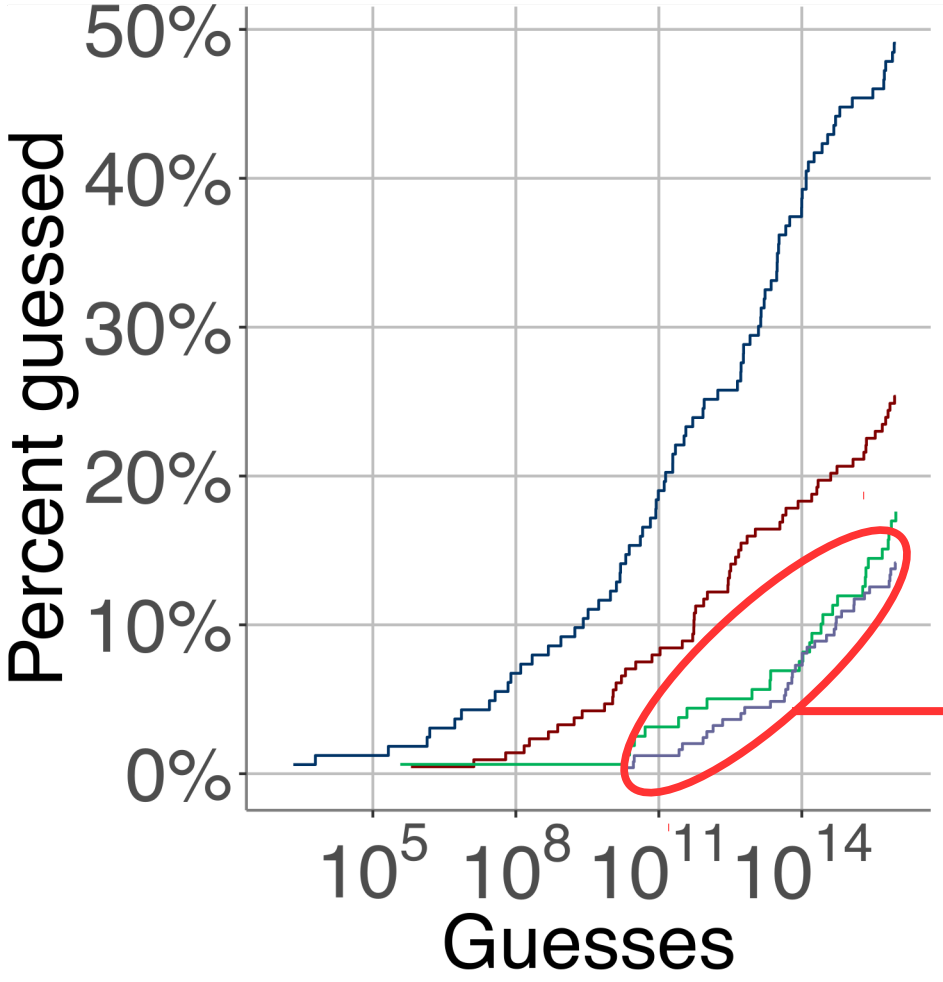


Longer traditional policy

~2,000 blacklisted structures

~9,000 blacklisted structures

~48,000 blacklisted structures



