Online Password Attack and Prevention Methods

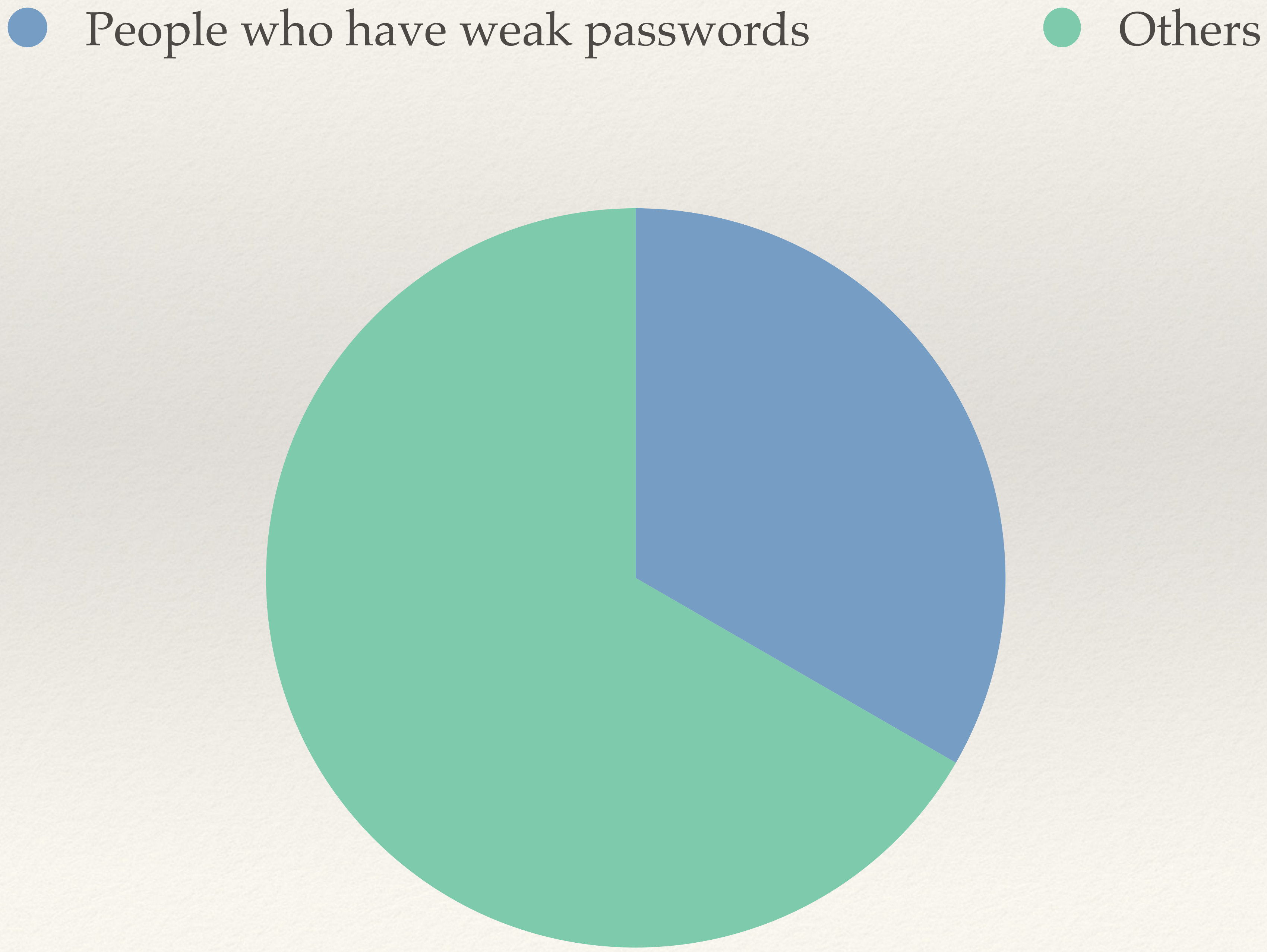
Boya Song
Rui Dai
Sam Olds

Numbers

Today an average person have over **27** passwords to remember

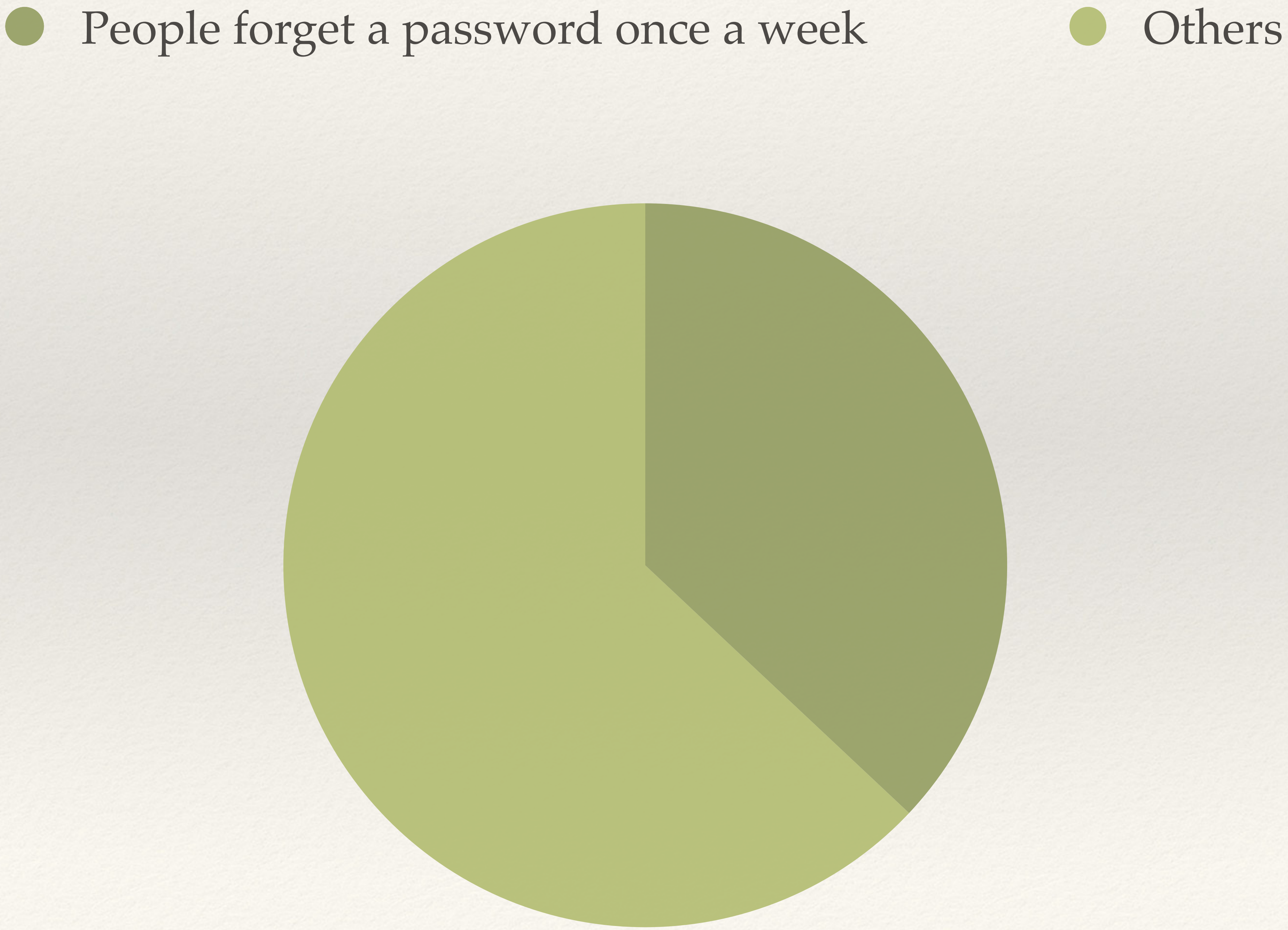
Numbers

- More than **1/3** people don't make passwords strong enough



Numbers

- **37%** percent of people forget a password at least once a week



Numbers

Average of **37** *"forget password"* email per email address

Has this happened to you?

- You have a set of passwords that you remember and use, but can't remember which password you choose for account x.
- You try to reset your password but can't remember the answer to your secrete questions
- You try to figure out which password you used, but had three wrong attempts in a row, now your account is locked...

Online Dictionary Attack

You might not realize,
but you just attempted an
online dictionary attack

Online Dictionary Attack

Definition

- An attacker moves down a dictionary of possible password and attempt to break into an account

Online Dictionary Attack

How can we effectively stop this attack while not denying service to legitimate user?

We will look into this problem from two approach

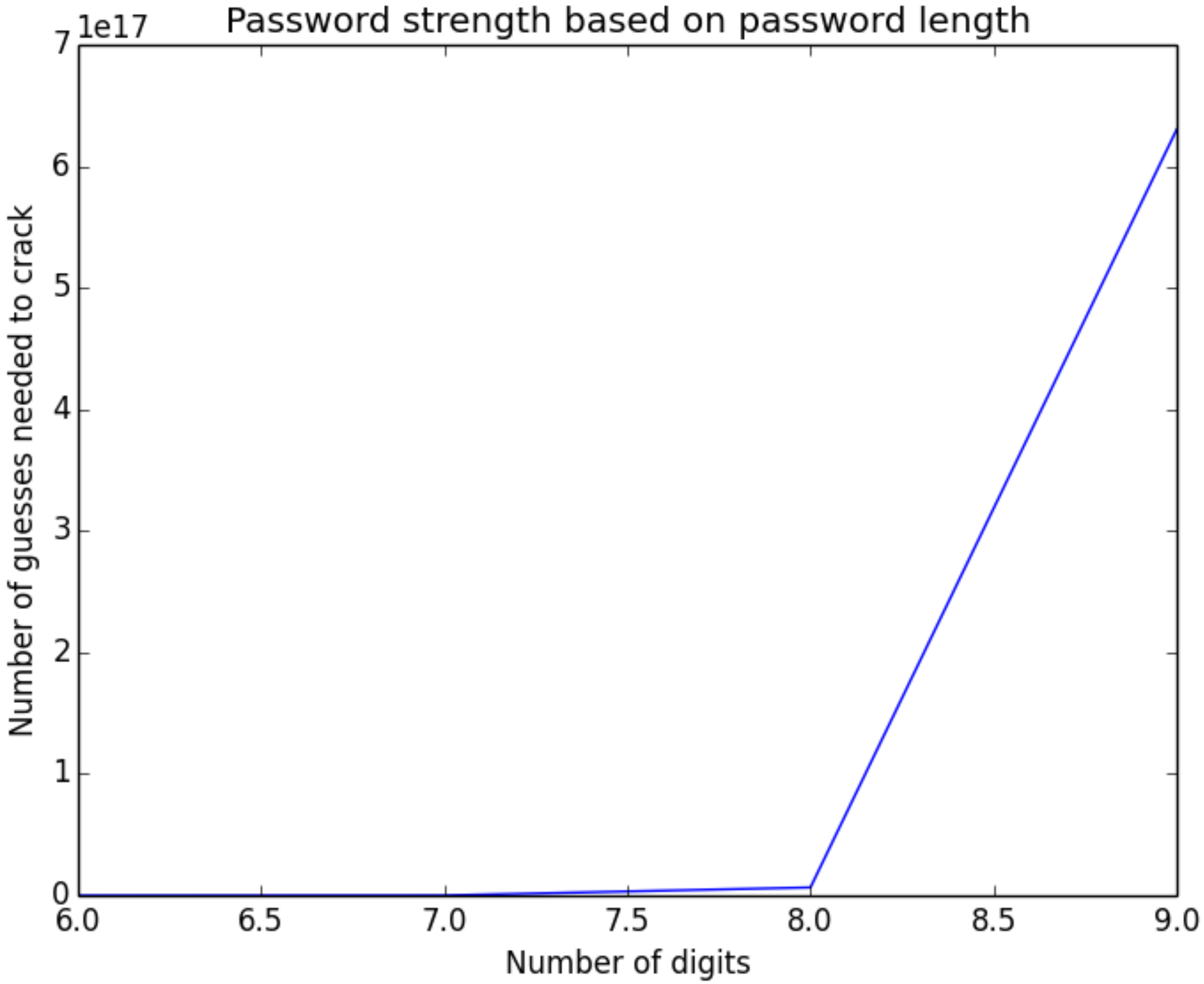
- Increase password strength
- Reduce number of password guessed