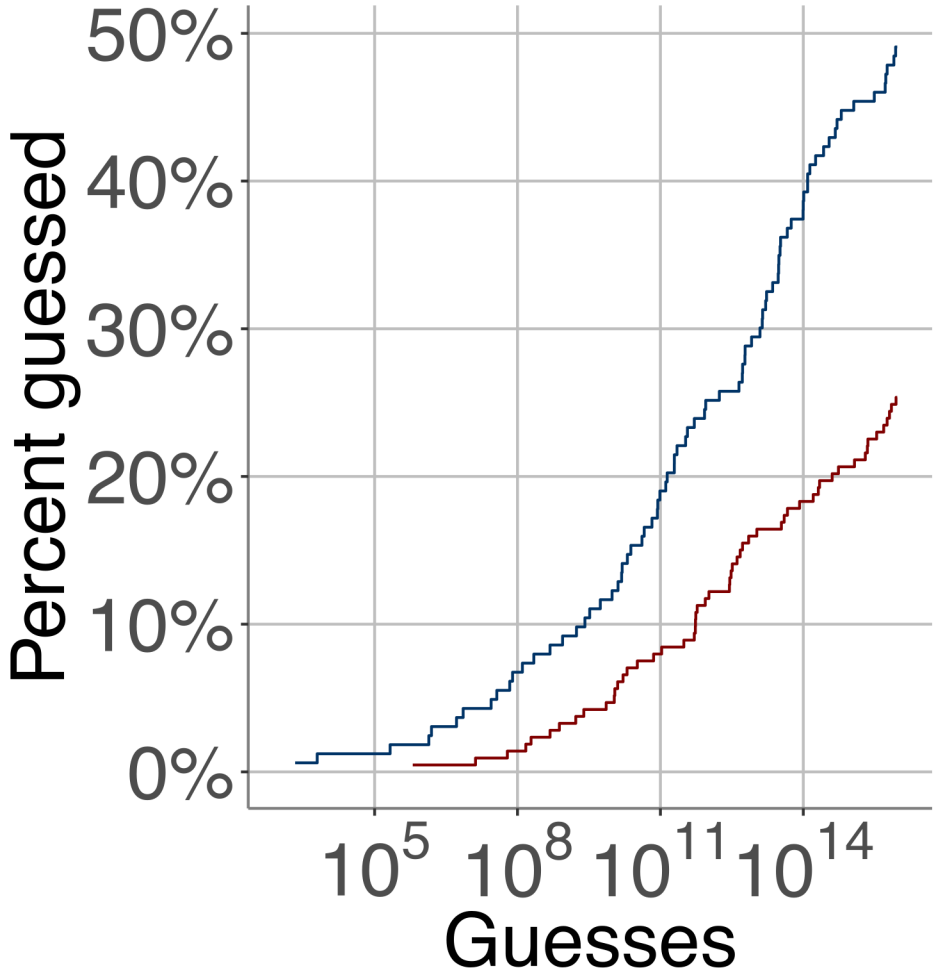
Longer traditional policy

~2,000 blacklisted structures

~9,000 blacklisted structures

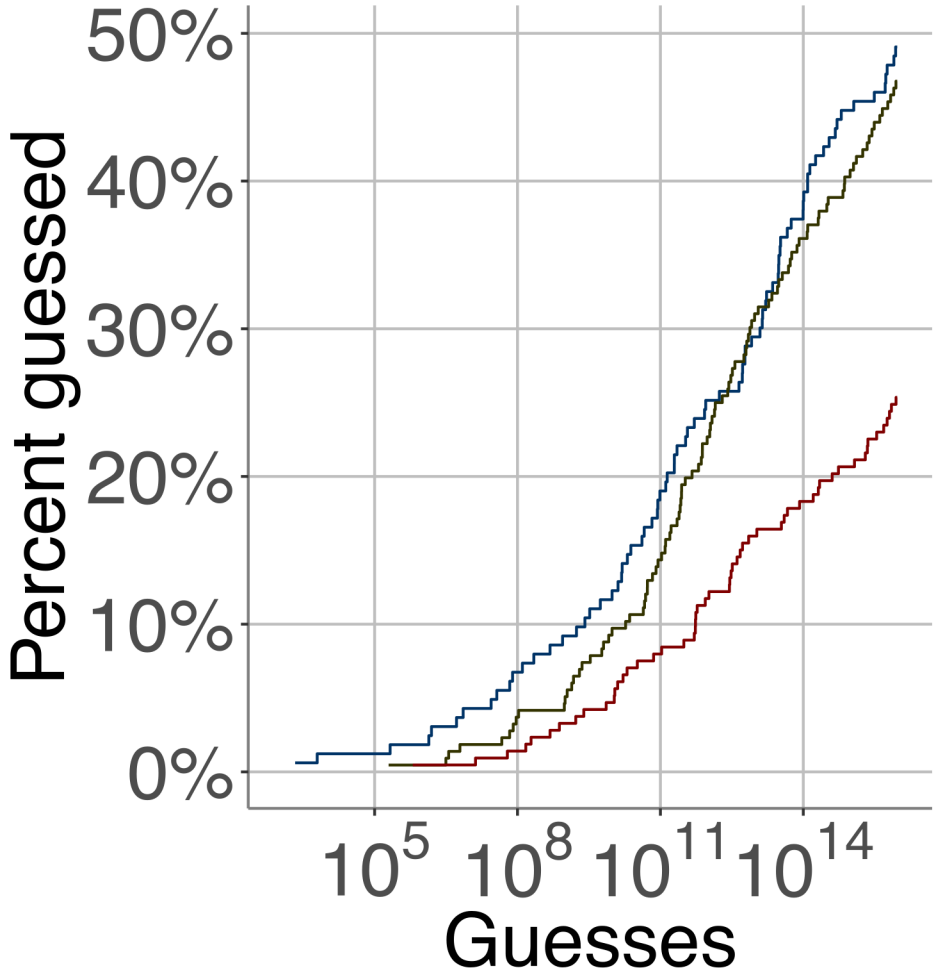
~48,000 blacklisted structures

Diminishing returns



Longer traditional policy

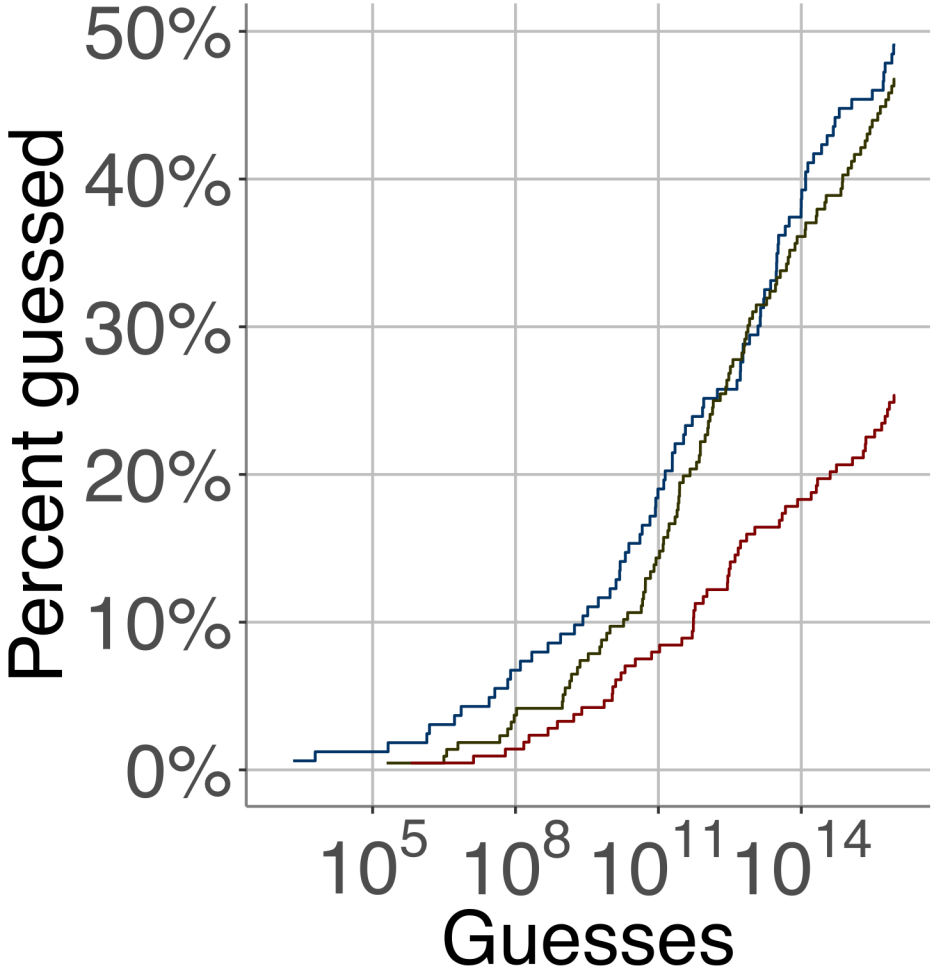
+ structure-based policy



Longer traditional policy