Password Strength

The properties to investigate:

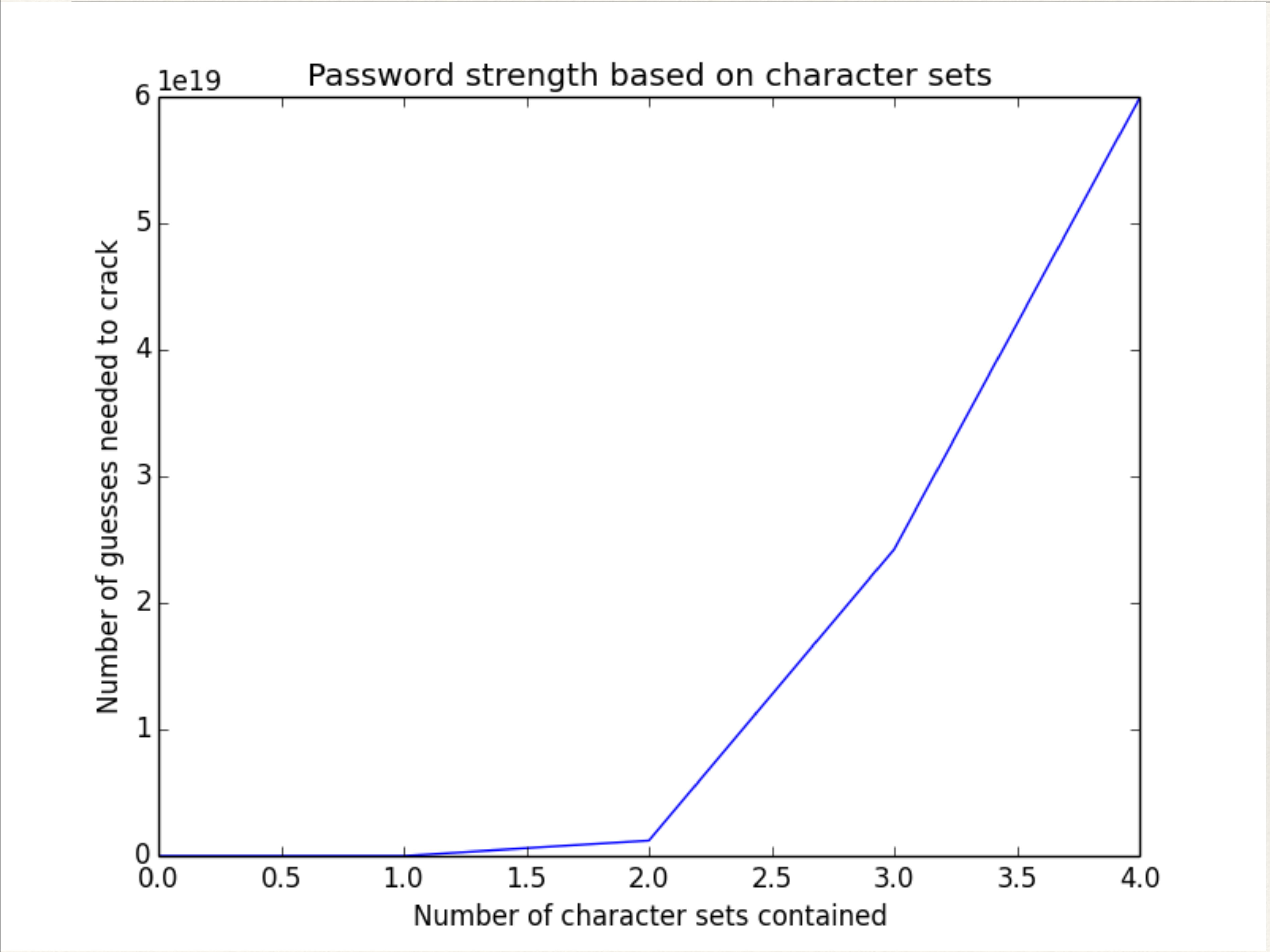
- Different length
- Combinations of character sets
  - upper case(26)
  - lower case(26)
  - number(10)
  - special characters(33)
- If contains critical information