+ string-based policy

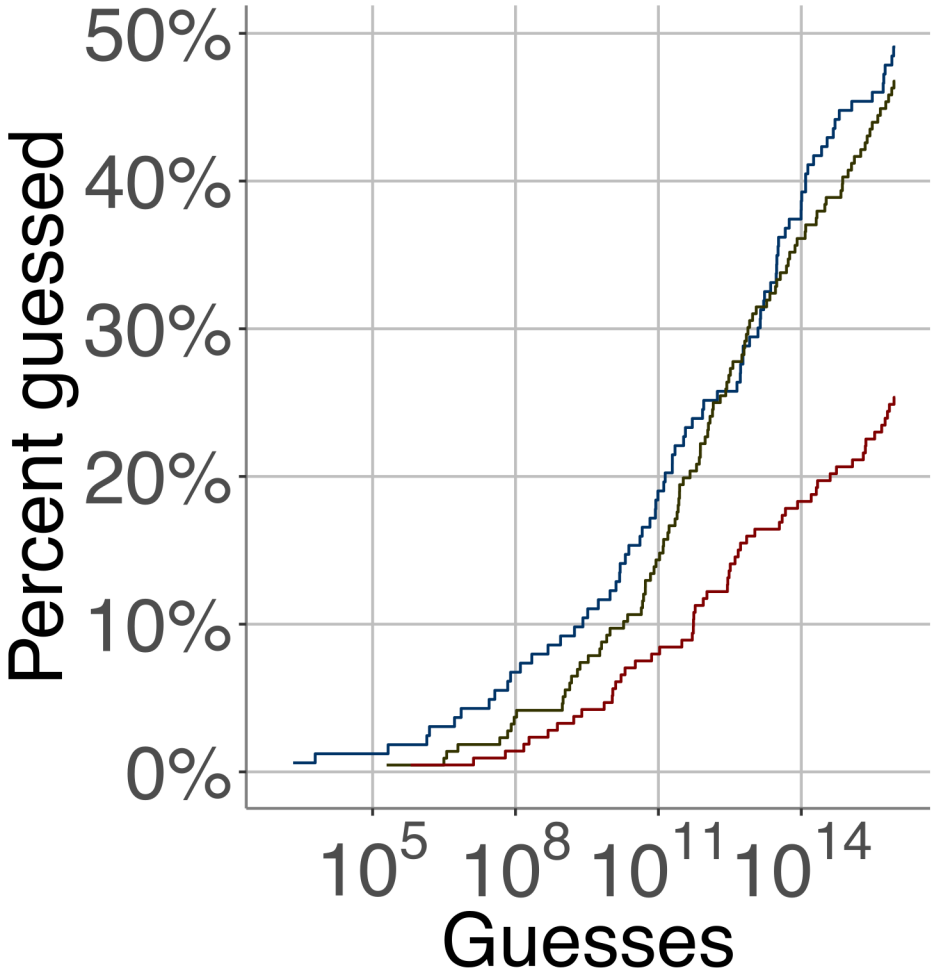
+ structure-based policy



Longer traditional policy

+ string-based policy (10,000 password “seed”)

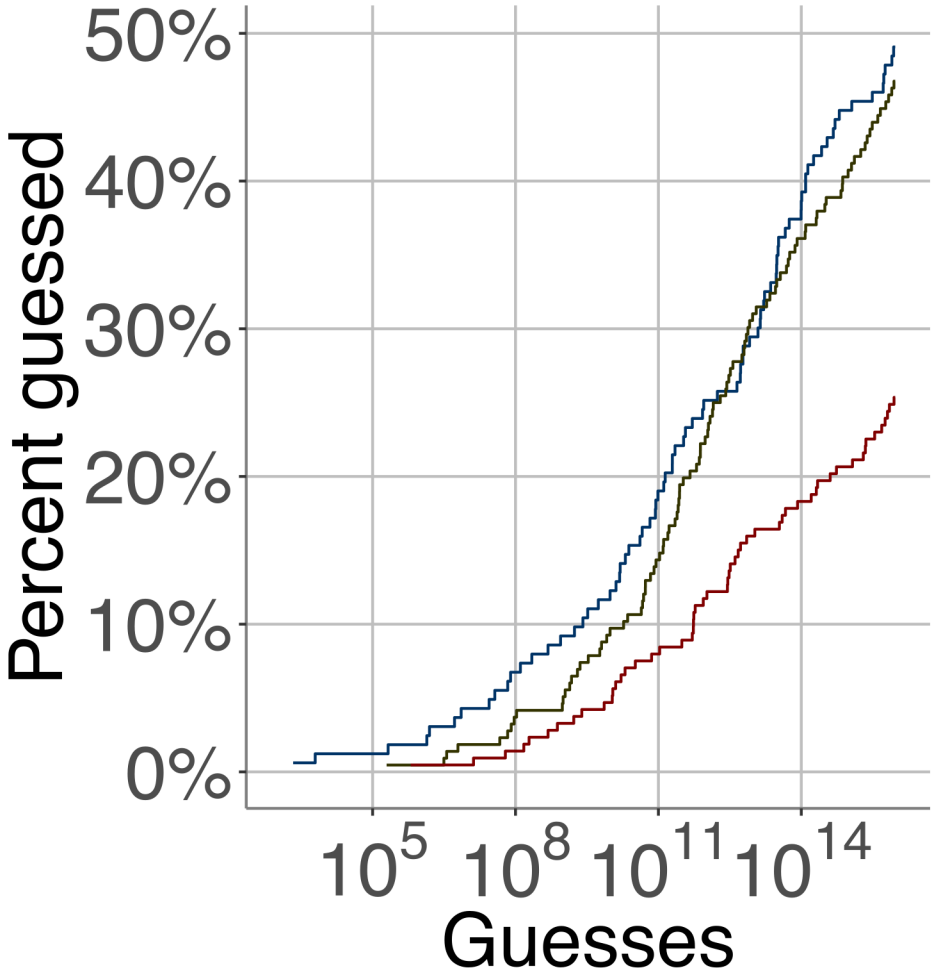
+ structure-based policy (10,000 password “seed”)



Longer traditional policy

+ string-based policy (10,000 blacklisted passwords)

+ structure-based policy (~2,000 blacklisted structures)



Longer traditional policy

+ string-based policy (10,000 blacklisted passwords)

+ structure-based policy (~2,000 blacklisted structures) (eq. ~10^{56} passwords)

Minimal Usability Costs

Minimal Usability Costs

No effect on: creation time, recall time/attempts, sentiment

Minimal Usability Costs

No effect on: creation time, recall time/attempts, sentiment

Structure-based policy: increase in creation attempts

- 1.5 vs. 2.1 attempts

Minimal Usability Costs

No effect on: creation time, recall time/attempts, sentiment

Structure-based policy: increase in creation attempts

1.5 vs. 2.1 attempts

Larger structure blacklist: more creation attempts

2.1 → 2.5 → 2.6 attempts

Diversify to Survive: Making Passwords Stronger With Adaptive Policies

Diversify to Survive: Making Passwords Stronger With Adaptive Policies

Adaptive policies can:

Diversify to Survive: Making Passwords Stronger With Adaptive Policies

Adaptive policies can:

- ✔ Increase password guessing attack resilience

Diversify to Survive: Making Passwords Stronger With Adaptive Policies

Adaptive policies can:

- ✔ Increase password guessing attack resilience
- ✔ Be implemented with minimal usability costs

Diversify to Survive: Making Passwords Stronger With Adaptive Policies

Adaptive policies can:

- ✔ Increase password guessing attack resilience
- ✔ Be implemented with minimal usability costs

Sean Segreti, William Melicher, Saranga Komanduri, Darya Melicher, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Michelle Mazurek

Diversify to Survive: Making Passwords Stronger With Adaptive Policies

Adaptive policies can:

- ✔ Increase password guessing attack resilience
- ✔ Be implemented with minimal usability costs

Sean Segreti, William Melicher, Saranga Komanduri, Darya Melicher, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Michelle Mazurek

ssegreti@cmu.edu Twitter: @cylab

Carnegie Mellon UNIVERSITY OF MARYLAND THE UNIVERSITY OF CHICAGO