Password Strength - Different Length



It's straightforward: Longer passwords are hard to crack!

Password Strength - Different Characters Combination



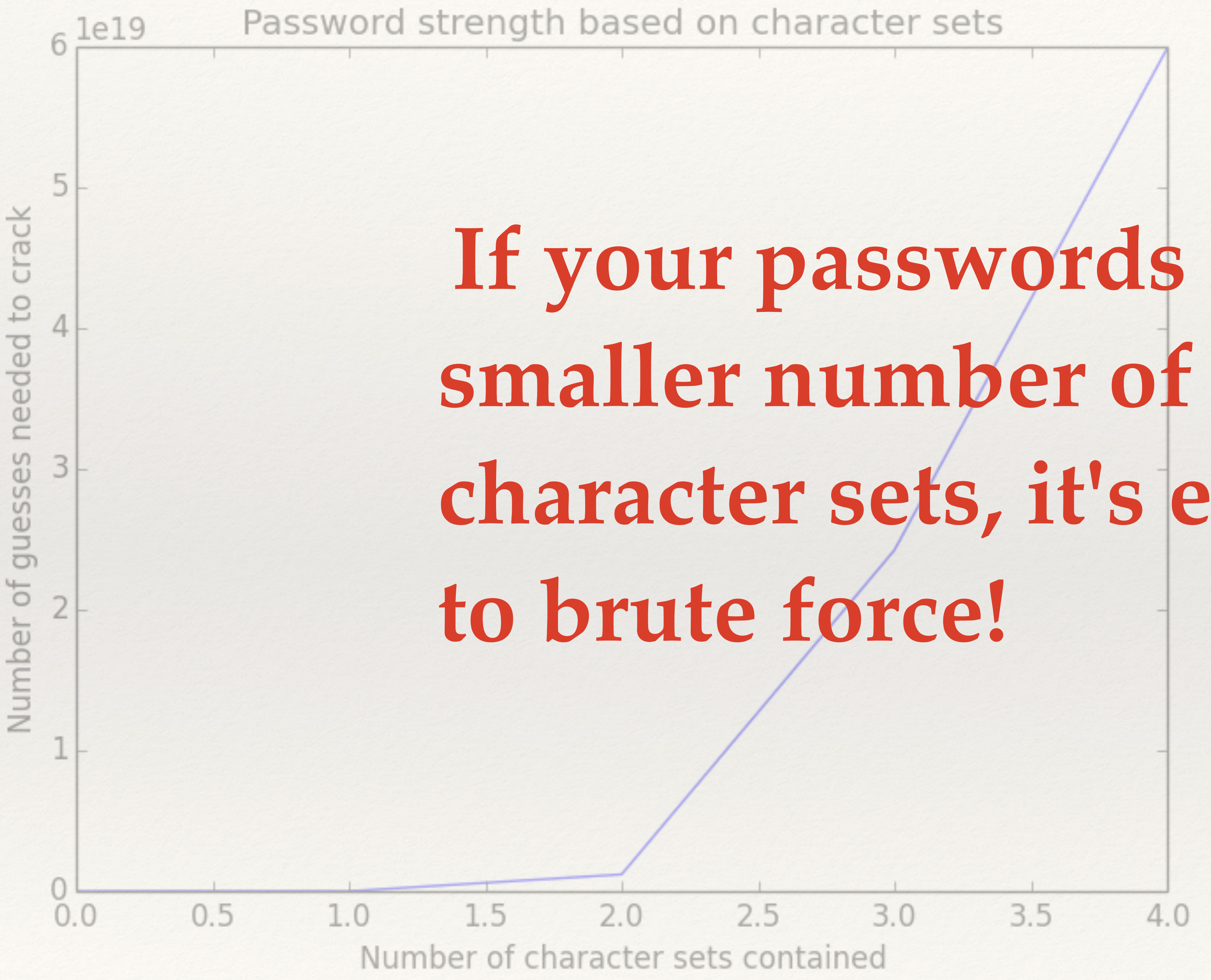
Character sets:

- upper case(26)
- lower case(26)
- number(10)
- special characters(35)

Bad passwords:

- 00000000
- 123456789
- admin
- ...

Password Strength - Different Characters Combination



If your passwords have smaller number of character sets, it's easy to brute force!

Character sets:

- upper case
- lower case
- number
- special characters

Bad passwords:

- 00000000
- 123456789
- admin
- ...

Password Strength - If contains critical information

Critical information:

- Birthday
- Name
- SSN
- ...

Bad password:

- alice1996
- 911130bob
- admin0504
- ...

Password Strength - If contains critical information

A general 8-digit password:

95 ^ 8 > 6 * 10 ^ 15

A password with critical information:
(eg. alice, 1991, 11, 30)

Just thousands of passwords!

Critical information:

- Birthday
- Name
- SSN
- …

Bad password:

- alice1996
- 911130bob
- admin0504
- …

Password Strength - If contains critical information

A general 8-digit password:

$95^8 > 6 * 10^{15}$

A password with critical information:
(eg. alice, 1991, 11, 30)

Just thousands of passwords!

Critical information:

- Birthday
- Name
- SSN
- …

Bad password:

- alice1996
- 911130bob
- admin0504
- …

If your passwords contains critical information and the attackers happen to know, they have much smaller set to brute force!

Password Strength

- Summary

Use different long and complicated passwords without your critical information!

But like ...

!1xwerjnv49j2345$%^*123lkajdbjbjahsgd?

?

????

Password Strength

It's painful to remember bunch of complicated passwords!

- Solution

Use password management tools like *1password* ! Each time it will generate a password for each application, the only thing you need to remember is a master password. Simple and secure!

(not an advertisement!)

Servers Side

In addition to strong passwords on the client side, servers can perform additional techniques to combat Online Dictionary Attacks.

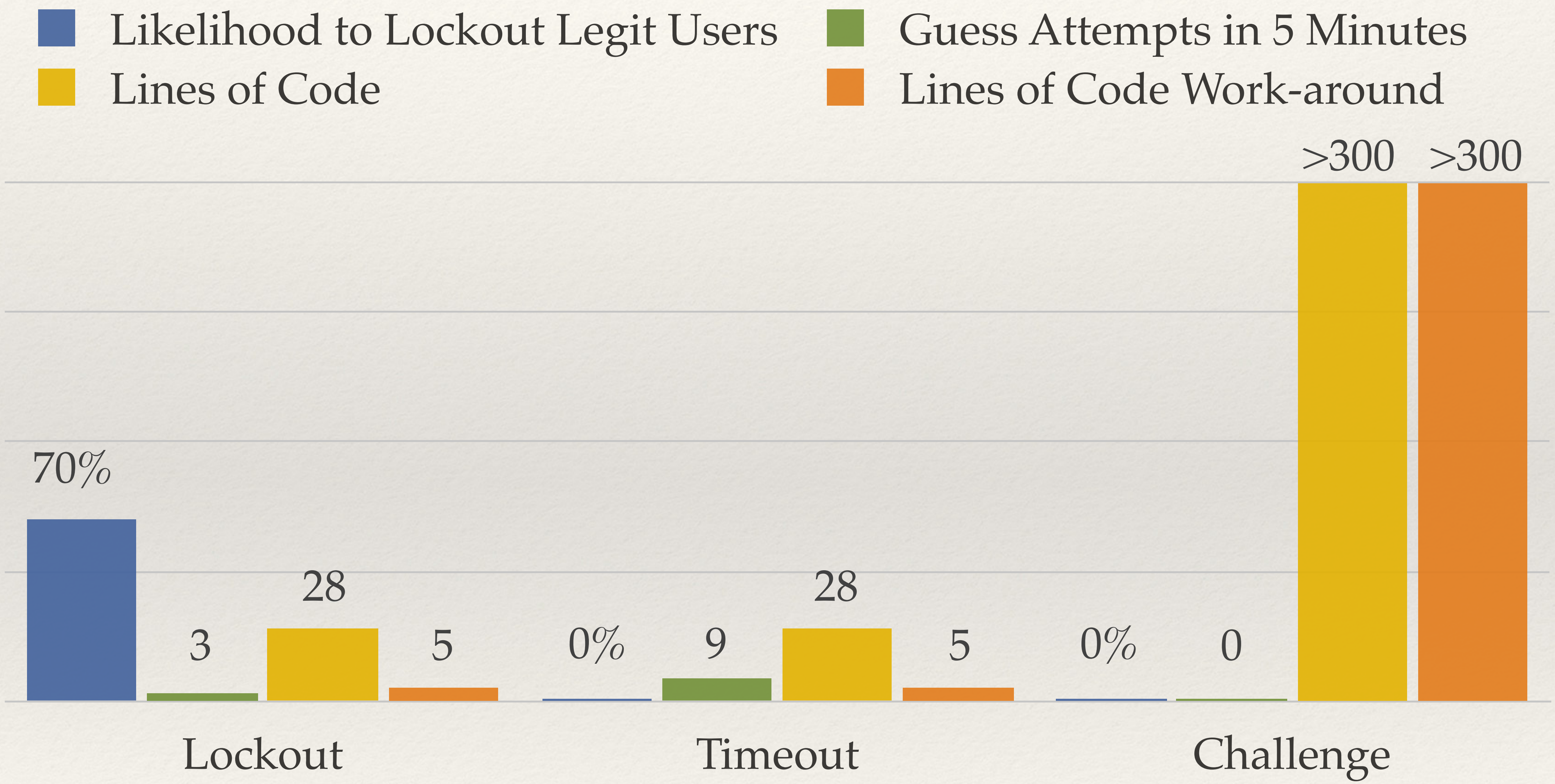
Reduce number of guesses

- Lock out account after 3 failed attempts
- Incrementally lock out user account (2^attempts second delay)
- Reverse Turing test (trying to guarantee a human is there)
    - Captcha, math problems, etc.

Reduce number of guesses

- We evaluated each method with the following criteria:
  - Ease of implementation
  - Likeliness to lock out legitimate user
  - Ease of implementation for counter measures
  - Number of passwords tried within 5 minutes

Evaluation



Likelihood to Lockout Legit Users
Guess Attempts in 5 Minutes
Lines of Code
Lines of Code Work-around
70%
3
28
5
0%
9
28
5
0%
0
>300
>300
Lockout
Timeout
Challenge

Summary

- Incremental delay has the best bang for your buck
- But reverse Turing test is your best bet if you would like a method that locks out bots but not legit users